

## Awali, Elabe

---

**From:**  
**Sent:** Monday, June 17, 2019 3:31 PM  
**To:** Wood, Kathleen  
**Cc:**  
**Subject:** Fw: P5 material - GAC  
**Attachments:** RRM Canada Ukraine Elections Final Report.pdf; IB\_LBP-#12412392-v1-RRM Canada - Ethical and Methodological Framework (J....docx; 1. Alberta Elections Analysis.docx; IB\_LBP-#12427128-v1-Briefing to P5.DOCX; IB\_LBP-#12427111-v1-Briefing to P5 - June.ppt

TTo be added to Panel binder

Sent from my BlackBerry 10 smartphone on the Bell network.

---

**From:** Tara.Denham@international.gc.ca  
**Sent:** Monday, June 17, 2019 2:10 PM  
**To:**  
**Cc:** eric.gordon@rcmp-grc.gc.ca;  
Marketa.Geislerova@international.gc.ca; Shelley.Whiting@international.gc.ca  
**Subject:** P5 material - GAC

Please find attached the material that DM approved to share with the P5 in advance of the briefing on June 20. The Ukraine report, Ethical & Methodological Framework and the Alberta report can be shared in advance. I will then bring hard-copies for the deck to share as visuals.

In addition are the talking points that would guide my intervention – focusing on tactics and trends that we see.

Thanks

Tara

Tara Denham  
Director, Centre for International Digital Policy | Directrice, Centre pour la Politique Numérique Internationale  
[tara.denham@international.gc.ca](mailto:tara.denham@international.gc.ca)  
Telephone | Téléphone: 343-203-2322  
125 Sussex Drive | 125 promenade Sussex  
Foreign Affairs, Trade and Development Canada | Affaires étrangères, Commerce et Développement Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

Canada



TOGETHER • ENSEMBLE

**CANADA**

UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU

2021-2022

*Together, celebrating the 70th Anniversary of the UDHR.*

*Ensemble, célébrons le 70<sup>e</sup> anniversaire de la DUDH.*

## 2019 UKRAINIAN ELECTIONS FINAL REPORT

### Purpose

[1] This open source report is the final report in a series prepared by Rapid Response Mechanism (RRM) Canada on Foreign Interference (FI) during the 2019 Ukrainian presidential elections. The aim of the series was to enhance the global understanding of contemporary threats to democratic systems of governance while informing Canadian efforts aimed at safeguarding Canada's elections from FI. This report is a summary of key findings from the series of reports that was produced with the objective of identifying key lessons learned from the Ukrainian presidential elections. The reports were based on secondary sources, including insight from the RRM network and the community of experts, as well as primary research conducted by RRM Canada leveraging its open data monitoring and analytical capacity.

### Overall Assessment

[2] Based on evidence summarized below and previous RRM reports, the Ukrainian presidential election was likely the target of a Russian FI campaign aimed at undermining local and international confidence in the Ukrainian democracy. Initial assessments by multiple observation teams conclude that this FI campaign did not achieve its aim.<sup>1</sup> Key findings include:

- Russian speakers were a priority audience for accounts employing automation.
- With the exception of the days following major incidents such as the July 2014 downing of Malaysian Air flight MH-17, covert social media influence campaigns appear most active during election periods in Ukraine as well as the days immediately following.
- Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.
- "Meta-trolling" or content designed to be detected and called out as Russian propaganda in order to discredit the information it contains may be a newly emerging tactic which RRM Canada will continue to monitor.

### General Observations – Secondary and Primary Sources

#### Tactics/Strategies

[3] Reporting from

notes a high degree of automation observed in social media posts about Ukraine's elections. RRM Canada observed similar automated accounts or bots. In addition to the use of bots, RRM Canada observed that many accounts used a random string of alphanumeric characters as a username. These accounts were mostly created after January 2019 and were posting in the Russian language about the Ukrainian elections. The usernames and young age of these accounts indicates that a computer program was likely used to quickly generate new accounts for use in bot networks. Additionally, RRM Canada notes that the highest degree in automation was observed within communities discussing the Ukrainian elections in the Russian language indicating that Russian speakers were likely a priority target audience.

[4] Historical Twitter based analysis has shown that accounts associated with the Kremlin have been most active following the May 2014 elections. However, tweet volume was much smaller in comparison to the July 2014 downing of Malaysian flight MH-17.<sup>2</sup> While RRM Canada does not have a database of accounts associated with the Kremlin, within our collection of accounts discussing the 2019 elections,

---

<sup>1</sup> Previous reporting

<sup>2</sup> <https://voxukraine.org/longreads/twitter-database/index-en.html>

our team observed a large spike in account creation dates from 2014. Further analysis of account creation dates reveals another spike in January 2019. This spike was most pronounced among accounts posting in the Russian language. This indicates that although far below the level of resources dedicated to deflecting blame away from Russia for the downing of MH-17, covert social media influence campaigns are probably most active during election periods in Ukraine. Our data also indicates a spike in posting activity in the days immediately following the elections however, examination of the posts did not reveal any specific narrative being amplified.

[5] Two tactics which have to date been less frequently reported, were observed much more prominently during the Ukraine elections. These tactics were the purchase or renting of social media accounts and the use of “meta-trolling.”

[6] New York Times and the Ukrainian Security Service (SBU) report that Russian intelligence agents had been offering to purchase or rent established social media accounts from Ukrainian citizens for the purposes of spreading divisive content or furthering other Kremlin narratives. Owners of these social media accounts reported that they were unaware they were dealing with Russian intelligence personnel or what purpose their accounts would ultimately serve once sold or rented. The number of accounts purchased by Russian agents remains unknown at this time and description of this tactic stems from a video-taped confession released by the SBU.<sup>3</sup> Given the financial and human resources required to find and purchase established social media accounts from citizens willing to sell them, it is unlikely this tactic was widespread during this election and unknown if it will be employed in other FI campaigns.

[7] Finally, Government of Canada (GoC) partners deployed to Ukraine to assist with cyber security during the elections period reported a new meta-trolling technique. In this technique, certain content was designed to be detected as Russian propaganda and publicly called out as such in an effort to discredit the information it contained. While we cannot attribute the employment of this tactic to Russia, it falls within the well-known concept of “reflexive control.” This concept, whereby specifically prepared information is conveyed in order to incline an opponent to voluntarily take a certain course of action, has a long history within Soviet and Russian military doctrine.<sup>4</sup> RRM Canada has no further information or current examples of this technique and we cannot attribute it to any particular actor at this time.

[8] RRM Canada cannot tie the employment of automated accounts or the spread of divisive content to Russia. However, Facebook did shut down thousands of accounts posting about Ukraine which they attributed to Kremlin-linked Internet Research Agency (IRA) and Sputnik News.<sup>5</sup> Based primarily on this evidence, RRM Canada assesses that the Russian state was likely conducting a disinformation campaign targeting the Ukrainian elections.

### **Narratives**

[9] In addition to observations of automation, reports from the UK Foreign & Commonwealth Office’s (FCO) Counter Disinformation Cell note divisive narratives being spread by these automated accounts. AoD notes that much of this content ostensibly<sup>6</sup> emanated from Russia and, at least for a period in late

---

<sup>3</sup> Previous reporting

<sup>4</sup> <http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/>

<sup>5</sup> Previous reporting

<sup>6</sup> Alliance for Securing Democracies methodology relies on user selection of location within preference settings.

March,<sup>7</sup> dominated approximately 13% of the conversation on social media about the Ukrainian elections. Previous RRM Canada reports have noted that divisive content was primarily along the following themes:

- Ukraine was reverting to its Nazi past while chauvinism and xenophobia were current state policy;
- Ukraine was becoming increasingly corrupt and becoming a banana republic.
- Ukraine was not capable of hosting free and fair elections; and
- The illegitimacy of the Ukrainian Orthodox Church was put forward.

[10] While the break of the Ukrainian Orthodox Church from the Moscow patriarch is uniquely Ukrainian, claims of corruption, elections fraud, and otherwise divisive content are common tropes within FI campaigns.<sup>8</sup> Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.<sup>9</sup> The Atlantic Council's Digital Forensics Research Lab notes these tactics appear to be common across both foreign and domestic disinformation campaigns targeting elections.<sup>10</sup>

### **On Gender**

[11] On the gender dimensions of FI within the Ukrainian elections, RRM Canada observed crudely Photo-shopped, degrading, highly sexualized imagery targeting the most prominent female candidate, Yulia Tymoshenko. RRM Canada cannot attribute any of these images to any specific actor. We note that this imagery dominated our collection of all images related to political candidates for a period in February indicating the possibility of some level of coordinated amplification; however, there are many plausible explanations related to this imagery.

### **On Diasporas**

[12] Lastly, RRM Canada detected and analyzed two multilingual groups discussing the Ukrainian elections in the Ukrainian, Russian and English languages on Twitter. Within these groups, relatively few indications of automated content spreading or accounts assessed to be possible Kremlin trolls were observed. Based on the mix of languages, RRM Canada assesses these communities to likely be Ukrainian diaspora communities from English speaking countries. Based on the lack of automated content spreading within these communities, RRM Canada assesses they were likely not priority target audiences for disinformation campaigns.<sup>11</sup>

Released: 4 June 2019

**Disclaimer:** Rapid Response Mechanism Canada team monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

---

<sup>7</sup> Other reports from the Alliance of Democracies did not mention the amount of content possibly emanating from Russia.

<sup>8</sup> As noted within research conducted by the Atlantic Council's Digital Forensics Research Lab.

<sup>9</sup> Previous reporting

<sup>10</sup> As presented by DFR Lab.

<sup>11</sup> Previous reporting

## ALBERTA ELECTION ANALYSIS

## PURPOSE

This report analyses open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019. Prepared in support of the [G7 Rapid Response Mechanism \(RRM\)](#), the report was penned by RRM Canada. The RRM is mandated to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

## KEY FINDINGS

Based on primary and secondary research, RRM Canada concludes that there were very likely **no significant foreign interference campaigns** targeting the Alberta election in the online space in April 2019. However, coordinated inauthentic activity was detected:

- **RRM Canada identified accounts that demonstrated coordinated inauthentic behaviour.** RRM Canada judges the activity is very unlikely to comprise one third of the online conversation as reported by [Press Progress on April 11, 2019](#).
- RRM Canada identified cases of social media accounts, which were **likely inauthentic, coordinated behaviour**<sup>1</sup> around online discussions about the Alberta election. However, the majority of these accounts were very likely not foreign.
- RRM Canada identified known national far-right and hate group actors who have previously disseminated material, **using similar tactics as known malign foreign actors.**
- RRM identified **accounts tied to lobbying groups** that were unaffiliated with a political party spreading disinformation online in the run-up to the Alberta election.
- The Alberta election provides an example of a situation where there may be evidence of **coordinated inauthentic behaviour undertaken by Canadian actors**, making the identification of foreign interference more difficult.

## Alberta Election Findings

[1] RRM Canada reviewed social media data to search for obvious cases of coordinated, inauthentic behaviour with the objective of identifying any potential foreign activities. Based on available information, it is very unlikely there was any foreign interference. The two largest components of the graph are made up of supporters of the former Premier Notley and Premier Kenney, as expected in an election campaign [Annex A].

[2] RRM Canada assesses that none of the major communities taking part in online conversations related to the elections are driven by foreign interference. The presence of automated inauthentic activities does not appear central or crucial to the overall conversation or activity.

---

<sup>1</sup> Scale of Estimative Language: Almost No Chance – [0 – 10]; Very Unlikely/Very Improbable – [11 – 29]; Unlikely/Improbable – [30 – 39]; Roughly Even Chance – [40 – 59]; Likely/Probable – [60 – 69]; Very Likely/Very Probable – [70 – 89]; Almost Certainly – [90 – 100]

[3] RRM Canada's findings stand opposite to the [April 11, Press Progress report](#), which claimed that a third of accounts talking about the Alberta election were bots. **RRM Canada's findings, using multiple tools and methods, judges that the online activity is very unlikely to comprise one third of bots.** The article appears to rely only on the online tool mentionsmap as a metric for "bot activity", which is not a proper means of assessment for inauthentic account behaviour or bot activity. RRM Canada therefore does not support the findings articulated in the Press Progress Report.

[4] RRM Canada identified communities that **demonstrated a suspicious account creation pattern that is indicative of troll or bot activity.** Recent spikes in account creation suggest the presence of accounts developed for a specific purpose; however, **the community was determined to very likely be domestic,** as it was mainly comprised of supporters of the United Conservative Party (UCP). A second small community was identified as supporters of the People's Party of Canada, which had similar suspicious patterns of account creation. This pattern was not identified within communities of supporters of the Alberta Liberal Party or Alberta New Democratic Party. The overall number of accounts is a small percentage of a larger collection [Annex B]. This highlights a key point, namely that **domestic actors are also emulating the tactics used by foreign actors, within the context of provincial elections. This behaviour will make it increasingly difficult to distinguish national from foreign interference efforts in the upcoming Federal election.**

[5] The RRM identified a small group of anonymous accounts pushing a pro-separation movement in Alberta and the Prairies. Though Alberta has an official separatist party, <https://albertaindependence.ca/>, these accounts do not appear affiliated with this movement. Creating false separatist movements or amplifying domestic ones is a known tactic in foreign interference. Though unaffiliated, at this time, RRM Canada cannot tie this small group of accounts to any foreign entity.

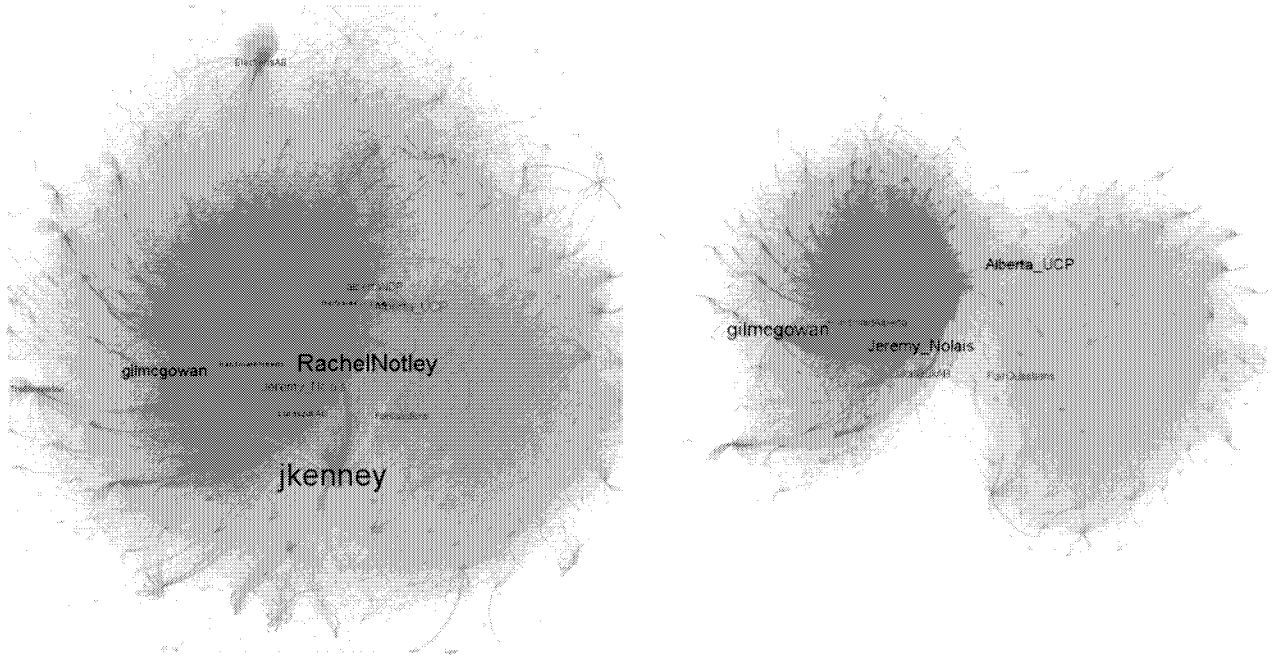
[6] In its review of the data of this election, RRM Canada found no evidence supporting a broad, coordinated campaign to influence the Alberta election. **RRM Canada assesses that automated inauthentic behaviour and trolling activities are very likely domestic in nature;**

Released: May 1, 2019

**Disclaimer:** G7 Rapid Response Mechanism Canada (RRM Canada) monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

**Annex A**

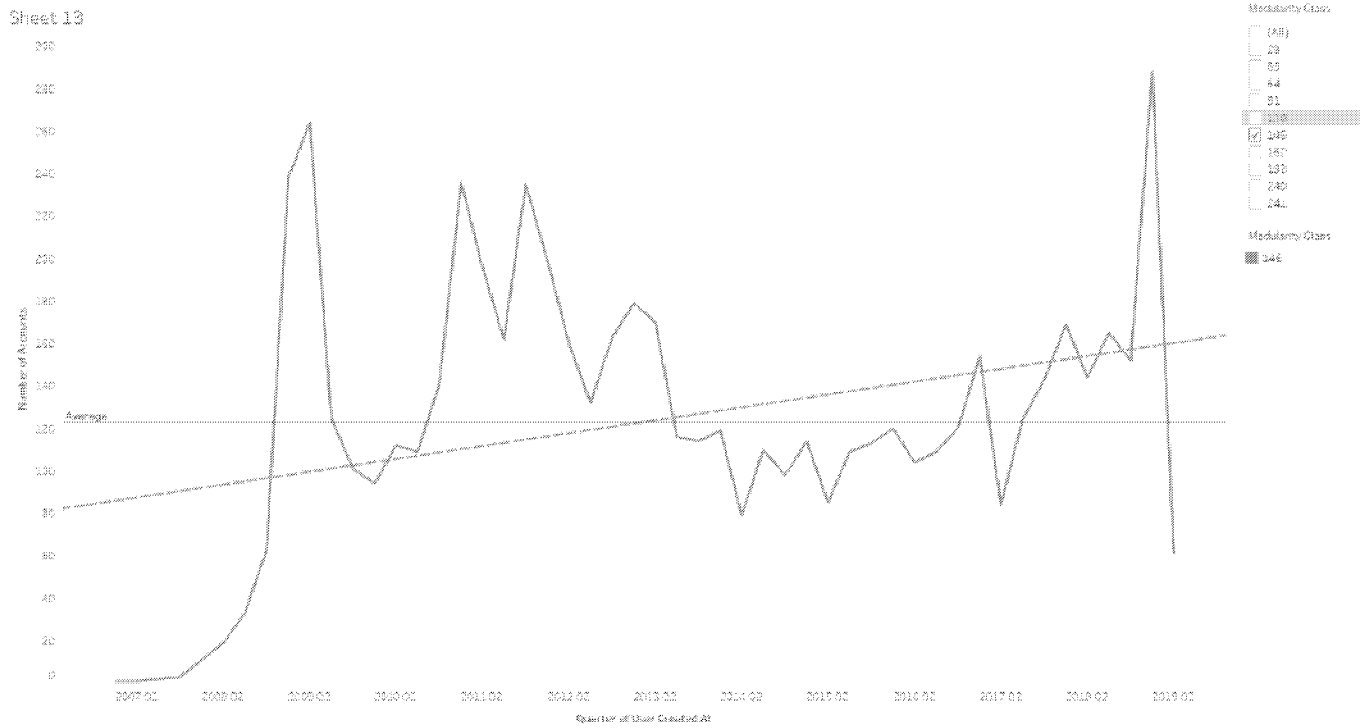
This Annex is a visual representation of RRM Canada’s data collection illustrating a high level of normality in the online conversation related to the Alberta provincial election. The analysis of activity would have been noteworthy for RRM Canada if there were other communities that rivaled the main political communities in size, but were predominately unknown actors, or actors from another geographical location.





Annex B

A review of the account creation dates of accounts in the community of UCP supporters. The size of the final spike is an indicator of inauthentic activity. One indicator of bot activity is a large number of recently-created accounts. In this case, a large spike in accounts created in Q1 2019 is suggestive of inauthentic activity by either automated accounts or anonymous accounts. This combined with a qualitative evaluation of the accounts by RRM Canada, as well as their posting behaviours and the social network analysis; these are indications of likely inauthentic behaviour.



# Key Tactics/Trends

- “Meta-trolling”
  - Example from Ukraine and US mid-terms
- Transnational narratives
  - EU Parliamentary Elections
  - Socially divisive issues
- National actors leveraging tactics
  - Alberta Provincial election

# Meta-Trolling:

Content Designed to be Seen as Russian Propaganda

**Internet Research Agency**  
**American Department** \_\_\_\_\_



## OFFICIAL STATEMENT OF THE INTERNET RESEARCH AGENCY

CITIZENS OF THE UNITED STATES OF AMERICA! YOUR INTELLIGENCE AGENCIES ARE POWERLESS.

DESPITE ALL THEIR EFFORTS, WE HAVE THOUSANDS OF ACCOUNTS REGISTERED ON FACEBOOK, TWITTER AND REDDIT SPREADING POLITICAL PROPAGANDA. THESE ACCOUNTS WORK 24 HOURS A DAY, SEVEN DAYS A WEEK TO DISCREDIT ANTI-RUSSIAN CANDIDATES AND SUPPORT POLITICIANS MORE USEFUL FOR US THAN FOR YOU.

HUNDREDS OF YOUR FELLOW CITIZENS ARE OUR UNINTENTIONAL AGENTS UNAWARE OF THE FACT THAT THEY ACTUALLY ACT FOR THE GOOD OF THE RUSSIAN 'TROLL FARM'. WE HAVE ALLIES AND SPOILERS INTERVENING THE POLITICAL CAMPAIGNS OF THE CANDIDATES FOR BOTH PARTIES. THE VICTORY OF THE DEMOCRATIC PARTY IS OUR TOP PRIORITY IN THESE MIDTERM ELECTIONS.

WHEN THE DEMOCRATS TALK ABOUT TRUMP-RUSSIA COLLUSION OR RUSSIAN-REPUBLICAN COLLUSION THAT'S BECAUSE WE WANT THEM TO SAY THIS NONSENSE. IT IS A PART OF OUR PLAN.

SOON AFTER NOVEMBER 6, YOU WILL REALIZE THAT YOUR VOTE MEANS NOTHING. WE DECIDE WHO YOU VOTE FOR AND WHAT CANDIDATES WILL WIN OR LOSE.

WHETHER YOU VOTE OR NOT, THERE IS NO DIFFERENCE AS WE CONTROL THE VOTING AND COUNTING SYSTEMS. REMEMBER, YOUR VOTE HAS ZERO VALUE. WE ARE CHOOSING FOR YOU.

# Network Analysis

# Transnational Narratives

**King Dog Of Britain** (@kdog1984) · 13 May

Salvini nails it "Who betrayed Europe? The extremists are those that governed Europe for 20 years, the elites the multinationals Soros Merkel Macron Juncker" [twitter.com/LeaveEUofficials](https://twitter.com/LeaveEUofficials) ...  
 @EUContador2000 @Smileygirl19681 @ultimateOne @Lin45222098 @SubeStabo2 @Kalimnalyinn @ICTHopkins

**King Dog Of Britain** (@kdog1984) · 13 May

Salvini nails it "Who betrayed Europe? The extremists are those that governed Europe for 20 years, the elites the multinationals Soros Merkel Macron Juncker" [twitter.com/LeaveEUofficials](https://twitter.com/LeaveEUofficials) ...  
 @EUContador2000 @Smileygirl19681 @ultimateOne @Lin45222098 @SubeStabo2 @Kalimnalyinn @ICTHopkins

**Matteo Salvini** (@m.salvini) · 13 May

Matteo Salvini Saviour of Europe  
 "Not Far Right, it's Common Sense  
 Europe of DeGaulle, Thatcher Not Merkel, Macron, Soros  
 EU Dream destroyed by Banks, Big Corps, Mass Migration"  
 Salvini, LePens, Farage, Orbán at Power Now or be S.O.N

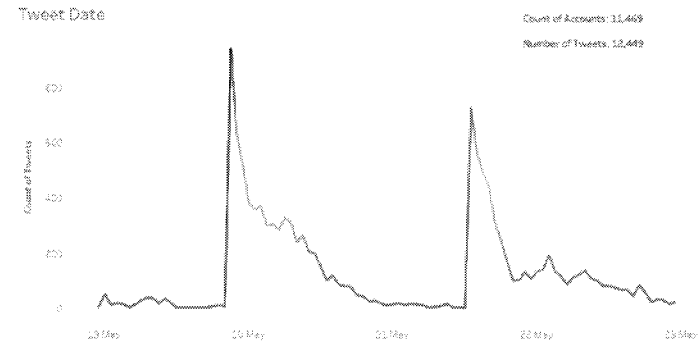
**FREE EUROPE** · 13 May

beautiful dreams hypothesized by the founding fathers?

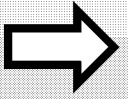
**Paul Joseph Watson** (@PjWatson) · 13 May

Salvini says the real "extremists" are the elites who occupied Europe in the name of "finance, multinationals, of money and of uncontrolled immigration."

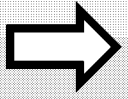
Podcast is Over



Anonymous Spreading of content

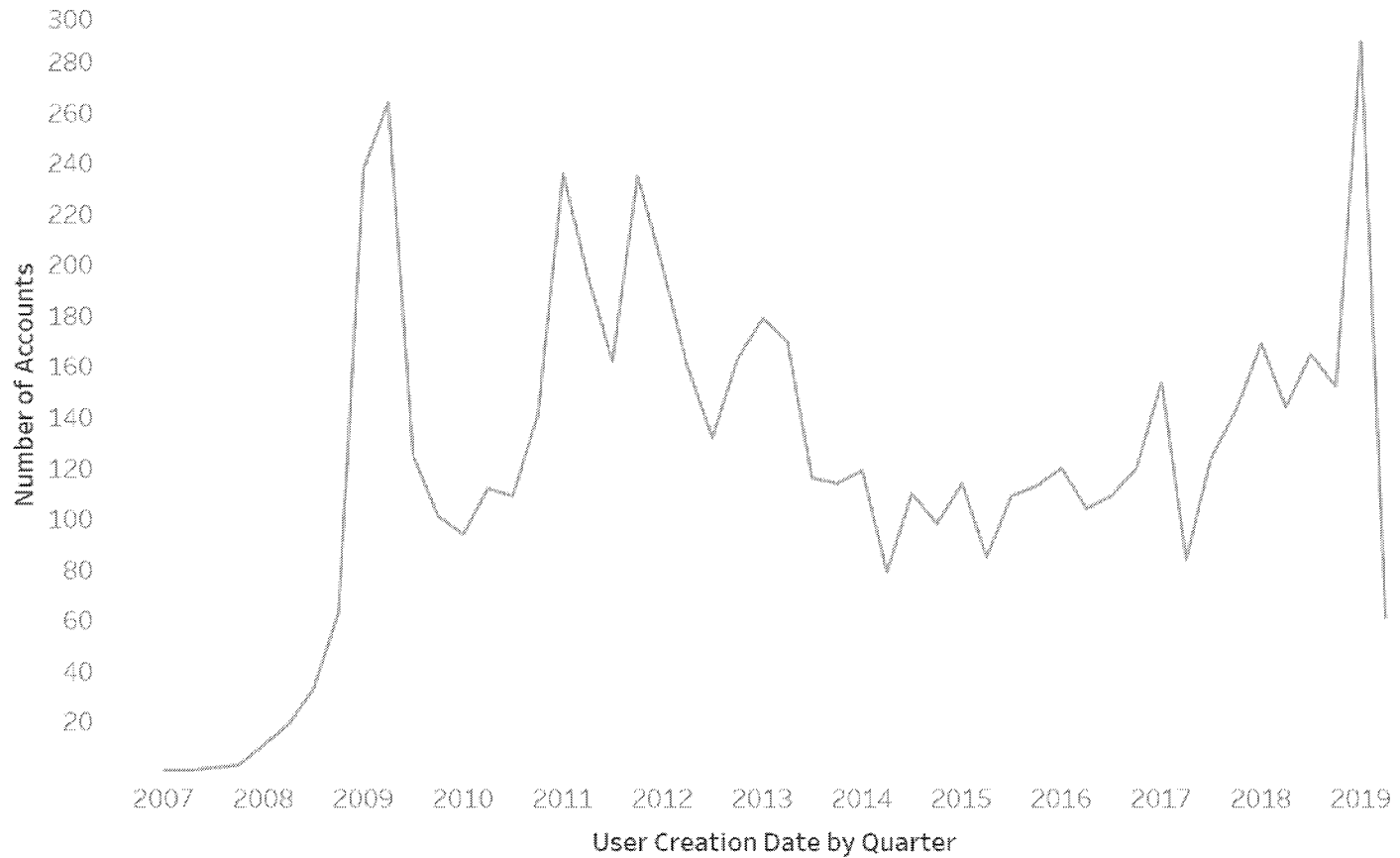


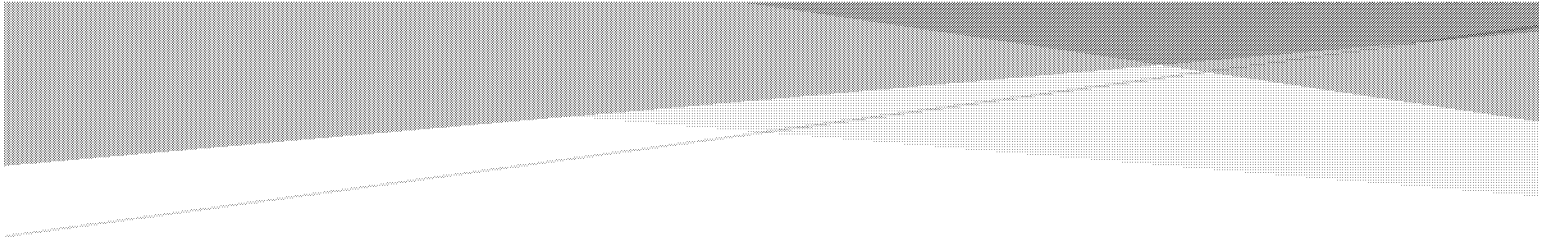
Known Far-Right Voices



Content repurposed on spreads in different languages by "alternative media"

# Account Creation Dates





# ETHICAL AND METHODOLOGICAL FRAMEWORK FOR OPEN SOURCE DATA MONITORING AND ANALYSIS

Rapid Response Mechanism Canada

Centre for International Digital Policy

Global Affairs Canada

June 2019

# ETHICAL AND METHODOLOGICAL FRAMEWORK FOR OPEN SOURCE DATA MONITORING AND ANALYSIS<sup>1</sup>

---

## Contents

- Purpose ..... 2
- Background and Mandate..... 2
- Challenges and Obstacles ..... 3
- Thresholds and Protocols..... 3
- Methodology and Tools ..... 4
- Human Rights Approach ..... 5
  - Privacy..... 5
  - Freedom of Expression ..... 5
  - Gender Equality ..... 6
- Principles and Ethical Considerations ..... 6
  - Transparency and Accountability..... 6
  - Internal Oversight and Partnerships ..... 6

---

<sup>1</sup> This document is meant to be iterative and sensitive to the evolving nature of digital technologies, foreign threats, policy orientation, and social and political issues. In developing this document several stakeholders have already been consulted, including multiple divisions at Global Affairs Canada, various other departments in the Government of Canada, the Oxford Internet Institute, and others.



## Purpose

Contemporary international relations theory and practice must consider the rapidly evolving digital information ecosystem. This ecosystem, including social media platforms and their content ranking algorithms, is creating new opportunities for economic growth and connectivity, while also presenting a range of new challenges for foreign policy. The threat from malign foreign actors, who seek to leverage aspects of this ecosystem for nefarious activities that are detrimental to our democratic systems of governance, is among the most pressing issues requiring attention by democracies such as Canada. Governments are developing new capacities to better understand this threat, including by harnessing open source data monitoring and analytical tools and approaches.

The purpose of this framework is to outline ethical and methodological principles and guidelines for open source data monitoring and analysis undertaken by Rapid Response Mechanism Canada (RRM Canada). These open source data activities support the G7 Rapid Response Mechanism (RRM) – an initiative aimed at defending G7 democracies from foreign threats as well as Government of Canada efforts aimed at safeguarding its own democratic institutions and processes, including its general elections. The need for such a framework stems from the following three needs, among others:

- 1) Anchoring these relatively new activities in an existing policy, legal, and regulatory context.
- 2) Ensuring that the activities respect and reinforce human rights and freedoms.
- 3) Providing transparency and accountability to Canadians and the G7.

## Background and Mandate

Supported by a team of policy and data analysts, RRM Canada is housed at Global Affairs Canada in the Centre for International Digital Policy. The RRM was announced at the G7 Charlevoix Summit in 2018 and re-affirmed at the G7 ministerial meeting in Dinard, France, in 2019. Led by Canada on an ongoing basis, its mandate is “to strengthen coordination to identify and respond to diverse and evolving threats” to G7 democracies.<sup>2</sup> More specifically, the foreign threats that G7 members committed to confront seek to undermine democratic institutions and processes through “coercive, corrupt, covert or malicious means.”<sup>3</sup>

While the threat landscape covered by the RRM is broad, disinformation in digital context figures prominently.<sup>4</sup> In the lead up to the RRM’s announcement, Foreign and Security Ministers recognised the threat posed by “acts or measures by foreign actors with the malicious intent of undermining trust in the independent media, manipulating public discourse, and violating privacy,” by including these activities in the Toronto Commitment, among other key illustrative examples.

Additionally, RRM Canada supports the Government of Canada efforts to safeguard the 2019 general elections. As part of the Security and Intelligence Threats to Elections (SITE) Task Force, RRM Canada works with Canada’s Security and Intelligence organisations “to prevent covert, clandestine, or criminal activities from influencing or interfering with the electoral process in Canada.” The other members of

---

<sup>2</sup> Charlevoix Commitment

<sup>3</sup> Toronto Commitment

<sup>4</sup> Digital context in this note refers to the overarching network or framing environment generated by the digital information ecosystem.

the Task Force are: the Communications Security Establishment (CSE), Canadian Security Intelligence Services (CSIS), and the Royal Canadian Mounted Police (RCMP).

- The aim of RRM Canada’s open source data activities is to support the RRM mandate to defend democracies, and help safeguard Canada’s 2019 general elections, by better understanding foreign threats in the digital context, shining light on them, and recommending effective response options.

## Challenges and Obstacles

Among the central challenges in addressing foreign interference in the digital ecosystems of G7 democracies is determining the foreign nature of the online activities being undertaken. This challenge reflects the limitations of employing open and publicly available information from social media platforms for analytical purposes. This is because foreign states and state proxies exploit the anonymity offered by digital platforms, “weaponise” elements of the digital information ecosystem, and continuously adapt to strategies aimed at stopping them. While anonymity can be integral to facilitating sensitive discussions online (where those discussions are discouraged or are otherwise dangerous to individuals engaging in them), it is also the same mechanism exploited by foreign actors to conduct coercive, corrupt, covert, or malicious activities.

Perhaps the most problematic aspect of distinguishing foreign interference from organic domestic debate is that foreign actors target domestic audiences with content that may resonate with the audiences’ pre-existing opinions and worldviews. This targeting, often undertaken clandestinely, involves a foreign actor creating content that has been designed to sow discord or exploit existing societal differences in the domestic population. When this foreign content is received by domestic audiences, it then can be amplified further either wittingly or unwittingly. This sequence intertwines foreign and domestic narratives in ways that are difficult to untangle. Foreign actors may also coerce or induce Canadians to promote a given narrative, but these overtures are often hidden and difficult to substantiate.

The challenge of separating foreign interference from domestic engagement raises the potential of inadvertently affecting the enjoyment of human rights and freedoms of Canadians, in particular, freedom of expression and privacy rights. To avoid this situation, open source data activities conducted by RRM Canada are subject to clear thresholds and protocols for monitoring, analysis, and information sharing.

- RRM Canada thresholds and protocols ensure that its open source data monitoring and analytical activities fall under the RRM mandate, safeguard and reinforce human rights and freedoms of Canadians, comply with relevant legal and regulatory provisions, and meet high ethical standards.

## Thresholds and Protocols

RRM Canada has developed thresholds for what are considered coercive, corrupt, covert or malicious activities as well as protocols for open source data monitoring and information sharing activities. To be the subject of RRM Canada monitoring activities, an account or network of coordinated accounts must display a number of characteristics outlined in the RRM Canada methodology. The methodology sets high thresholds established in cooperation with leading experts; computational social scientists; and

security, intelligence, and law enforcement organisations. Additional factors for open source data activities include concurrence with secondary sources and significant impact on public discourse.

These thresholds inform RRM Canada's monitoring activities, including its approach to analysing suspicious accounts and networks associated with foreign interference. These thresholds are not impacted by the accuracy or perceived acceptability of content that any given account or network disseminates. In the event that a foreign connection cannot be established within a reasonable period, monitoring activities cease, and no data is retained. However, in cases when suspicious activities may potentially meet criminal or national security thresholds, insight is shared with security, intelligence, and law enforcement organisations. When activities may potentially contravene the Canada Elections Act, the Commissioner of Canada Elections will be notified by RRM Canada. These organisations independently determine whether or not an investigation is required pursuant their respective mandates and legislative frameworks.

Furthermore, in January 2019 the Government of Canada announced a number of new measures to protect the 2019 general election, including the Critical Elections Incident Public Protocol. This Protocol lays out a clear and impartial process by which Canadians may be notified of a threat to the integrity of the elections that occur within the writ period.

## Methodology and Tools

RRM Canada examines trends, anomalies, and emerging narratives in online conversations across the digital information ecosystem pertaining to potentially divisive issues and public political actors that could be exploited by malign foreign actors. By observing baseline structures of what are considered normal conversations surrounding issues, as they evolve over time, it is possible to identify abnormalities that may indicate a concerted foreign information operation. RRM Canada examines multiple indicators of coordinated foreign interference campaigns, some of which are indicative of foreign coercive, corrupt, covert, or malicious behaviour.

Caution is exercised in divulging detailed indicators pertaining to threshold-setting in order to prevent malign foreign actors from developing counter strategies. Nevertheless, indicators for covert behaviour can include artificial or inauthentic amplification of narratives, for example. Narratives can be amplified by employing different tactics including bots, botnets, and trolls. RRM Canada uses indicators to identify bot and troll activity, as well as those to identify the foreign nature of suspicious activities. All determinations are made based on a confidence scale and identified using estimative language.

To monitor and analyse potential foreign interference, RRM Canada uses tools that are publicly available. The combination of these tools is not released in order to prevent malign foreign actors from developing strategies in response. To complement their use, RRM Canada also experiments with open source data modeling, natural language processing, social network analysis, machine learning and algorithms all of which process only openly available public data. Any automated outcomes these technologies render can be meaningfully explained.

- The methodologies and tools employed by RRM Canada are consistent with those adopted and employed by various actors in the private and public sectors as well as non-government organisations and advocacy groups. This is in line with a growing awareness of the digital information ecosystem as an important political, social, economic, and cultural space.

## Human Rights Approach

Leading to the Charlevoix announcement of the RRM, all G7 Foreign and Security Ministers endorsed a strategic approach to responding to foreign threats that is consistent with universal human rights and fundamental freedoms. Canada is committed to respecting its international commitments and obligations including being a party to the International Covenant on Civil and Political Rights. In Canada, the Charter of Rights and Freedoms protects a number of rights and freedoms, including those most evidently impacted by foreign interference in digital contexts, namely: privacy rights, freedom of expression, and the right to equality.

## Privacy

The subject of RRM Canada open source data monitoring and analysis is limited to publicly available data. RRM Canada monitors, analyses, and shares information in a manner that is consistent with Canada's privacy laws, the Access to Information Act, and the Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities. The information sharing practices of Global Affairs Canada to which RRM Canada adheres are subject to review by multiple actors, including: the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians. All RRM Canada analysts are required to complete the Access to Information and Privacy Fundamentals course, in order to strengthen the understanding of what is considered personal information and how best to protect it.

Moreover, RRM Canada takes care to limit unintended harms and therefore, is additionally guided by firm ethical and principled considerations to facilitate responsible practices for handling personal data, even if it is publicly available. The focus of RRM Canada's open source data monitoring and analysis is trends, tactics, and strategies undertaken by malign foreign actors. The questions RRM Canada seeks to answer include: How do foreign states and their proxies exploit online discussions? What tactics do they employ for coercive, corrupt, covert or malicious activities? How do they leverage tactics such as artificial or inauthentic amplification to manipulate online discussions and what type of coordination strategies do they employ? How do these tactics and strategies evolve over time?

## Freedom of Expression

RRM Canada seeks to identify foreign activities with a coercive, corrupt, covert, or malicious dimension, which attempt to sway public opinion to undermine Canadian democracy. To mitigate risks related to the difficulty of separating foreign and domestic activities and unwittingly impinging upon the freedom of expression of Canadians, RRM Canada:

- Focuses on the structure and context of conversations, as opposed to the content, to understand what indicators may signal foreign interference.
- Relies on established open source data monitoring protocols that set out thresholds for foreign activity and guide information sharing with Canadian security, intelligence, and law enforcement organisations as well as the Commissioner of Canada Elections.
- Excludes personally identifiable information from public reports. In certain cases such as national security considerations shares such information with responsible security organizations.
- Does not undertake active measures or engage in any way with content creators or those sharing content.

## Gender Equality

RRM Canada adopts a Gender-Based Analysis Plus (GBA+) approach as it undertakes open source data monitoring and analytical activities. Malign actors target, exploit, and sometimes co-opt women and marginalized groups and issues in their activities to undermine social cohesion. Understanding how these processes occur and how they differentially impact these groups is crucial to both countering foreign interference and protecting human rights.

The methodological approach is also informed by academics and civil society organisations who are experts on gender and intersectional identity issues. Several of these interlocutors are conducting research that directly supports the RRM Canada mandate. Finally, all RRM Canada analysts are required to take the [Gender-Based Analysis Plus \(GBA+\) online course](#) and integrate the approach systematically into their work.

## Principles and Ethical Considerations

RRM Canada has incorporated principles and ethical considerations beyond the existing legal and policy considerations to enhance its approach to open source data monitoring and analysis that is effective in protecting Canadians, while limiting undue and unintended harms.

## Transparency and Accountability

RRM Canada is committed to working in a manner that prioritizes transparency and openness. Our commitment is reflected in the following actions:

- Treatment of open and publicly available data *only*.
- Focus on tactics, strategies, and trends.
- Use of publically available tools, explainable algorithms and other technologies.
- Ethical and human rights respecting approach to monitoring and analysis.
- Established thresholds and information sharing protocols with Government of Canada organisations and G7 partners.
- Systematic engagement with a wide network of experts, academics, and civil society actors.

## Internal Oversight and Partnerships

RRM Canada has developed an internal review mechanism to ensure analytical accuracy and robustness. Its multi-disciplinary team of social scientists, data experts and policy analysts allows for the agility and capacity to address evolving threats, while incorporating broader perspectives into its open source data activities. RRM Canada frequently engages in challenge functions or a peer-review process within the Government of Canada. This allows final conclusions to be determined through a rigorous process whereby results are challenged by fellow analysts and possibilities of cognitive and other bias are reduced. Collaboration beyond the Government of Canada is essential for developing innovative open source data monitoring and analytical capacity. RRM Canada relies on a growing community of experts which includes representatives from other governments, academia, civil society, and non-governmental organisations.

## Briefing to P5

June 21 8:30-11:30am

### GAC/RRM's role in SITE

- The RRM came out of Canada's presidency of the G7 last year, and is a concrete and demonstrable effort by the G7 to respond to emerging threats to democracies
- It will be led by Canada on an ongoing basis – Coordination Unit housed at GAC
- At its core – it's about open-source/unclassified information sharing and analysis across the G7, to understand emerging threats to G7 democracies, and identify opportunities for coordinated response as required.
- Mandate is the full spectrum of threats to democracy (coercive, corrupt, covert and malicious foreign interference that negatively impacts our democracies). Given the level of interest and need to consolidate international expertise on the issue, **disinformation** is a central focus of the RRM over its initial year of work – and particularly relevant to GAC's contribution to SITE.
- We also have a specialized expertise to undertake SM analysis related to disinformation.
- Focus: identify overarching tactics and trends in the disinformation landscape in order to identify inauthentic activity and amplification of content, and based on a methodology, see if there is evidence of potential foreign interference.
  - We use publically available tools
  - We don't monitor for individuals (individuals may appear in searches – as it would do if a person was looking through openly available data), but we don't monitor or focus on individuals when reporting on trends or tactics
  - We only access openly available information (information anyone else could see)
    - due to complexity of tactics used.
    - Clear definition of mandates and authorities with other members of SITE.
- Guided by ethical and methodological framework.
- Products: monthly newsletter (the Wire); deep dive reports on particular issues or tactics; and monthly social media trend analysis related to the upcoming federal election.
- Given our ability to watch for trends in the social media landscape for inauthentic or amplified content, our role is an **'early warning' system** which may initiate further investigation by other entities should there be sufficient information available to meet mandates and legal authorities ; to educate GoC and others on the complexity of the landscape and emerging trends (Alberta, Ukraine & EU elections); and not focused on attribution per se.

s.21(1)(b)

s.16(1)(c)

### Examples of work

- **US mid-term elections & Ukraine:** "meta-trolling" – Openly claiming disinformation campaigns  
  
Content designed to be detected and called out as Russian propaganda in order to discredit the information it contains (Ukraine). This tactic is designed to call into question the legitimacy of an election or any given piece of information by deliberately associating it with "Russian Trolls"

s.15(1)

- **Alberta:** evidence of coordinated inauthentic behavior undertaken by Canadian actors – more challenging to identify foreign interference. Tools include historical analysis of account creation (spike with Twitter creation, again before election). News reports on high level of bot activity – not validated by RRM Canada. Although did see use of amplification tactics by national actors. Low barriers to entry for use of bots as tactic.
- **EU Parliamentary elections:** transnational narratives on divisive issues (climate change, immigration, LGBTQ, religious intolerance) being amplified across borders, but a mix of national and international actors involved. See attempt to reproduce and repurpose narratives in regional/international context, promoting similar narratives and sentiments around divisive issues (mostly far-right community). Again, increased complexity to identify foreign interference.

**Awali, Elabe**

---

**From:**  
**Sent:** Wednesday, August 28, 2019 3:23 PM  
**To:**  
**Subject:** RRM reports to flag to NSIA  
**Attachments:** RRM Wire - August 2019; RRM Wire - July 2019; RRM Canada: Alberta Elections Analysis and NATO StratCom Report; RRM Canada: Final Ukrainian Elections Report ; RRM Canada: European Parliamentary elections report

Hi

Per today's discussion, I have attached the five reports that GAC intends to post to their external website this Friday as part of the communications strategy for the RRM. We may wish to flag these to NSIA ahead of the site going live. We have not reviewed final communications products.

Thanks,



**From:** G7RRM@international.gc.ca  
**Sent:** Monday, August 12, 2019 4:59 PM  
**To:** G7RRM@international.gc.ca  
**Subject:** RRM Wire - August 2019

# RRM WIRE

August 2019

The RRM Wire strives to highlight original insight, shine light on new developments and projects, and draw attention to potential partners working in defence of democracy in support of the RRM's information and analysis-sharing mandate. If you become aware of information that you feel should be shared or have feedback, please send it along to the RRM Coordination Unit: [G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)

## Announcements

- On July 19, the US Director of National Intelligence (DNI) Daniel R. Coats [Established the Intelligence Community \(IC\) Election Threats Executive \(ETE\)](#). Shelby Pierson has been appointed as the ETE and will serve as the DNI's principal advisor on threats to elections and matters related to election security. The ETE will **coordinate and integrate all election security activities, initiatives, and programs across the IC and synchronize intelligence efforts in support of the broader U.S. government.**

## Key Reports and Developments

### Defending Democracy

- [Social Media Monitoring During Elections: Cases and Best Practice to Inform Electoral Observation Missions](#)  
The report **explores best practices in electoral observation missions**, by studying three main groups of actors: the main organizations that deploy international election observation missions; state actors in the EU that track disinformation; and non-state actors that look at disinformation in the EU, with a few examples from beyond the EU.
- [Americans could be a bigger fake news threat than Russians in the 2020 presidential campaign](#)  
This article discusses the role of domestic actors in disinformation operations. As argued by the author, Russia and Iran are not the only actors we need to worry about for 2020; **domestic actors are poised to be the bigger information threat.**
- [Combating disinformation and foreign interference in democracies: Lessons from Europe](#)  
This post is part of "[Cybersecurity and Election Interference](#)," a Brookings series that explores **digital threats to American democracy, cybersecurity risks in elections, and ways to mitigate possible problems.** This report explores how other countries, specifically Sweden, France, the United Kingdom and Hungary have addressed the challenges posed by foreign interferences.
- [Adversarial Narratives: A New Model for Disinformation](#)  
This paper is an attempt to **set out a theoretical model for understanding how the "digital influence machine" operates and how disinformation spreads.** It outlines a novel approach for understanding the current state of digital warfare – how adversarial and collective narratives are used for networked conflict.
- [The Journalists Who Exist Only on Paper](#)  
This report looks at how the New Eastern Outlook, and English-language website managed by the Russian Academy of Science's Institute for Oriental Studies, **uses authors with fake names to spread disinformation.**
- [Why crafty Internet trolls in the Philippines may be coming to a website near you](#)

This article explores how the world of Internet trolls is now a fact of life in the Web ecosystem nearly everywhere. As discussed in the article, experienced public relations experts in the Philippines are **using internet trolls to alter dramatically the political landscape.**

- [The Washington Post establishes a computational political journalism R&D lab to augment its campaign 2020 coverage](#)  
The Washington Post's newly launched elections engineering team **will establish a computational political journalism R&D lab in the newsroom this fall.** Under the leadership of Jeremy Bowers, the team will collaborate with Nick Diakopoulos, an assistant professor in communication studies and computer science at Northwestern University, to experiment with algorithmic and computational journalism tools to support The Post's political data efforts in advance of the 2020 election.
- [Digital Authoritarianism and The Threat to Global Democracy](#)  
Digital technologies empower the growing number of autocratic governments around the globe to surveil their citizens more comprehensively and for less cost than ever before. These technologies promise to concentrate power in the hands of a few, and, as they prove effective and efficient, set in motion a vicious cycle of deeper and more pervasive surveillance. In the process, **digital-abetted authoritarianism contributes to undermining global democracy.**
- [In the Age of Social Media, Expand the Reach of the First Amendment](#)  
In this article, David L. Hudson, Jr., argues that a society that cares for the protection of free expression needs to recognize that **the time has come to extend the reach of the First Amendment to cover powerful, private entities** – particularly social networking sites such as Facebook, Twitter, and others – that have ushered in a revolution in terms of communication capabilities.
- [Libyan Hashtag Campaign Has Broader Designs: Trolling Qatar](#)  
A network of more than 100 Twitter accounts exhibited inauthentic coordinated behavior by encouraging public support for Libyan General Khalifa Haftar and his self-styled Libyan National Army (LNA) while simultaneously criticizing Qatar and promoting the interests of the United Arab Emirates (UAE) — though its impact appears to have been modest. This is **the second article of a two-part series on a hashtag campaign supporting Libyan warlord Khalifa Haftar** during his campaign to take Tripoli. Part 1 can be found [here](#).
- [Facebook says it was 'not our role' to remove fake news during Australian election](#)  
In response to [the death tax misinformation](#) which circulated on Facebook during the Australian federal election, the platform has declared it is not “our role to remove content that one side of a political debate considers to be false.”
- [Facebook says it dismantles covert influence campaign tied to Saudi government](#)  
Facebook said it had suspended more than 350 accounts and pages with about 1.4 million followers, the latest takedown in an ongoing effort to combat “coordinated inauthentic behavior” on its platform, and **the first such activity it has linked to the Saudi government.** Details are available [here](#).
- [Facebook's fact-checking program falls short](#)  
In December of 2016, after receiving a firestorm of criticism about online disinformation during the presidential election, Facebook announced its Third Party Fact-Checking project. Independent organizations would debunk false news stories, and Facebook would make the findings obvious to users, down-ranking the relevant post in its News Feed. Now the project includes 50 partner organizations around the world, operating in 42 languages, **yet it's still very much an open question how effective the program is at stopping the spread of disinformation.**
- [Full Fact has been fact-checking Facebook posts for six months. Here's what they think needs to change](#)  
Full Fact, the independent U.K. fact-checking organization, signed on as one of Facebook's third-party fact-checking partners in January. Six months in, the organization [has released a report](#) about its experience so far — **what it's learned, what it likes, and what it thinks needs to change.**
- [Psychologists Should Speak Out Against the Abuse of Psychographic Data for Political Purposes](#)

In this article, Dr Emmy van Deurzen argues that the British Psychological Society and the American Psychological Association ought to develop **guidelines for the use of psychographic methods and personality profiling**, especially since these methods have been recently applied to political campaigning.

- [Is the Threat of 'Fake Science' Real?](#)

How could a country use disinformation to affect scientific research? At present, evidence does not suggest the existence of nation-state efforts to inject “fake science” into academic publishing. Although fake science could be used offensively like “fake news,” such an operation faces inherent constraints that limit its scope and effect. That being said, the **scientific community still bears significant vulnerabilities, making it a potentially attractive target for disinformation.**

## Russia

- [Report of the Select Committee on Intelligence, United States Senate, on Russian Measures Campaigns and Interference in the 2016 U.S. Election](#)

As reported [here](#), the Senate Intelligence Committee released a bipartisan report on Russian election interference that **found the U.S. election infrastructure was unprepared to combat “extensive activity” by Russia** that began in 2014 and carried on at least into 2017.

- [Russia-proofing your election: Global lessons for protecting Canadian democracy against foreign interference](#)

This report by the Macdonald-Laurier Institute Senior Fellow Marcus Kolga, Jakub Janda, and Nathalie Vogel **looks to the experiences of other Western states that have faced active threats from Russia**, including Sweden, the three Baltic states, France, and Germany. The report applies the insights from these case studies to outline tools that Canada can use to protect its elections and the democratic processes that underpin them.

- [Disinformation Space Oddity](#)

This article provides a **list of recent disinformation narratives circulated by pro-Russia disinformation outlets** targeting a wide range of issues, including the Moon landing, Ukraine, Ursula von der Leyen, and more.

- [Russian Journalist Punished for Telling Truth about MH17](#)

Pavel Kanygin is a Russian journalist who has been covering the downing of Malaysia Airlines flight MH17 for the independent newspaper Novaya Gazeta since the catastrophe happened five years ago. As explained in this article, the **Russian authorities decided to punish Pavel Kanygin using one of their most powerful weapons, namely a personal attack on prime-time state TV.**

- [Facing Pro-Democracy Wave, Kremlin Violently Suppresses Moscow Protests](#)

In the framework of the DFRLab’s “Four Ds” of Disinformation, RT **“distracted” its audience by turning attention away from the Russian protests and covering protests taking place elsewhere** in the world. This tactic likely aimed to minimize the significance of the Moscow protests.

- [The ABC of Kremlin Crisis Management](#)

In Russia’s current crisis around the upcoming local elections in Moscow, some of the dominating media outlets have conducted a disinformation campaign targeting those who demonstrate against the authorities. The strategy has been to present **the protesters as not local to Moscow; to downplay their numbers; and to accuse them of being part of a foreign conspiracy.**

- [Russian embassy in Syria's Twitter account suspended after posting White Helmets 'fake news'](#)

The Twitter account of the **Russian embassy in Syria has been suspended by the social media company** after it posted claims alleging that “White Helmet” civil defence rescuers were faking images of bombings. The embassy claimed that news of an air strike on a vegetable market in the Maarat al-Numan neighbourhood of rebel-held Idlib, which left at least 38 civilians dead and 100 wounded, was fabricated and that the market was still intact.

- [Lie, Manipulate, Spread, Change, Spread Again](#)

Penetration of the information space by pro-Kremlin actors goes far beyond using state-funded media or a troll factory. As shown in the [new report by Info Ops Polska](#), disinformation messages can be spread by multiple actors using a variety of tools – so that at the end of the day, **its recipients cannot see its original source or its fake ventilation.**

## China

- [Confucius Institute Chinese language and culture teachers must 'love the motherland' to apply](#)  
Australian students are being taught Chinese language and culture by **teaching assistants vetted by the Chinese Government for "good political quality" and a love of "the motherland."** The assistants teach Mandarin alongside Australian teachers in classrooms and universities across the country under the Confucius Institute program overseen by Chinese Government agency Hanban.
- [A Preliminary Survey of CCP Influence Operations in Singapore](#) and [A Preliminary Survey of CCP Influence Operations in Japan](#)  
In these two articles, Russell Hsiao presents an analysis of the means by which the **Chinese Communist Party seeks to gain influence over public discourse and government policy** in Singapore and Japan.
- [Hong Kong protests: 'I'm in Australia but I feel censored by Chinese students'](#)  
The **impact of the Hong Kong protest is being felt overseas**, particularly among the hundreds of thousands of mainland Chinese and Hong Kong students studying in Australia. At the University of Queensland, the tensions spilled over into violent clashes last week, when a group staging a support rally for the Hong Kong demonstrators were confronted by pro-Beijing protesters.

## Tech Bytes

- [Advanced Persistent Manipulators, Part Three: Social Media Kill Chain](#)  
This brief is part three of a three-part series. It **outlines the stages in a social media kill chain for analyzing and mitigating the efforts of Advanced Persistent Manipulators.**
- [Estimating the success of re-identifications in incomplete datasets using generative models](#)  
While rich medical, behavioral, and socio-demographic data are key to modern data-driven research, their collection and use raise legitimate privacy concerns. Anonymizing datasets through de-identification and sampling before sharing them has been the main tool used to address those concerns. **This study finds that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes.**
- [A Two-Track Algorithm To Detect Deepfake Images](#)  
Researchers have demonstrated **a new algorithm for detecting so-called deepfake images**—those altered imperceptibly by AI systems, potentially for nefarious purposes. Initial tests of the algorithm picked out phony from undoctored images down to the individual pixel level with between 71 and 95 percent accuracy, depending on the sample data set used. The algorithm has not yet been expanded to include the detection of deepfake videos.

## Disclaimer

The ideas and opinions expressed in these reports belong to the authors and do not necessarily reflect the views and opinions of the Government of Canada. By sharing these reports, RRM Coordination Unit does not endorse or validate their content.

RRM Coordination Unit collects and shares information consistent with Canada's privacy laws and the Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities. The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

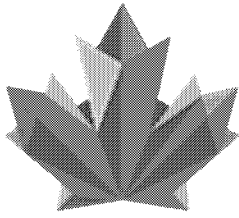
G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique internationale  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

Canada



TOGETHER · ENSEMBLE  
**CANADA**  
UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU  
2021-2022

---

### Bcc List

\*IOC <D-IOC@international.gc.ca>; \*IOD <D-IOD@international.gc.ca>; \*IOL <D-IOL@international.gc.ca>; \*IOP <D-IOP@international.gc.ca>; \*IOR <D-IOR@international.gc.ca>; \*USS-DMA Advisors <D-USS-DMAAdvisors@international.gc.ca>; \*MINA-Dept Unit <D-MINA-Dept-Unit@international.gc.ca>; Friele, Shawn -IFM <Shawn.Friele@international.gc.ca>; Whiting, Shelley -IOD <Shelley.Whiting@international.gc.ca>; Lévêque, Alexandre -POD <Alexandre.Leveque@international.gc.ca>; Thompson, Graeme -POL <Graeme.Thompson@international.gc.ca>; Higginbotham, Ian -POL <Ian.Higginbotham@international.gc.ca>; Dondey, Laurent -POG <Laurent.Dondey@international.gc.ca>; Bonser, Michael -POG <Michael.Bonser@international.gc.ca>; Jansen, Ralph -PRD <Ralph.Jansen@international.gc.ca>; Mills, Amy -LCBR; Lindblad, Anabel -LCB <Anabel.Lindblad@international.gc.ca>; Brisebois, Charles -LDS <Charles.Brisebois@international.gc.ca>; Mojsej, Charles -LCD <Charles.Mojsej@international.gc.ca>; Galligan, Gregory -LCF <Gregory.Galligan@international.gc.ca>; Dunev, Jennifer -LCFA <Jennifer.Dunev@international.gc.ca>; Cranfield, Leilla -LDN <Leilla.Cranfield@international.gc.ca>; Paterson, Robert -LCM <Robert.Paterson@international.gc.ca>; Stéphane.levesque@international.gc.ca; May, Adria -OPB <Adria.May@international.gc.ca>; Lee, Albert -OPC <Albert.Lee@international.gc.ca>; Puxley, Evelyn -OPX <Evelyn.Puxley@international.gc.ca>; Bergeron, Jean-François -OPB <Jean-Francois.Bergeron@international.gc.ca>; Payne, Nichola -OPB <Nichola.Payne@international.gc.ca>; Lu, Tim -OPB <tim.lu@international.gc.ca>; David, Arthur -IOC <Arthur.David@international.gc.ca>; Shapardanov, Chris -IDS <Chris.Shapardanov@international.gc.ca>; Nelson, David -IGR <David.Nelson@international.gc.ca>; Norman, Giles -IGR <Giles.Norman@international.gc.ca>; Therrien, Anne -EUA <Anne.Therrien@international.gc.ca>; Flanagan Whalen, Ann -EUA <Ann.FlanaganWhalen@international.gc.ca>; Grant, Alison -ECE <Alison.Grant@international.gc.ca>; LeClaire, Alison -ECD <Alison.LeClaire@international.gc.ca>; Roma, Giovanna -EUA <Giovanna.Roma@international.gc.ca>; Beloin, Valérie -ECE <Valerie.Beloin@international.gc.ca>; Fry, Robert -EUD <Robert.Fry@international.gc.ca>; Colvin, Richard -EUA <Richard.Colvin@international.gc.ca>; Nouvet, Antoine -IGR <Antoine.Nouvet@international.gc.ca>; BREU (CBSA-ASFC) <BREUCBSA-ASFC@international.gc.ca>; Ebel, Brian -BGRAD -GR <Brian.Ebel@international.gc.ca>; Gibbins, Christopher -WSHDC -GR <Christopher.Gibbins@international.gc.ca>; Senay, Claudie -LDN -GR <Claudie.Senay@international.gc.ca>; Laporte, Eric -BNATO -GR <Eric.Laporte@international.gc.ca>; Gartshore, Geoff -BRLIN -GR <Geoff.Gartshore@international.gc.ca>; Reckseidler, Jarrett -BREU -GR <Jarrett.Reckseidler@international.gc.ca>; Tolland, Jason -HSNKI -HOM/CDM <Jason.Tolland@international.gc.ca>; Blitt, Jessica -BREU -GR <Jessica.Blitt@international.gc.ca>; Reeves, Jordan -TAPEI -HOM/CDM <Jordan.Reeves@international.gc.ca>; Tunney, Kevin -WSHDC -GR <Kevin.Tunney@international.gc.ca>; Sarty, Leigh -DSIR <Leigh.Sarty@international.gc.ca>; Vidal, Maeva -BNATO -GR <Maeva.Vidal@international.gc.ca>; Laflamme, Martin -BEJING -PA <Martin.Laflamme@international.gc.ca>; Loken, Martin -WSHDC -GR <Martin.Loken@international.gc.ca>; Delisle, Richard -BNATO -GR <Richard.Delisle@international.gc.ca>; Dobner, Gallit -HAGUE -GR; Gagnon, Thomas -HAGUE -GR <Thomas.Gagnon@international.gc.ca>; Gillis, Sarah -HAGUE -GR <Sarah.Gillis@international.gc.ca>; Waschuk, Roman -KYIV -HOM/CDM <Roman.Waschuk@international.gc.ca>; Nguyen, Huy -TAPEI <Huy.Nguyen@international.gc.ca>; McEvoy, Vance -BEJING -GR <Vance.McEvoy@international.gc.ca>; Nolke, Sabine -HAGUE HOM/CDM <Sabine.Nolke@international.gc.ca>; Wallbaum, Alistair -WSHDC -GR <Alistair.Wallbaum@international.gc.ca>; Ambler, Kristen -BERN -GR <Kristen.Ambler@international.gc.ca>; Landry, Tristan -PARIS -GR <Tristan.Landry@international.gc.ca>; Alex.Jasperse@tbs-sct.gc.ca; Bianca.Healy@tbs-sct.gc.ca; Bronwyn.Cline@tbs-sct.gc.ca; Dana.Robinson@tbs-sct.gc.ca; Doug.McCallum@tbs-sct.gc.ca; Helene.Potvin@tbs-sct.gc.ca; jonathan.Macdonald@tbs-sct.gc.ca; kirsten.duke@tbs-

s.15(1)

s.24(1)

sct.gc.ca; Lesley.Kiely@tbs-sct.gc.ca; Lucas.Beal@tbs-sct.gc.ca; Mark.Stokes@tbs-sct.gc.ca; Michael.Murphy2@tbs-sct.gc.ca; Nathalie.Dussault@tbs-sct.gc.ca; Sean.Sutton@tbs-sct.gc.ca; Scott.MacIntosh@tbs-sct.gc.ca; Véronique.Gauvreau@tbs-sct.gc.ca; William.McMahon@tbs-sct.gc.ca; Anna.Cichosz@pco-bcp.gc.ca; Christos.Sarakinos@pco-bcp.gc.ca; Cloe.Prieur@pco-bcp.gc.ca; Colum.Grove-White@pco-bcp.gc.ca; David.Ott@pco-bcp.gc.ca; Guylaine.hamel@pco-bcp.gc.ca; Jean.Tessier@pco-bcp.gc.ca; Jessica.Kingsbury@pco-bcp.gc.ca; Kate.Binnie@pco-bcp.gc.ca; Michael.Waters@pco-bcp.gc.ca; Philippe-Andre.Rodriguez@pco-bcp.gc.ca; Raymond.Rivet@pco-bcp.gc.ca; Rob.Ammerman@pco-bcp.gc.ca; Sandra.Boudreau@pco-bcp.gc.ca; Alain.beaudoin@pco-bcp.gc.ca; Valerie.Samaan@pco-bcp.gc.ca;

Lorna.Bonvie@pco-bcp.gc.ca; Tracy.Dool@pco-bcp.gc.ca;

David.Ennis-

Dawson@canada.ca; Dennis.Giguere@canada.ca; Gillian.Badger@canada.ca; julie.grenier@canada.ca; Jamie.tomlinson@canada.ca; Leanne.maidment@canada.ca; lynn.fournier2@canada.ca; mike.ashman@canada.ca; stephanie.sprott@canada.ca; nicholas.kaminsky@canada.ca; jason.martin@canada.ca; ryan.murphy2@canada.ca; Gabriel.TremblayGiroux@canada.ca; Janice.Keenan@forces.gc.ca; MARK.FARFANDELOSGODOS@forces.gc.ca; Alex.Stanford@forces.gc.ca; Myriam.Bower@forces.gc.ca; Ryan.Ferrara@forces.gc.ca; LISA.ALLAIRE@forces.gc.ca; CHRIS.HENDERSON2@forces.gc.ca; Doug.Keirstead@forces.gc.ca; JOE.DEMORA@forces.gc.ca; ELIZABETH.MCKELVEY@forces.gc.ca; DANIEL.LEBOUTHILLIER@forces.gc.ca; TAMARA.MURPHY@forces.gc.ca; KIRSTEN.GOODNOUGH@forces.gc.ca; RICHARD.PERREAULT@forces.gc.ca; DOUGLAS.ALLISON@forces.gc.ca; DESMOND.JAMES@forces.gc.ca; jay.janzen@forces.gc.ca; Stephanie.Kennedy@forces.gc.ca; DAVID.ENNS4@forces.gc.ca; JOHN.ROACH2@forces.gc.ca; SHANNON.ALFORD@forces.gc.ca; YVETTE.GRYGORYEV@forces.gc.ca; Amelia.brown@elections.ca; anne.lawson@elections.ca; Daniel.fischer@elections.ca; Darrell.Kekanovich@elections.ca; jane.dunlop@elections.ca; Melanie.Wise@elections.ca; Rahul.badami@elections.ca; serge.caron@elections.ca; bruno.bosse@elections.ca; reference@elections.ca; internationalaffairs@elections.ca; Isabelle.Duguay@elections.ca; Genevieve.Bourgeois@elections.ca; susan.torosian@elections.ca; Jacinthe.Dumont@cef-cce.ca; Mylene.Gigou@cef-cce.ca; Jane.Leeke@cef-cce.ca; Josee.LebLANC@cef-cce.ca; Al.Mathews@cef-cce.ca; Amanda.Bellefeuille@rcmp-grc.gc.ca; Bill.Ricketts@rcmp-grc.gc.ca; Christopher.Johnson@rcmp-grc.gc.ca; Rampersad, Dave -RCMP/GRC <dave.rampersad@rcmp-grc.gc.ca>; Deanne.Morgan@rcmp-grc.gc.ca; Holly.Richter@rcmp-grc.gc.ca; Maria.Gurina@rcmp-grc.gc.ca; Kirk.Chiasson@rcmp-grc.gc.ca; Steve.Strang@rcmp-grc.gc.ca;

Gordon, Eric -RCMP/GRC <eric.gordon@rcmp-grc.gc.ca>;

cameron.ortis@rcmp-grc.gc.ca; boudriasc@smtp.gc.ca;

caitlin.cowan@canada.ca; danielbezalel.richardsen@canada.ca;

Jack.Branswell@cic.gc.ca; james.lewis@canada.ca; josee.sirois3@canada.ca; katherine.snow@canada.ca; Kirstan.Gagnon@justice.gc.ca; Lisa.Scarizzi@cic.gc.ca; marie-eve.lamoureux@canada.ca; michael.himsl@canada.ca; paul.piasko@canada.ca; ps.goc-cog.sp@canada.ca; raymond.snow2@canada.ca; Ritu.Gill@drdc-rddc.gc.ca; ryan.baker3@canada.ca; samson.kan@canada.ca; taylor.bildstein@canada.ca; Tony.Seaboyer@rmc-cmr.ca; Toban.Morrison@justice.gc.ca; ShirleyAnne.Off@justice.gc.ca; Julien.houle@canada.ca; laura.peckett@canada.ca

## Awali, Elabe

---

**From:** G7RRM@international.gc.ca  
**Sent:** Tuesday, June 4, 2019 12:07 PM  
**To:** G7RRM@international.gc.ca  
**Subject:** RRM Canada: Final Ukrainian Elections Report  
**Attachments:** RRM Canada Ukraine Elections Final Report.pdf

Dear colleagues,

This email is to circulate the final Ukrainian Elections Report prepared by Rapid Response Mechanism (RRM) Canada, which summarizes key trends/tactics observed in the Ukrainian election. The attached report is based on open-source primary and secondary information related to the Ukrainian Elections, with a focus on understanding potential threats posed by foreign actors in the election process. Its objective is to identify lessons learned and new trends in foreign interference and share these findings widely to ensure that they are integrated into national initiatives.

Regards,

G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique internationale  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

Canada



TOGETHER • ENSEMBLE  
**CANADA**  
UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU  
2021-2022

---

### Bcc List

\*IOC; \*IOD; \*IOL; \*IOP; \*IOR; \*USS-DMA Advisors; \*MINA-Dept Unit; Shawn.Friele@international.gc.ca; Shelley.Whiting@international.gc.ca; Alexandre.Leveque@international.gc.ca; Graeme.Thompson@international.gc.ca; Ian.Higginbotham@international.gc.ca; Laurent.Dondey@international.gc.ca; Michael.Bonser@international.gc.ca; Ralph.Jansen@international.gc.ca; Amy.Mills@international.gc.ca; Anabel.Lindblad@international.gc.ca; Charles.Brisebois@international.gc.ca; Charles.Mojsej@international.gc.ca; Gregory.Galligan@international.gc.ca; Jennifer.Dunev@international.gc.ca; Leilla.Cranfield@international.gc.ca; Robert.Paterson@international.gc.ca; Stéphane.levesque@international.gc.ca; Adria.May@international.gc.ca; Albert.Lee@international.gc.ca; Evelyn.Puxley@international.gc.ca; Jean-Francois.Bergeron@international.gc.ca; Nichola.Payne@international.gc.ca; tim.lu@international.gc.ca; Arthur.David@international.gc.ca; Chris.Shapardanov@international.gc.ca; David.Nelson@international.gc.ca; Giles.Norman@international.gc.ca; Anne.Therrien@international.gc.ca; Ann.FlanaganWhalen@international.gc.ca; Alison.Grant@international.gc.ca; Alison.LeClaire@international.gc.ca; Giovanna.Roma@international.gc.ca; Valerie.Beloin@international.gc.ca; Robert.Fry@international.gc.ca; Richard.Colvin@international.gc.ca; Antoine.Nouvet@international.gc.ca; BREUCBSA-ASFC@international.gc.ca;

Brian.Ebel@international.gc.ca; Christopher.Gibbins@international.gc.ca; Claudie.Senay@international.gc.ca; Eric.Laporte@international.gc.ca; Geoff.Gartshore@international.gc.ca; Jarrett.Reckseidler@international.gc.ca; Jason.Tolland@international.gc.ca; Jessica.Blitt@international.gc.ca; Jordan.Reeves@international.gc.ca; Kevin.Tunney@international.gc.ca; Leigh.Sarty@international.gc.ca; Maeva.Vidal@international.gc.ca; Martin.Laflamme@international.gc.ca; Martin.Loken@international.gc.ca; Richard.Delisle@international.gc.ca; Gallit.Dobner@international.gc.ca; Thomas.Gagnon@international.gc.ca; Sarah.Gillis@international.gc.ca; Roman.Waschuk@international.gc.ca; Huy.Nguyen@international.gc.ca; Vance.McEvoy@international.gc.ca; Sabine.Nolke@international.gc.ca; Alistair.Wallbaum@international.gc.ca; Tristan.Landry@international.gc.ca; Alex.Jasperse@tbs-sct.gc.ca; Bianca.Healy@tbs-sct.gc.ca; Bronwyn.Cline@tbs-sct.gc.ca; Dana.Robinson@tbs-sct.gc.ca; Doug.McCallum@tbs-sct.gc.ca; Helene.Potvin@tbs-sct.gc.ca; jonathan.Macdonald@tbs-sct.gc.ca; kirsten.duke@tbs-sct.gc.ca; Lesley.Kiely@tbs-sct.gc.ca; Lucas.Beal@tbs-sct.gc.ca; Mark.Stokes@tbs-sct.gc.ca; Michael.Murphy2@tbs-sct.gc.ca; Nathalie.Dussault@tbs-sct.gc.ca; Sean.Sutton@tbs-sct.gc.ca; Scott.MacIntosh@tbs-sct.gc.ca; Véronique.Gauvreau@tbs-sct.gc.ca; William.McMahon@tbs-sct.gc.ca; Anna.Cichosz@pco-bcp.gc.ca; Christos.Sarakinos@pco-bcp.gc.ca; Cloe.Prieur@pco-bcp.gc.ca; Colum.Grove-White@pco-bcp.gc.ca; David.Ott@pco-bcp.gc.ca; Guylaine.hamel@pco-bcp.gc.ca; Jean.Tessier@pco-bcp.gc.ca; Jessica.Kingsbury@pco-bcp.gc.ca; Kate.Binnie@pco-bcp.gc.ca; Michael.Waters@pco-bcp.gc.ca; Philippe-Andre.Rodriguez@pco-bcp.gc.ca; Raymond.Rivet@pco-bcp.gc.ca; Rob.Ammerman@pco-bcp.gc.ca; Sandra.Boudreau@pco-bcp.gc.ca; Valerie.Samaan@pco-bcp.gc.ca; Tracy.Dool@pco-bcp.gc.ca;

David.Ennis-

Dawson@canada.ca; Dennis.Giguere@canada.ca; Gillian.Badger@canada.ca; julie.grenier@canada.ca; Jamie.tomlinson@canada.ca; Leanne.maidment@canada.ca; lynn.fournier2@canada.ca; mike.ashman@canada.ca; stephanie.sprott@canada.ca;

Gabriel.TremblayGiroux@canada.ca; Janice.Keenan@forces.gc.ca; MARK.FARFANDELOSGODOS@forces.gc.ca; RICHARD.PERREAU@forces.gc.ca; DOUGLAS.ALLISON@forces.gc.ca; DESMOND.JAMES@forces.gc.ca; jay.janzen@forces.gc.ca; Stephanie.Kennedy@forces.gc.ca; SHANNON.ALFORD@forces.gc.ca; YVETTE.GRYGORYEV@forces.gc.ca; Amelia.brown@elections.ca; anne.lawson@elections.ca; Daniel.fischer@elections.ca; Darrell.Kekanovich@elections.ca; jane.dunlop@elections.ca; Melanie.Wise@elections.ca; Rahul.badami@elections.ca; serge.caron@elections.ca; bruno.bosse@elections.ca; reference@elections.ca; internationalaffairs@elections.ca; susan.torosian@elections.ca; Jacinthe.Dumont@cef-cce.ca; Mylene.Gigou@cef-cce.ca; Jane.Leeke@cef-cce.ca; Josee.Lebanc@cef-cce.ca; Amanda.Bellefeuille@rcmp-grc.gc.ca; Bill.Ricketts@rcmp-grc.gc.ca; Christopher.Johnson@rcmp-grc.gc.ca; Dave.Rampersad@rcmp-grc.gc.ca; Deanne.Morgan@rcmp-grc.gc.ca; Holly.Richter@rcmp-grc.gc.ca; Maria.Gurina@rcmp-grc.gc.ca; Kirk.Chiasson@rcmp-grc.gc.ca; Steve.Strang@rcmp-grc.gc.ca;

eric.gordon@rcmp-grc.gc.ca; cameron.ortis@rcmp-grc.gc.ca;

caitlin.cowan@canada.ca; danielbezalel.richardsen@canada.ca; Jack.Branswell@cic.gc.ca; james.lewis@canada.ca; josee.sirois3@canada.ca; katherine.snow@canada.ca; Kirstan.Gagnon@justice.gc.ca; Lisa.Scarizzi@cic.gc.ca; marie-eve.lamoureux@canada.ca; michael.himsl@canada.ca; paul.piasko@canada.ca; ps.goc-cog.sp@canada.ca; raymond.snow2@canada.ca; Ritu.Gill@drdc-rddc.gc.ca; ryan.baker3@canada.ca; samson.kan@canada.ca; taylor.bildstein@canada.ca; Tony.Seaboyer@rmc-cmr.ca; Toban.Morrison@justice.gc.ca; ShirleyAnne.Off@justice.gc.ca



## 2019 UKRAINIAN ELECTIONS FINAL REPORT

### Purpose

[1] This open source report is the final report in a series prepared by Rapid Response Mechanism (RRM) Canada on Foreign Interference (FI) during the 2019 Ukrainian presidential elections. The aim of the series was to enhance the global understanding of contemporary threats to democratic systems of governance while informing Canadian efforts aimed at safeguarding Canada's elections from FI. This report is a summary of key findings from the series of reports that was produced with the objective of identifying key lessons learned from the Ukrainian presidential elections. The reports were based on secondary sources, including insight from the RRM network and the community of experts, as well as primary research conducted by RRM Canada leveraging its open data monitoring and analytical capacity.

### Overall Assessment

[2] Based on evidence summarized below and previous RRM reports, the Ukrainian presidential election was likely the target of a Russian FI campaign aimed at undermining local and international confidence in the Ukrainian democracy. Initial assessments by multiple observation teams conclude that this FI campaign did not achieve its aim.<sup>1</sup> Key findings include:

- Russian speakers were a priority audience for accounts employing automation.
- With the exception of the days following major incidents such as the July 2014 downing of Malaysian Air flight MH-17, covert social media influence campaigns appear most active during election periods in Ukraine as well as the days immediately following.
- Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.
- "Meta-trolling" or content designed to be detected and called out as Russian propaganda in order to discredit the information it contains may be a newly emerging tactic which RRM Canada will continue to monitor.

### General Observations – Secondary and Primary Sources

#### Tactics/Strategies

[3] Reporting from

s.15(1) notes a high degree of automation observed in social media posts about Ukraine's elections. RRM Canada observed similar automated accounts or bots. In addition to the use of bots, RRM Canada observed that many accounts used a random string of alphanumeric characters as a username. These accounts were mostly created after January 2019 and were posting in the Russian language about the Ukrainian elections. The usernames and young age of these accounts indicates that a computer program was likely used to quickly generate new accounts for use in bot networks. Additionally, RRM Canada notes that the highest degree in automation was observed within communities discussing the Ukrainian elections in the Russian language indicating that Russian speakers were likely a priority target audience.

[4] Historical Twitter based analysis has shown that accounts associated with the Kremlin have been most active following the May 2014 elections. However, tweet volume was much smaller in comparison to the July 2014 downing of Malaysian flight MH-17.<sup>2</sup> While RRM Canada does not have a database of accounts associated with the Kremlin, within our collection of accounts discussing the 2019 elections,

---

<sup>1</sup> Previous reporting

<sup>2</sup> <https://voxukraine.org/longreads/twitter-database/index-en.html>

our team observed a large spike in account creation dates from 2014. Further analysis of account creation dates reveals another spike in January 2019. This spike was most pronounced among accounts posting in the Russian language. This indicates that although far below the level of resources dedicated to deflecting blame away from Russia for the downing of MH-17, covert social media influence campaigns are probably most active during election periods in Ukraine. Our data also indicates a spike in posting activity in the days immediately following the elections however, examination of the posts did not reveal any specific narrative being amplified.

[5] Two tactics which have to date been less frequently reported, were observed much more prominently during the Ukraine elections. These tactics were the purchase or renting of social media accounts and the use of “meta-trolling.”

[6] New York Times and the Ukrainian Security Service (SBU) report that Russian intelligence agents had been offering to purchase or rent established social media accounts from Ukrainian citizens for the purposes of spreading divisive content or furthering other Kremlin narratives. Owners of these social media accounts reported that they were unaware they were dealing with Russian intelligence personnel or what purpose their accounts would ultimately serve once sold or rented. The number of accounts purchased by Russian agents remains unknown at this time and description of this tactic stems from a video-taped confession released by the SBU.<sup>3</sup> Given the financial and human resources required to find and purchase established social media accounts from citizens willing to sell them, it is unlikely this tactic was widespread during this election and unknown if it will be employed in other FI campaigns.

[7] Finally, Government of Canada (GoC) partners deployed to Ukraine to assist with cyber security during the elections period reported a new meta-trolling technique. In this technique, certain content was designed to be detected as Russian propaganda and publicly called out as such in an effort to discredit the information it contained. While we cannot attribute the employment of this tactic to Russia, it falls within the well-known concept of “reflexive control.” This concept, whereby specifically prepared information is conveyed in order to incline an opponent to voluntarily take a certain course of action, has a long history within Soviet and Russian military doctrine.<sup>4</sup> RRM Canada has no further information or current examples of this technique and we cannot attribute it to any particular actor at this time.

[8] RRM Canada cannot tie the employment of automated accounts or the spread of divisive content to Russia. However, Facebook did shut down thousands of accounts posting about Ukraine which they attributed to Kremlin-linked Internet Research Agency (IRA) and Sputnik News.<sup>5</sup> Based primarily on this evidence, RRM Canada assesses that the Russian state was likely conducting a disinformation campaign targeting the Ukrainian elections.

### **Narratives**

[9] In addition to observations of automation, reports from the UK Foreign & Commonwealth Office’s (FCO) Counter Disinformation Cell note divisive narratives being spread by these automated accounts. AoD notes that much of this content ostensibly<sup>6</sup> emanated from Russia and, at least for a period in late

---

<sup>3</sup> Previous reporting

<sup>4</sup> <http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/>

<sup>5</sup> Previous reporting

<sup>6</sup> Alliance for Securing Democracies methodology relies on user selection of location within preference settings.

March,<sup>7</sup> dominated approximately 13% of the conversation on social media about the Ukrainian elections. Previous RRM Canada reports have noted that divisive content was primarily along the following themes:

- Ukraine was reverting to its Nazi past while chauvinism and xenophobia were current state policy;
- Ukraine was becoming increasingly corrupt and becoming a banana republic.
- Ukraine was not capable of hosting free and fair elections; and
- The illegitimacy of the Ukrainian Orthodox Church was put forward.

[10] While the break of the Ukrainian Orthodox Church from the Moscow patriarch is uniquely Ukrainian, claims of corruption, elections fraud, and otherwise divisive content are common tropes within FI campaigns.<sup>8</sup> Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.<sup>9</sup> The Atlantic Council's Digital Forensics Research Lab notes these tactics appear to be common across both foreign and domestic disinformation campaigns targeting elections.<sup>10</sup>

### **On Gender**

[11] On the gender dimensions of FI within the Ukrainian elections, RRM Canada observed crudely Photo-shopped, degrading, highly sexualized imagery targeting the most prominent female candidate, Yulia Tymoshenko. RRM Canada cannot attribute any of these images to any specific actor. We note that this imagery dominated our collection of all images related to political candidates for a period in February indicating the possibility of some level of coordinated amplification; however, there are many plausible explanations related to this imagery.

### **On Diasporas**

[12] Lastly, RRM Canada detected and analyzed two multilingual groups discussing the Ukrainian elections in the Ukrainian, Russian and English languages on Twitter. Within these groups, relatively few indications of automated content spreading or accounts assessed to be possible Kremlin trolls were observed. Based on the mix of languages, RRM Canada assesses these communities to likely be Ukrainian diaspora communities from English speaking countries. Based on the lack of automated content spreading within these communities, RRM Canada assesses they were likely not priority target audiences for disinformation campaigns.<sup>11</sup>

Released: 4 June 2019

**Disclaimer:** Rapid Response Mechanism Canada team monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

---

<sup>7</sup> Other reports from the Alliance of Democracies did not mention the amount of content possibly emanating from Russia.

<sup>8</sup> As noted within research conducted by the Atlantic Council's Digital Forensics Research Lab.

<sup>9</sup> Previous reporting

<sup>10</sup> As presented by DFR Lab.

<sup>11</sup> Previous reporting

**From:** G7RRM@international.gc.ca  
**Sent:** Thursday, July 18, 2019 11:54 AM  
**To:** G7RRM@international.gc.ca  
**Subject:** RRM Wire - July 2019

## RRM WIRE

July 2019

The RRM Wire strives to highlight original insight, shine light on new developments and projects, and draw attention to potential partners working in defence of democracy in support of the RRM's information and analysis-sharing mandate. If you become aware of information that you feel should be shared or have feedback, please send it along to the RRM Coordination Unit: [G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)

### RRM in Focus

The following reports draw attention to the work of the G7 Rapid Response Mechanism in addressing threats to democracy:

- [Election Risk Monitor: Canada](#)  
After reviewing a range of threats and Canada's new laws, policies and investments designed to anticipate and respond to them, **this report documents strategies that the Canadian government has adopted at home, as well as its contributions to international efforts.** The report outlines the policy choices that lie ahead for Canada regarding the exploitation of social media platforms by malicious actors who have an interest in influencing Canadian elections.
- [Democratic Defense Against Disinformation 2.0](#)  
This second edition of the paper, Democratic Defense Against Disinformation, seeks to capture the rapid development of policy responses to the challenge—especially by governments and social media companies—since initial publication in February 2018. The Atlantic Council stands by the fundamentals of the earlier analysis and recommendations: that democratic societies can **combat and mitigate the challenge of foreign disinformation while working within democratic norms and respect for freedom of expression.**

### Original Insight

- [The "Macron Leaks" Operation: A Post-Mortem](#)  
This report is the result of a joint effort between the Atlantic Council's Digital Forensic Research Lab, Eurasia Center, and Future Europe Initiative, and the Institute for Strategic Research (IRSEM) at the French Ministry of the Armed Forces, as a part of joint efforts to combat disinformation. Among the long list of electoral interference attempts in recent years, **one case is especially important to study: the 2017 French presidential election, because it failed.**
- [Reuters Institute Digital News Report](#)  
This year's report comes against the backdrop of rising populism, political and economic instability, along with intensifying concerns about giant tech companies and their impact on society.
- [The Oxford Handbook of Electoral Persuasion](#)  
This handbook contains a number of articles related to persuasion, campaigns and elections, and media usage.

### Key Reports and Developments

#### Defending Democracy

- [Canada's October elections and the risks of CCP interference: J. Michael Cole for Inside Policy](#)  
Following Russia's meddling in the 2016 US elections and growing evidence of interference by authoritarian regimes in other democracies, it is now feared that Canada's federal elections in October could become the latest target in a mounting challenge to democratic processes worldwide. Cole argues that **while attention has rightly focused on Russia, Ottawa also needs to contend with the possibility of interference by Beijing.**
- [Parution de l'ouvrage « Stratégies d'influence et guerres de l'information »](#)  
Quel rôle les États-Unis ont-ils joué dans les guerres de l'information depuis la guerre froide? Quelles stratégies d'influence ont-ils mises en oeuvre pour favoriser leurs objectifs de politique étrangère? **Cet ouvrage apporte un éclairage inédit sur le rôle de la diplomatie publique au sein de la fabrique de la politique étrangère américaine.** Outre la description de son fonctionnement institutionnel à Washington, il propose une analyse de l'évolution des stratégies mises en oeuvre dans les « zones critiques » à l'Ouest et à l'Est dans l'Europe de la guerre froide.
- [Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Elections and Beyond](#)  
The report begins by summarizing the Kremlin's interference activities in the 2016 U.S. elections. Chapters two through eight then **offer concrete prescriptions for protecting the integrity and independence of U.S. elections,** focusing in particular on strengthening resiliency before the 2020 presidential election.
- [How people want to feel determines whether others can influence their emotions, Stanford psychologists find](#)  
In a new study, Stanford psychologists examined why some people respond differently to an upsetting situation and learned that people's motivations play an important role in how they react. Their study found that **when a person wanted to stay calm, they remained relatively unfazed by angry people, but if they wanted to feel angry, then they were highly influenced by angry people.**
- [How information is like snacks, money, and drugs—to your brain](#)  
Can't stop checking your phone, even when you're not expecting any important messages? Blame your brain. A new study by researchers at UC Berkeley's Haas School of Business has found that **information acts on the brain's dopamine-producing reward system in the same way as money or food.**
- [2019 EU Elections Information Operations Analysis: Interim Briefing Paper](#)  
This paper **addresses the groups and parties behind the malign influence operations active in the 2019 EU elections** and analyses the techniques they use. It also assesses the record of the tech companies in addressing these threats to electoral integrity.
- [How Fake News Could Lead to Real War](#)  
The current fake news epidemic isn't just shaking up U.S. politics, it might end up causing a war, or just as consequentially, impeding a national response to a genuine threat. **Misinformation in geopolitics could lead not only to the continued weakening of our institutions but also to combat deaths.**
- [How Artificial Intelligence Can Detect – And Create – Fake News](#)  
Despite some basic potential flaws, **AI can be a useful tool for spotting online propaganda – but it can also be startlingly good at creating misleading material.** Researchers already know that online fake news spreads much more quickly and more widely than real news. In an online world where viewers have limited attention and are saturated with content choices, it often appears as though fake information is more appealing or engaging to viewers.
- [Fake antifa Twitter accounts spread disinformation on Fourth of July](#)  
An ongoing disinformation campaign aimed at antifa — shorthand for antifascist or antifascism — took a new turn as **freshly created fake Twitter accounts spread false and inflammatory information** about antifa's plans for the Fourth of July.
- [FBI warns of foreign actors trying to 'sow discord' in the wake of mass shootings](#)  
Houses of worship remain a vulnerable target for attacks and **foreign entities could be looking to "sow discord" using the internet,** an FBI official warned at a security event with law enforcement officials and faith leaders this week.
- [NATO-Skeptic Online Personas Target Fringe Media Sites](#)

A small group of personas — accounts with unverified operators — from Latvia and Lithuania amplified anti-NATO and anti-establishment opinions about the Baltic states on fringe English-language media outlets beginning in August 2018. While the subset of accounts was small and achieved little engagement overall, **the operation nonetheless demonstrated a multi-platform approach to online content amplification.**

- [A Change of Tactics: Blurring Disinformation's Source](#)  
If a domestic source spreads a typical lie originating in the Kremlin-controlled media ecosystem about MH17 being shot down by Ukraine, the United States being an occupying power in Europe, or the EU promoting sexual perversion, **does that message suddenly stop being the Kremlin's disinformation?**
- [The Gulf Information War | Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis](#)  
To address the **dual need to examine the weaponization of social media and the nature of non-Western propaganda**, this article explores the use of Twitter bots in the Gulf crisis that began in 2017.
- [Alphabet-Owned Jigsaw Bought a Russian Troll Campaign as an Experiment](#)  
A targeted troll campaign today can cost very little—as little as **\$250, says Andrew Gully, a research manager at Alphabet subsidiary Jigsaw**. He knows because that's the price Jigsaw paid for one last year.
- [Twitter removes thousands of accounts linked to Iran government](#)  
Twitter has removed nearly **4,800 accounts with ties to the Iranian government** in a continuing effort to prevent election interference and misinformation on the platform.

## Russia

- [Reverse engineering Russian Internet Research Agency tactics through network analysis.](#)  
In mid-October of 2018, Twitter released a dataset containing both the contents and information for accounts on their platform related to the Internet Research Agency. These accounts were used to influence the 2016 US Presidential election, as well as elections and referenda in several other countries, including the UK and Venezuela. This article documents a data analysis of these tweets, and through data visualisation **demonstrates a rigorous methodology of practice at work in Russia's online interference in foreign democracies**, particularly through St. Petersburg's Internet Research Agency (IRA).
- [Figure of the Week: 111,486](#)  
Analysis by De Groene Amsterdammer shows that in three days, the Internet Research Agency produced as many as 111,486 tweets. Out of this number, at least 65,000 tweets were blaming Ukraine for downing of the MH17 plane. **The MH17 crash was the time of the biggest activity of Russian trolls ever.**
- [Top Takes: Suspected Russian Intelligence Operation](#)  
On May 6, 2019, Facebook announced that it had taken down “16 accounts, four pages, and one Instagram account as part of a small network emanating from Russia.” Facebook shared the names (expressed as unique user ID numbers) of the accounts it assessed as involved in coordinated inauthentic behavior shortly before the takedown. Working outwards from those accounts, the **DFR Lab identified a much larger operation that ran across many platforms, languages and subjects** but consistently used the same approach and concealment techniques. The full report, titled “**Operation Secondary Infektion**,” is available [here](#).
- [Study suggests Russian social media trolls had impact on 2016 election](#)  
A new study **found a correlation between retweets of known Russian troll accounts during the 2016 election and Donald Trump's poll numbers**. The study, conducted by a team headed at the University of Tennessee-Knoxville and published in the peer-reviewed University of Illinois-Chicago journal "First Monday," suggests that — despite protests to the contrary by Republicans and Trump allies — the Russian disinformation campaign was successful in influencing the 2016 election.
- [Libya Uncovers Alleged Russian Plot to Meddle in African Votes](#)  
Libyan security forces have **arrested two men accused of working for a Russian troll farm seeking to influence elections in the oil exporter and other African countries**. A letter from the state prosecutor of the internationally-backed Tripoli government to a Libyan security chief said the men were involved in “securing a

meeting” with Saif al-Islam al-Qaddafi, the fugitive son of the ousted dictator and a potential presidential candidate who enjoys the backing of some officials in Moscow.

- [Leaked documents reveal Russian effort to exert influence in Africa](#)  
**Russia is seeking to bolster its presence in at least 13 countries across Africa** by building relations with existing rulers, striking military deals, and grooming a new generation of “leaders” and undercover “agents”, leaked documents reveal.
- [Russia beating U.S. in race for global influence, Pentagon study says](#)  
The more than [150-page white paper](#), prepared for the Joint Chiefs of Staff and shared with POLITICO, **says the U.S. is still underestimating the scope of Russia's aggression**, which includes the use of propaganda and disinformation to sway public opinion across Europe, Central Asia, Africa and Latin America. The study also points to **the dangers of a growing alignment between Russia and China**, which share a fear of the United States' international alliances and an affinity for "authoritarian stability."
- [Lessons from the Mueller report on Russian political warfare](#)  
Alina Polyakova, director of the Project on Global Democracy and Emerging Technology at Brookings, testifies at a hearing of the House Judiciary Committee, "Lessons from the Mueller Report, Part II: Bipartisan Perspectives."

## China

- [Chinese Malign Influence and the Corrosion of Democracy](#)  
A new report from the International Republican Institute's (IRI) Building Resiliency for Interconnected Democracies in Global Environments (BRIDGE) initiative **examines the malign effects of China's economic influence and manipulation of the information space worldwide.**
- [Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate](#)  
When a pro-Beijing Taiwanese politician won an upset victory in the city of Kaohsiung last year, his supporters credited it to his charisma, political savvy, and tempting promises of richness and economic wealth from China. Barely six months into office, Kaohsiung Mayor Han Kuo-yu is already eyeing a run for the presidency in 2020 and is seen as the godsend that Beijing has been waiting for: the emergence of a populist, pro-China candidate in Taiwan. But Han's rise from obscurity to superstardom had a little help: **a campaign of social media manipulation orchestrated by a mysterious, seemingly professional cybergroup from China.**
- [Huawei Technologies' Links to Chinese State Security Services](#)  
This document **reviews data that provides direct, first-person accounts of Huawei personnel activity, relationships to Chinese military and intelligence agencies**, and the confluence of them both. They demonstrate the links between the two organisations, in spite of claims of Huawei to the contrary. The author reviews and demonstrates this through the use of three specific anonymised CVs.
- [How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument](#)  
The Chinese government has long been suspected of hiring as many as 2,000,000 people to surreptitiously insert huge numbers of pseudonymous and other deceptive writings into the stream of real social media posts, as if they were the genuine opinions of ordinary people. In the first large scale empirical analysis of this operation, **the authors show how to identify the secretive authors of these posts, the posts written by them, and their content.** The authors also estimate that **the government fabricates and posts about 448 million social media comments a year.** In contrast to prior claims, this study shows that the Chinese regime's strategy is to avoid arguing with skeptics of the party and the government, and to not even discuss controversial issues. Instead, the goal of this massive secretive operation is to distract the public and change the subject, as most of these posts involve cheerleading for China, the revolutionary history of the Communist Party, or other symbols of the regime.

## Tech Bytes

- [Fake news 'vaccine' works: 'pre-bunk' game reduces susceptibility to disinformation](#)  
Study of thousands of players shows a **simple online game works like a 'vaccine', increasing skepticism of "fake news"** by giving people a “weak dose” of the methods behind disinformation.

- [Real-Time Voice Cloning](#)  
This repository is an implementation of Transfer Learning from Speaker Verification to Multispeaker Text-To-Speech Synthesis (SV2TTS) with a vocoder that works in real-time. SV2TTS is a three-stage deep learning framework that allows to **create a numerical representation of a voice from a few seconds of audio**, and to use it to condition a text-to-speech model trained to generalize to new voices.
- [Fighting Fake News](#)  
A friend sends you a story that claims some outrageous facts. You try searching, but most of what you find is suspect, because you can't tell if the site is just repeating the same info, or if it's actually a credible site. Instead, use this search. **This limits your search to specific sites that are ranked Highly Factual by [Media Bias/Fact Check](#)**. Each site is tagged with its bias, allowing you to understand the viewpoint of the news source.
- [Giant Language model Test Room](#)  
The GLTR demo enables forensic inspection of the visual footprint of a language model on input text **to detect whether a text could be real or fake**. It is a collaborative effort between Hendrik Strobelt, Sebastian Gehrmann, and Alexander Rush from the MIT-IBM Watson AI lab and Harvard NLP.
- [The Most Comprehensive TweetDeck Research Guide In Existence \(Probably\)](#)  
This guide shows **how TweetDeck can vastly simplify and organize your research** while allowing you to collect a greater amount of information with less time and effort.
- [Researchers discover "Fishwrap" influence campaign recycling old terror news](#)  
Researchers at Recorded Future have uncovered what appears to be a new, growing social media-based influence operation involving more than 215 social media accounts. While relatively small in comparison to influence and disinformation operations run by the Russia-affiliated Internet Research Agency (IRA), **the campaign is notable because of its systematic method of recycling images and reports from past terrorist attacks and other events and presenting them as breaking news**—an approach that prompted researchers to call the campaign "Fishwrap."
- [Adobe trained AI to detect facial manipulation in Photoshop](#)  
A team of Adobe and UC Berkeley researchers **trained AI to detect facial manipulation in images edited with Adobe Photoshop**. The researchers hope the tool will help restore trust in digital media at a time when deepfakes and fake faces are more common and more deceptive. It could also democratize image forensics, making it possible for more people to uncover image manipulation.
- [You can train an AI to fake UN speeches in just 13 hours](#)  
Deep-learning techniques have made it easier and easier for anyone to forge convincing misinformation. But just how easy? Two researchers at Global Pulse, an initiative of the United Nations, decided to find out.
- [This AI-powered subreddit has been simulating the real thing for years](#)  
Can the human discourse on social media in 2019 be properly captured by a group of well-programmed bots? Of course it can. [r/subredditsimulator](#) is a subreddit -- three years in the making -- that consists solely of neural network bots.

## Disclaimer

The ideas and opinions expressed in these reports belong to the authors and do not necessarily reflect the views and opinions of the Government of Canada. By sharing these reports, RRM Coordination Unit does not endorse or validate their content.

RRM Coordination Unit collects and shares information consistent with Canada's privacy laws and the Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities. The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.



G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique international  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

Canada



TOGETHER • ENSEMBLE  
**CANADA**  
UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU  
2021-2022

---

**Bcc List:**

\*IOC; \*IOD; \*IOL; \*IOP; \*IOR; \*USS-DMA Advisors; \*MINA-Dept Unit; Shawn.Friele@international.gc.ca;  
Shelley.Whiting@international.gc.ca; Alexandre.Leveque@international.gc.ca; Graeme.Thompson@international.gc.ca;  
Ian.Higginbotham@international.gc.ca; Laurent.Dondey@international.gc.ca; Michael.Bonser@international.gc.ca;  
Ralph.Jansen@international.gc.ca; Amy.Mills@international.gc.ca; Anabel.Lindblad@international.gc.ca;  
Charles.Brisebois@international.gc.ca; Charles.Mojsej@international.gc.ca; Gregory.Galligan@international.gc.ca;  
Jennifer.Dunev@international.gc.ca; Leilla.Cranfield@international.gc.ca; Robert.Paterson@international.gc.ca;  
Stéphane.levesque@international.gc.ca; Adria.May@international.gc.ca; Albert.Lee@international.gc.ca;  
Evelyn.Puxley@international.gc.ca; Jean-Francois.Bergeron@international.gc.ca; Nichola.Payne@international.gc.ca;  
tim.lu@international.gc.ca; Arthur.David@international.gc.ca; Chris.Shapardanov@international.gc.ca;  
David.Nelson@international.gc.ca; Giles.Norman@international.gc.ca; Anne.Therrien@international.gc.ca;  
Ann.FlanaganWhalen@international.gc.ca; Alison.Grant@international.gc.ca; Alison.LeClaire@international.gc.ca;  
Giovanna.Roma@international.gc.ca; Valerie.Beloin@international.gc.ca; Robert.Fry@international.gc.ca;  
Richard.Colvin@international.gc.ca; Antoine.Nouvet@international.gc.ca; BREUCBSA-ASFC@international.gc.ca;  
Brian.Ebel@international.gc.ca; Christopher.Gibbins@international.gc.ca; Claudie.Senay@international.gc.ca;  
Eric.Laporte@international.gc.ca; Geoff.Gartshore@international.gc.ca; Jarrett.Reckseidler@international.gc.ca;  
Jason.Tolland@international.gc.ca; Jessica.Blitt@international.gc.ca; Jordan.Reeves@international.gc.ca;  
Kevin.Tunney@international.gc.ca; Leigh.Sarty@international.gc.ca; Maeva.Vidal@international.gc.ca;  
Martin.Laflamme@international.gc.ca; Martin.Loken@international.gc.ca; Richard.Delisle@international.gc.ca;  
Gallit.Dobner@international.gc.ca; Thomas.Gagnon@international.gc.ca; Sarah.Gillis@international.gc.ca;  
Roman.Waschuk@international.gc.ca; Huy.Nguyen@international.gc.ca; Vance.McEvoy@international.gc.ca;  
Sabine.Nolke@international.gc.ca; Alistair.Wallbaum@international.gc.ca; Kristen.Ambler@international.gc.ca;  
Tristan.Landry@international.gc.ca; Alex.Jasperse@tbs-sct.gc.ca; Bianca.Healy@tbs-sct.gc.ca; Bronwyn.Cline@tbs-  
sct.gc.ca; Dana.Robinson@tbs-sct.gc.ca; Doug.McCallum@tbs-sct.gc.ca; Helene.Potvin@tbs-sct.gc.ca;  
jonathan.Macdonald@tbs-sct.gc.ca; kirsten.duke@tbs-sct.gc.ca; Lesley.Kiely@tbs-sct.gc.ca; Lucas.Beal@tbs-sct.gc.ca;  
Mark.Stokes@tbs-sct.gc.ca; Michael.Murphy2@tbs-sct.gc.ca; Nathalie.Dussault@tbs-sct.gc.ca; Sean.Sutton@tbs-  
sct.gc.ca; Scott.MacIntosh@tbs-sct.gc.ca; Véronique.Gauvreau@tbs-sct.gc.ca; William.McMahon@tbs-sct.gc.ca;  
Anna.Cichosz@pco-bcp.gc.ca; Christos.Sarakinis@pco-bcp.gc.ca; Cloe.Prieur@pco-  
bcp.gc.ca; Colum.Grove-White@pco-bcp.gc.ca; David.Ott@pco-bcp.gc.ca; Guylaine.hamel@pco-bcp.gc.ca;  
Jean.Tessier@pco-bcp.gc.ca; Jessica.Kingsbury@pco-bcp.gc.ca; Kate.Binnie@pco-bcp.gc.ca;  
Michael.Waters@pco-bcp.gc.ca; Philippe-Andre.Rodriguez@pco-bcp.gc.ca;  
Raymond.Rivet@pco-bcp.gc.ca; Rob.Ammerman@pco-bcp.gc.ca; Sandra.Boudreau@pco-bcp.gc.ca;  
Alain.beaudoin@pco-bcp.gc.ca; Valerie.Samaan@pco-bcp.gc.ca;  
Katie.Abbott@pco-bcp.gc.ca; Lorna.Bonvie@pco-bcp.gc.ca;  
Tracy.Dool@pco-bcp.gc.ca;

David.Ennis-

Dawson@canada.ca; Dennis.Giguere@canada.ca; Gillian.Badger@canada.ca; julie.grenier@canada.ca;  
 Jamie.tomlinson@canada.ca; Leanne.maidment@canada.ca; lynn.fournier2@canada.ca; mike.ashman@canada.ca;  
 stephanie.sprott@canada.ca;  
 ryan.murphy2@canada.ca; Gabriel.TremblayGiroux@canada.ca;  
 Janice.Keenan@forces.gc.ca; MARK.FARFANDELOSGODOS@forces.gc.ca; RICHARD.PERREAU@forces.gc.ca;  
 DOUGLAS.ALLISON@forces.gc.ca; DESMOND.JAMES@forces.gc.ca; jay.janzen@forces.gc.ca;  
 Stephanie.Kennedy@forces.gc.ca; DAVID.ENNS4@forces.gc.ca; JOHN.ROACH2@forces.gc.ca;  
 SHANNON.ALFFORD@forces.gc.ca; YVETTE.GRYGORYEV@forces.gc.ca; Amelia.brown@elections.ca;  
 anne.lawson@elections.ca; Daniel.fischer@elections.ca; Darrell.Kekanovich@elections.ca; jane.dunlop@elections.ca;  
 Melanie.Wise@elections.ca; Rahul.badami@elections.ca; serge.caron@elections.ca; bruno.bosse@elections.ca;  
 reference@elections.ca; internationalaffairs@elections.ca; Isabelle.Duguay@elections.ca; susan.torosian@elections.ca;  
 Jacinthe.Dumont@cef-cce.ca; Mylene.Gigou@cef-cce.ca; Jane.Leeke@cef-cce.ca; Josee.Leb Blanc@cef-cce.ca;  
 Al.Mathews@cef-cce.ca; Amanda.Bellefeuille@rcmp-grc.gc.ca; Bill.Ricketts@rcmp-grc.gc.ca;  
 Christopher.Johnson@rcmp-grc.gc.ca; Dave.Rampersad@rcmp-grc.gc.ca; Deanne.Morgan@rcmp-grc.gc.ca;  
 Holly.Richter@rcmp-grc.gc.ca; Maria.Gurina@rcmp-grc.gc.ca; Kirk.Chiasson@rcmp-grc.gc.ca; Steve.Strang@rcmp-  
 grc.gc.ca;

caitlin.cowan@canada.ca;

danielbezalel.richardsen@canada.ca; Jack.Branswell@cic.gc.ca; james.lewis@canada.ca; josee.sirois3@canada.ca;  
 katherine.snow@canada.ca; Kirstan.Gagnon@justice.gc.ca; Lisa.Scarizzi@cic.gc.ca; marie-eve.lamoureux@canada.ca;  
 michael.himsl@canada.ca; paul.piasko@canada.ca; ps.goc-cog.sp@canada.ca; raymond.snow2@canada.ca;  
 Ritu.Gill@drdc-rddc.gc.ca; ryan.baker3@canada.ca; samson.kan@canada.ca; taylor.bildstein@canada.ca;  
 Tony.Seaboyer@rmc-cmr.ca; Toban.Morrison@justice.gc.ca; ShirleyAnne.Off@justice.gc.ca; Julien.houle@canada.ca;  
 laura.peckett@canada.ca

## Awali, Elabe

---

**From:** G7RRM@international.gc.ca  
**Sent:** Thursday, July 18, 2019 5:00 PM  
**To:** G7RRM@international.gc.ca  
**Subject:** RRM Canada: European Parliamentary elections report  
**Attachments:** RRM Canada - Comprehensive Report on the 2019 European Parliamentary Elections.pdf

Dear colleagues,

Please see attached the **European Parliamentary elections report produced by RRM Canada** using open-source data from social-media platforms in the lead-up to the elections. Various partners from the RRM network provided guidance in the development of this report; its findings may differ from other reports that have used other data sources, had different objectives or monitored for a longer period of time. It is important to note that RRM Canada monitors and analyzes all potential cases of foreign interference, regardless of the political party affected or political nature of any given issue.

The objectives of this report are to:

- **Shine light on any effort to artificially amplify unsubstantiated or false information by malign foreign actors** challenging the legitimacy and fairness of the UK, Irish or EU democratic and electoral system;
- **Identify key issues that were highly divisive and exploited** within the context of the EU elections in the UK, Ireland and Italy in order to identify narratives that may transcend borders and be used in other contexts; and
- **Identify notable tactics used by malign foreign actors.**

Key Findings:

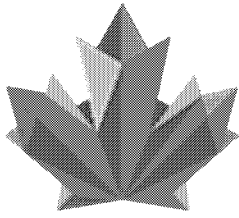
- RRM Canada **did not observe significant evidence of foreign state interference** in the data collected for the case studies examined during the European Parliamentary elections.
- However, RRM Canada **identified some tactics that had been previously used by foreign malign actors**, such as the Internet Research Agency (based in St. Petersburg) employed by non-state national and international actors.
- Moreover, RRM Canada **identified cases of strategic inauthentic amplification of divisive and inflammatory content**. This agrees with broader consensus of a move away from outright falsification to a greater emphasis on subtle and strategic manipulation and amplification of divisive narratives, as well as the adoption of well-known tactics of foreign interference and information manipulation by various non-state actors, creating a highly complex ecosystem.

As always, your feedback and comments are welcome.

G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique internationale  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada

Government  
of CanadaGouvernement  
du Canada

Canada



TOGETHER • ENSEMBLE

CANADA

UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU

2021-2022

**Bcc List**

\*IOC; \*IOD; \*IOL; \*IOP; \*IOR; \*USS-DMA Advisors; \*MINA-Dept Unit; [Shawn.Friele@international.gc.ca](mailto:Shawn.Friele@international.gc.ca);  
[Shelley.Whiting@international.gc.ca](mailto:Shelley.Whiting@international.gc.ca); [Alexandre.Leveque@international.gc.ca](mailto:Alexandre.Leveque@international.gc.ca); [Graeme.Thompson@international.gc.ca](mailto:Graeme.Thompson@international.gc.ca);  
[Ian.Higginbotham@international.gc.ca](mailto:Ian.Higginbotham@international.gc.ca); [Laurent.Dondey@international.gc.ca](mailto:Laurent.Dondey@international.gc.ca); [Michael.Bonser@international.gc.ca](mailto:Michael.Bonser@international.gc.ca);  
[Ralph.Jansen@international.gc.ca](mailto:Ralph.Jansen@international.gc.ca); [Amy.Mills@international.gc.ca](mailto:Amy.Mills@international.gc.ca); [Anabel.Lindblad@international.gc.ca](mailto:Anabel.Lindblad@international.gc.ca);  
[Charles.Brisebois@international.gc.ca](mailto:Charles.Brisebois@international.gc.ca); [Charles.Mojsej@international.gc.ca](mailto:Charles.Mojsej@international.gc.ca); [Gregory.Galligan@international.gc.ca](mailto:Gregory.Galligan@international.gc.ca);  
[Jennifer.Dunev@international.gc.ca](mailto:Jennifer.Dunev@international.gc.ca); [Leilla.Cranfield@international.gc.ca](mailto:Leilla.Cranfield@international.gc.ca); [Robert.Paterson@international.gc.ca](mailto:Robert.Paterson@international.gc.ca);  
[Stéphane.levesque@international.gc.ca](mailto:Stéphane.levesque@international.gc.ca); [Adria.May@international.gc.ca](mailto:Adria.May@international.gc.ca); [Albert.Lee@international.gc.ca](mailto:Albert.Lee@international.gc.ca);  
[Evelyn.Puxley@international.gc.ca](mailto:Evelyn.Puxley@international.gc.ca); [Jean-Francois.Bergeron@international.gc.ca](mailto:Jean-Francois.Bergeron@international.gc.ca); [Nichola.Payne@international.gc.ca](mailto:Nichola.Payne@international.gc.ca);  
[tim.lu@international.gc.ca](mailto:tim.lu@international.gc.ca); [Arthur.David@international.gc.ca](mailto:Arthur.David@international.gc.ca); [Chris.Shapardanov@international.gc.ca](mailto:Chris.Shapardanov@international.gc.ca);  
[David.Nelson@international.gc.ca](mailto:David.Nelson@international.gc.ca); [Giles.Norman@international.gc.ca](mailto:Giles.Norman@international.gc.ca); [Anne.Therrien@international.gc.ca](mailto:Anne.Therrien@international.gc.ca);  
[Ann.FlanaganWhalen@international.gc.ca](mailto:Ann.FlanaganWhalen@international.gc.ca); [Alison.Grant@international.gc.ca](mailto:Alison.Grant@international.gc.ca); [Alison.LeClaire@international.gc.ca](mailto:Alison.LeClaire@international.gc.ca);  
[Giovanna.Roma@international.gc.ca](mailto:Giovanna.Roma@international.gc.ca); [Valerie.Beloin@international.gc.ca](mailto:Valerie.Beloin@international.gc.ca); [Robert.Fry@international.gc.ca](mailto:Robert.Fry@international.gc.ca);  
[Richard.Colvin@international.gc.ca](mailto:Richard.Colvin@international.gc.ca); [Antoine.Nouvet@international.gc.ca](mailto:Antoine.Nouvet@international.gc.ca); [BRUCBSA-ASFC@international.gc.ca](mailto:BRUCBSA-ASFC@international.gc.ca);  
[Brian.Ebel@international.gc.ca](mailto:Brian.Ebel@international.gc.ca); [Christopher.Gibbins@international.gc.ca](mailto:Christopher.Gibbins@international.gc.ca); [Claudie.Senay@international.gc.ca](mailto:Claudie.Senay@international.gc.ca);  
[Eric.Laporte@international.gc.ca](mailto:Eric.Laporte@international.gc.ca); [Geoff.Gartshore@international.gc.ca](mailto:Geoff.Gartshore@international.gc.ca); [Jarrett.Reckseidler@international.gc.ca](mailto:Jarrett.Reckseidler@international.gc.ca);  
[Jason.Tolland@international.gc.ca](mailto:Jason.Tolland@international.gc.ca); [Jessica.Blitt@international.gc.ca](mailto:Jessica.Blitt@international.gc.ca); [Jordan.Reeves@international.gc.ca](mailto:Jordan.Reeves@international.gc.ca);  
[Kevin.Tunney@international.gc.ca](mailto:Kevin.Tunney@international.gc.ca); [Leigh.Sarty@international.gc.ca](mailto:Leigh.Sarty@international.gc.ca); [Maeva.Vidal@international.gc.ca](mailto:Maeva.Vidal@international.gc.ca);  
[Martin.Laflamme@international.gc.ca](mailto:Martin.Laflamme@international.gc.ca); [Martin.Loken@international.gc.ca](mailto:Martin.Loken@international.gc.ca); [Richard.Delisle@international.gc.ca](mailto:Richard.Delisle@international.gc.ca);  
[Gallit.Dobner@international.gc.ca](mailto:Gallit.Dobner@international.gc.ca); [Thomas.Gagnon@international.gc.ca](mailto:Thomas.Gagnon@international.gc.ca); [Sarah.Gillis@international.gc.ca](mailto:Sarah.Gillis@international.gc.ca);  
[Roman.Waschuk@international.gc.ca](mailto:Roman.Waschuk@international.gc.ca); [Huy.Nguyen@international.gc.ca](mailto:Huy.Nguyen@international.gc.ca); [Vance.McEvoy@international.gc.ca](mailto:Vance.McEvoy@international.gc.ca);  
[Sabine.Nolke@international.gc.ca](mailto:Sabine.Nolke@international.gc.ca); [Alistair.Wallbaum@international.gc.ca](mailto:Alistair.Wallbaum@international.gc.ca); [Kristen.Ambler@international.gc.ca](mailto:Kristen.Ambler@international.gc.ca);  
[Tristan.Landry@international.gc.ca](mailto:Tristan.Landry@international.gc.ca); [Alex.Jasperse@tbs-sct.gc.ca](mailto:Alex.Jasperse@tbs-sct.gc.ca); [Bianca.Healy@tbs-sct.gc.ca](mailto:Bianca.Healy@tbs-sct.gc.ca); [Bronwyn.Cline@tbs-sct.gc.ca](mailto:Bronwyn.Cline@tbs-sct.gc.ca);  
[Dana.Robinson@tbs-sct.gc.ca](mailto:Dana.Robinson@tbs-sct.gc.ca); [Doug.McCallum@tbs-sct.gc.ca](mailto:Doug.McCallum@tbs-sct.gc.ca); [Helene.Potvin@tbs-sct.gc.ca](mailto:Helene.Potvin@tbs-sct.gc.ca);  
[jonathan.Macdonald@tbs-sct.gc.ca](mailto:jonathan.Macdonald@tbs-sct.gc.ca); [kirsten.duke@tbs-sct.gc.ca](mailto:kirsten.duke@tbs-sct.gc.ca); [Lesley.Kiely@tbs-sct.gc.ca](mailto:Lesley.Kiely@tbs-sct.gc.ca); [Lucas.Beal@tbs-sct.gc.ca](mailto:Lucas.Beal@tbs-sct.gc.ca);  
[Mark.Stokes@tbs-sct.gc.ca](mailto:Mark.Stokes@tbs-sct.gc.ca); [Michael.Murphy2@tbs-sct.gc.ca](mailto:Michael.Murphy2@tbs-sct.gc.ca); [Nathalie.Dussault@tbs-sct.gc.ca](mailto:Nathalie.Dussault@tbs-sct.gc.ca); [Sean.Sutton@tbs-sct.gc.ca](mailto:Sean.Sutton@tbs-sct.gc.ca);  
[Scott.MacIntosh@tbs-sct.gc.ca](mailto:Scott.MacIntosh@tbs-sct.gc.ca); [Véronique.Gauvreau@tbs-sct.gc.ca](mailto:Véronique.Gauvreau@tbs-sct.gc.ca); [William.McMahon@tbs-sct.gc.ca](mailto:William.McMahon@tbs-sct.gc.ca);  
[Anna.Cichosz@pco-bcp.gc.ca](mailto:Anna.Cichosz@pco-bcp.gc.ca); [Christos.Sarakinos@pco-bcp.gc.ca](mailto:Christos.Sarakinos@pco-bcp.gc.ca); [Cloe.Prieur@pco-bcp.gc.ca](mailto:Cloe.Prieur@pco-bcp.gc.ca);  
[Colum.Grove-White@pco-bcp.gc.ca](mailto:Colum.Grove-White@pco-bcp.gc.ca); [David.Ott@pco-bcp.gc.ca](mailto:David.Ott@pco-bcp.gc.ca); [Guylaine.hamel@pco-bcp.gc.ca](mailto:Guylaine.hamel@pco-bcp.gc.ca);  
[Jean.Tessier@pco-bcp.gc.ca](mailto:Jean.Tessier@pco-bcp.gc.ca); [Jessica.Kingsbury@pco-bcp.gc.ca](mailto:Jessica.Kingsbury@pco-bcp.gc.ca); [Kate.Binnie@pco-bcp.gc.ca](mailto:Kate.Binnie@pco-bcp.gc.ca);  
[Michael.Waters@pco-bcp.gc.ca](mailto:Michael.Waters@pco-bcp.gc.ca); [Philippe-Andre.Rodriguez@pco-bcp.gc.ca](mailto:Philippe-Andre.Rodriguez@pco-bcp.gc.ca);  
[Raymond.Rivet@pco-bcp.gc.ca](mailto:Raymond.Rivet@pco-bcp.gc.ca); [Rob.Ammerman@pco-bcp.gc.ca](mailto:Rob.Ammerman@pco-bcp.gc.ca); [Sandra.Boudreau@pco-bcp.gc.ca](mailto:Sandra.Boudreau@pco-bcp.gc.ca);  
[Alain.beaudoin@pco-bcp.gc.ca](mailto:Alain.beaudoin@pco-bcp.gc.ca); [Valerie.Samaan@pco-bcp.gc.ca](mailto:Valerie.Samaan@pco-bcp.gc.ca);  
[Katie.Abbott@pco-bcp.gc.ca](mailto:Katie.Abbott@pco-bcp.gc.ca); [Lorna.Bonvie@pco-bcp.gc.ca](mailto:Lorna.Bonvie@pco-bcp.gc.ca);  
[Tracy.Dool@pco-bcp.gc.ca](mailto:Tracy.Dool@pco-bcp.gc.ca);

[David.Ennis-Dawson@canada.ca](mailto:David.Ennis-Dawson@canada.ca); [Dennis.Giguere@canada.ca](mailto:Dennis.Giguere@canada.ca); [Gillian.Badger@canada.ca](mailto:Gillian.Badger@canada.ca); [julie.grenier@canada.ca](mailto:julie.grenier@canada.ca);

[Jamie.tomlinson@canada.ca](mailto:Jamie.tomlinson@canada.ca); [Leanne.maidment@canada.ca](mailto:Leanne.maidment@canada.ca); [lynn.fournier2@canada.ca](mailto:lynn.fournier2@canada.ca); [mike.ashman@canada.ca](mailto:mike.ashman@canada.ca);  
[stephanie.sprott@canada.ca](mailto:stephanie.sprott@canada.ca);  
[ryan.murphy2@canada.ca](mailto:ryan.murphy2@canada.ca); [Gabriel.TremblayGiroux@canada.ca](mailto:Gabriel.TremblayGiroux@canada.ca);  
[Janice.Keenan@forces.gc.ca](mailto:Janice.Keenan@forces.gc.ca); [MARK.FARFANDELOSGODOS@forces.gc.ca](mailto:MARK.FARFANDELOSGODOS@forces.gc.ca); [RICHARD.PERREAU@forces.gc.ca](mailto:RICHARD.PERREAU@forces.gc.ca);  
[DOUGLAS.ALLISON@forces.gc.ca](mailto:DOUGLAS.ALLISON@forces.gc.ca); [DESMOND.JAMES@forces.gc.ca](mailto:DESMOND.JAMES@forces.gc.ca); [jay.janzen@forces.gc.ca](mailto:jay.janzen@forces.gc.ca);  
[Stephanie.Kennedy@forces.gc.ca](mailto:Stephanie.Kennedy@forces.gc.ca); [DAVID.ENNS4@forces.gc.ca](mailto:DAVID.ENNS4@forces.gc.ca); [JOHN.ROACH2@forces.gc.ca](mailto:JOHN.ROACH2@forces.gc.ca);  
[SHANNON.ALFFORD@forces.gc.ca](mailto:SHANNON.ALFFORD@forces.gc.ca); [YVETTE.GRYGORYEV@forces.gc.ca](mailto:YVETTE.GRYGORYEV@forces.gc.ca); [Amelia.brown@elections.ca](mailto:Amelia.brown@elections.ca);  
[anne.lawson@elections.ca](mailto:anne.lawson@elections.ca); [Daniel.fischer@elections.ca](mailto:Daniel.fischer@elections.ca); [Darrell.Kekanovich@elections.ca](mailto:Darrell.Kekanovich@elections.ca); [jane.dunlop@elections.ca](mailto:jane.dunlop@elections.ca);  
[Melanie.Wise@elections.ca](mailto:Melanie.Wise@elections.ca); [Rahul.badami@elections.ca](mailto:Rahul.badami@elections.ca); [serge.caron@elections.ca](mailto:serge.caron@elections.ca); [bruno.bosse@elections.ca](mailto:bruno.bosse@elections.ca);  
[reference@elections.ca](mailto:reference@elections.ca); [internationalaffairs@elections.ca](mailto:internationalaffairs@elections.ca); [Isabelle.Duguay@elections.ca](mailto:Isabelle.Duguay@elections.ca); [susan.torosian@elections.ca](mailto:susan.torosian@elections.ca);  
[Jacinthe.Dumont@cef-cce.ca](mailto:Jacinthe.Dumont@cef-cce.ca); [Mylene.Gigou@cef-cce.ca](mailto:Mylene.Gigou@cef-cce.ca); [Jane.Leeke@cef-cce.ca](mailto:Jane.Leeke@cef-cce.ca); [Josee.LebLANC@cef-cce.ca](mailto:Josee.LebLANC@cef-cce.ca);  
[Al.Mathews@cef-cce.ca](mailto:Al.Mathews@cef-cce.ca); [Amanda.Bellefeuille@rcmp-grc.gc.ca](mailto:Amanda.Bellefeuille@rcmp-grc.gc.ca); [Bill.Ricketts@rcmp-grc.gc.ca](mailto:Bill.Ricketts@rcmp-grc.gc.ca);  
[Christopher.Johnson@rcmp-grc.gc.ca](mailto:Christopher.Johnson@rcmp-grc.gc.ca); [Dave.Rampersad@rcmp-grc.gc.ca](mailto:Dave.Rampersad@rcmp-grc.gc.ca); [Deanne.Morgan@rcmp-grc.gc.ca](mailto:Deanne.Morgan@rcmp-grc.gc.ca);  
[Holly.Richter@rcmp-grc.gc.ca](mailto:Holly.Richter@rcmp-grc.gc.ca); [Maria.Gurina@rcmp-grc.gc.ca](mailto:Maria.Gurina@rcmp-grc.gc.ca); [Kirk.Chiasson@rcmp-grc.gc.ca](mailto:Kirk.Chiasson@rcmp-grc.gc.ca); [Steve.Strang@rcmp-grc.gc.ca](mailto:Steve.Strang@rcmp-grc.gc.ca);  
  
[eric.gordon@rcmp-grc.gc.ca](mailto:eric.gordon@rcmp-grc.gc.ca); [cameron.ortis@rcmp-grc.gc.ca](mailto:cameron.ortis@rcmp-grc.gc.ca);  
  
[caitlin.cowan@canada.ca](mailto:caitlin.cowan@canada.ca);  
[danielbezalel.richardsen@canada.ca](mailto:danielbezalel.richardsen@canada.ca); [Jack.Branswell@cic.gc.ca](mailto:Jack.Branswell@cic.gc.ca); [james.lewis@canada.ca](mailto:james.lewis@canada.ca); [josee.sirois3@canada.ca](mailto:josee.sirois3@canada.ca);  
[katherine.snow@canada.ca](mailto:katherine.snow@canada.ca); [Kirstan.Gagnon@justice.gc.ca](mailto:Kirstan.Gagnon@justice.gc.ca); [Lisa.Scarizzi@cic.gc.ca](mailto:Lisa.Scarizzi@cic.gc.ca); [marie-eve.lamoureux@canada.ca](mailto:marie-eve.lamoureux@canada.ca);  
[michael.himsl@canada.ca](mailto:michael.himsl@canada.ca); [paul.piasko@canada.ca](mailto:paul.piasko@canada.ca); [ps.goc-cog.sp@canada.ca](mailto:ps.goc-cog.sp@canada.ca); [raymond.snow2@canada.ca](mailto:raymond.snow2@canada.ca);  
[Ritu.Gill@drdc-rddc.gc.ca](mailto:Ritu.Gill@drdc-rddc.gc.ca); [ryan.baker3@canada.ca](mailto:ryan.baker3@canada.ca); [samson.kan@canada.ca](mailto:samson.kan@canada.ca); [taylor.bildstein@canada.ca](mailto:taylor.bildstein@canada.ca);  
[Tony.Seaboyer@rmc-cmr.ca](mailto:Tony.Seaboyer@rmc-cmr.ca); [Toban.Morrison@justice.gc.ca](mailto:Toban.Morrison@justice.gc.ca); [ShirleyAnne.Off@justice.gc.ca](mailto:ShirleyAnne.Off@justice.gc.ca); [Julien.houle@canada.ca](mailto:Julien.houle@canada.ca);  
[laura.peckett@canada.ca](mailto:laura.peckett@canada.ca)

## OPEN DATA ANALYSIS<sup>1</sup>

### European Parliamentary Elections: Comprehensive Report

**Issue:** This open source data report outlines comprehensive findings by the Rapid Response Mechanism Canada (RRM Canada) related to foreign interference during and leading up to the 2019 European Union Parliamentary Elections, May 23-26, 2019. RRM Canada's reporting is informed by in-house analysis and consolidates insights from members of the RRM network. It is important to note that RRM Canada monitors and analyzes all potential cases of foreign interference, regardless of the political party affected or political nature of any given issue.

#### The objectives of this report are to:

- Shine light on any effort to artificially amplify unsubstantiated or false information challenging the legitimacy and fairness of the UK, Irish or EU democratic and electoral systems;<sup>2</sup>
- Identify key issues that were highly divisive and exploited within the context of the EU elections in the UK, Ireland and Italy in order to identify narratives that may transcend borders and be used in other contexts; and
- Identify notable tactics used by malign, foreign actors.

#### Key Findings

- RRM Canada did not observe significant evidence of state-based foreign interference, or any large-scale, organized and coordinated efforts by non-state actors in any of the case studies examined during the European Parliamentary Elections.
- RRM Canada identified national and transnational actors taking a page out of the Internet Research Agency (IRA) playbook, using the same tactics the IRA used in previous elections, such as the 2016 U.S. Elections.
- The use of foreign interference tactics by national actors makes it difficult to identify foreign interference campaigns with a high degree of certainty.
- The disinformation identified by RRM Canada tended to use authentic information that had been manipulated and distorted by means of misrepresenting its content or context (i.e. “**de-contextualization**”). This tactic allows for the creation of divisive content aimed at undermining social cohesion and reducing trust in democratic institutions by targeting communities susceptible to divisive content, which is based on factual information. This is also in line with a continuing trend where there is a shift from information warfare to manipulation and amplification of divisive narratives through narrative competition.<sup>3</sup>
- Strategic, inauthentic amplification of divisive and inflammatory content was found around issues related to the following topics: immigration/migration, anti-religious sentiment (Muslim and Jewish), nationalist identity, women's health, gender-based harassment and climate change. This was likely done by national or international non-state actors.

---

<sup>1</sup> The purpose of Open Source Data reporting is to assist in charting trends, strategies and tactics in foreign interference. Prepared by RRM Canada, this work supports the G7 RRM – an initiative announced in 2018 in Charlevoix, mandated to strengthen coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response

<sup>2</sup> RRM Canada has selected 3 cases (UK, Ireland and Italy) based on initial research, linguistic limitations, and most importantly, it is an attempt to fill in gaps in the RRM networks coverage and support cases looked at by partner organizations. This approach was meant to ensure a more complete understanding of foreign interference within the context of the EU Parliamentary Elections.

<sup>3</sup> Also noted by partner organizations, including a recent report from the Institute for Strategic Dialogue (2019).

## Challenging the legitimacy and fairness of the UK, EU and Irish democratic system

RRM Canada identified some incidents of coordinated inauthentic behaviour in relation to the artificial amplification of disinformation on social media. However, the available data would appear to indicate that this coordinated inauthentic behaviour does not stem from a foreign state, or large-scale organized non-state actor. Rather, our findings show that national and international non-state actors, likely originating from various far-right communities across Europe and the United States, have most notably (though not exclusively) emulated approaches from the Russian sponsored IRA Playbook used during the 2016 American Presidential Election.

Twitter, Facebook and Reddit<sup>4</sup> accounts were used to spread divisive and false information to damage and negatively impact social cohesion and trust in democratic processes and institutions. These efforts also included the use of blogs and webpages to host disinformation, as well as coordinated networks of Facebook groups, Reddit accounts and Twitter account networks to disseminate content.

An example of these activities include false and unsubstantiated information on vote rigging, noting Counting Agents with the UK Brexit Party were barred from viewing the vote count. This was amplified through a series of inauthentic and coordinated accounts/networks online<sup>5</sup> during the voting period to challenge the legitimacy of the electoral process in Nottingham, UK, and the UK more generally.

## Use of Divisive Narrative to Undermine Social Cohesion

RRM Canada identified a shift from **information warfare**<sup>6</sup> to **narrative competition**.<sup>7</sup> A key trend in the data is the dissemination and amplification of divisive issues such as: immigration, Muslims in Europe, climate change and liberal vs conservative values. What is notable is the strategic pushing of inflammatory and divisive narratives across national borders and global political contexts to engage pan-European, regional and international communities.

### Migration/Immigration

An example of this would be the story of “400 African illegal immigrants stormed in the terminal of the Charles de Gaulle Airport in Paris”. This [tweet](#) was initially recounted by the NY Post “[Footage shows hundreds of migrants occupying French airport terminal](#)”. When this story was picked up by national and transnational far-right and Kremlin-affiliated news sites and blogs, it snow balled, being posted by [Voice of Europe](#), [ZeroHedge](#), [Westernjournal](#), [Jihadwatch](#), [Sputnik](#), [Breitbart](#), [TheBlaze](#), [InfoWars](#), etc. In this instance, a transnational network of actors shared, copied and reproduced divisive content related to a minor local protest with no noted incidents. Suspicious sites picked up this content to reach a broader audience by manipulating what is called Search Engine Optimization or SEO<sup>8</sup> and artificially amplified it days before the EU Parliamentary Election by both a network of dubious and unreliable

---

<sup>4</sup> Focus on these specific platforms was due to limitations in access, and indicators of key points of engagement.

<sup>5</sup> This incident showed no evidence of being linked to a foreign actor, according to information available to RRM Canada.

<sup>6</sup> Please see: New Knowledge. 2019. “Tactics and Tropes of the Internet Research Agency,” for further information.

<sup>7</sup> Competition for the way an issue is framed within public discourse, with each framing looking to become the dominant method of conceptualizing said issue, is referred to as “narrative competition”. Please see the Institute for Strategic Design (2019). “2019 EU Elections Information Operations Analysis” for further explanation.

<sup>8</sup> Search engine optimization is the process of affecting the online visibility of a website or a web page in a web search engine's unpaid results. It is a measurable, repeatable process that is used to send signals to search engines that a webpage is worth showing in Google's index. Though this process should occur organically by users visiting a website, this can be manipulated by multiple tactics to give an inauthentic SEO score thus artificially amplifying content.

websites, as well as a network of inauthentic accounts on Twitter and Reddit.<sup>9</sup> This aided in increasing reach and traction, using near identical, divisive framing of the event, playing on anti-immigrant, anti-African and identity-based sentiment with sensationalized and inflammatory language, and referencing the original content to provide the allusion of validation in reporting.

#### Health and Reproductive Issues<sup>10</sup>

Another example is an attempt to sow division and further polarize communities around an already highly charged topic. In the Irish context, RRM Canada found national and international non-state actors manipulating and framing authentic information from the public Health Service of Ireland using inflammatory and divisive rhetoric about abortion and pregnancy “remains.” This information was amplified and targeted at susceptible far/alt-right and conservative communities locally and internationally<sup>11</sup> through coordinated activity.

This tactic is valuable in transferring a narrative from one community to another, amplifying its significance, and targeting those susceptible to inflammatory and sensationalized content in order to affect discourse around divisive issue across states, Europe and internationally. A narrative may be altered slightly for different audiences, but the core aspects of its framing and messaging are transmitted regardless of the source.

#### **Additional Tactics and Approaches of Note**

RRM Canada observed a number of noteworthy tactics employed throughout the EU. One tactic is the use of manipulated authentic information posted on untrustworthy websites, blogs, and by questionable journalists or inauthentic accounts to seed conversations. The information is then picked up and framed using a divisive and inflammatory narrative by a broader network of accounts, websites and blogs<sup>12</sup> referencing the original posting to substantiate their story. Finally, this information is amplified by networks of inauthentic accounts in a coordinated fashion. This information targets susceptible communities and may be translated to various languages to target broader political contexts and audiences. RRM Canada describes this tactic as “**de-contextualization**,” as the basis of the information is authentic content that is manipulated and distorted. A version of this tactic has been observed as being used by Kremlin-linked actors and is a known tactic of covert, malicious foreign actors.<sup>13</sup>

A similar but notable tactic for amplifying content, and strategically translating and pushing it into new communities, was observed in our Italian case study. In this case, the initial content focused on Euroscepticism and anti-globalist sentiment and conspiracy. Using a speech by Italian Deputy Prime Minister Matteo Salvini, content was initially spread and amplified through a set of inauthentic and coordinated accounts. It was then strategically targeted at influential and well-known authentic online actors in order to have it boost engagement. Finally, the content was translated into four different languages and amplified again by systematically pushing it in these four separate communities simultaneously, in order to increase reach and prominence in various far-right European discussions and communities.

---

<sup>9</sup> The Twitter network of inauthentic accounts was observed as central to various attempts at amplification. Reddit posts targeted well-known conspiracy and far/alt-right groups, including *The\_Donald*, *New Right* and *The\_Europe*.

<sup>10</sup> According to Ireland Health Services Executive this falls under: Unplanned Pregnancy Support Services.

<sup>11</sup> This incident showed evidence of being linked to a foreign actor, according to RRM Canada.

<sup>12</sup> This includes several pro-Kremlin sites including, Zerohedge, RT, and Sputnik, as well as various alt-right or far-right sites.

<sup>13</sup> See DRF Lab’s work on the EU Parliamentary Elections.



RRM Canada also noted a small incident of inauthentic left progressive accounts,<sup>14</sup> engaging in left-leaning discussions, while also being embedded in a far-right inauthentic network. What was notable about these accounts was that they used hashtags, language characteristic of and played into the general performativity of a left progressive actor, but also prominently displayed their Muslim identity and the intention for a “Muslim takeover” of the west. They were then used as examples of the “radical left” and “radical Muslims” by various far/alt-right groups presenting accounts online. RRM Canada believes these to be experimentation with new tactics meant to provoke and act as a means to further and artificially aid in polarizing the left and the right over wedge issues.

### **Concluding Remarks**

Our findings are consistent in a number of ways with other experts in this field. Notable findings from published reports illustrate the impact of tactics like narrative competition, and the emergence of new actors using well-known information operation tactics, particularly non-state actors.<sup>15</sup> Some experts found instances of state-based foreign interference, including on platforms like Facebook, Reddit and Medium, while noting amongst the various findings the emergence of the tactic of planting, seeding and systematically amplifying false information across platforms and other information sources.<sup>16</sup> In relation to the EU Parliamentary Elections, a key insight from RRM Canada is that while no significant evidence of state-based foreign interference was observed, the digital ecosystem is ripe and ideal for exploitation by foreign malign actors.<sup>17</sup>

**Released: 18 July 2019**

**Disclaimer:** Rapid Response Mechanism Canada monitors and shares information consistent with Canada’s privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

---

<sup>14</sup> Only two accounts were observed exhibiting this inauthentic and dubious behaviour, and were taken down in advance of the election period. RRM Canada assesses that this is representative of the potential testing of a new tactic.

<sup>15</sup> Please see the Institute for Strategic Design (2019). “2019 EU Elections Information Operations Analysis.”

<sup>16</sup> Please See: Digital Forensics Research Lab. 2019. “Top Takes: Suspected Russian Intelligence Operations.” June 22, 2019.

<sup>17</sup> It must be noted that the findings of this report may differ from other reports that have used or have access to other source data and information, had different objectives or monitored for a longer period of time.

**From:** G7RRM@international.gc.ca  
**Sent:** Friday, May 3, 2019 5:47 PM  
**To:** G7RRM@international.gc.ca  
**Subject:** RRM Canada: Alberta Elections Analysis and NATO StratCom Report  
**Attachments:** 1. Alberta Elections Analysis.docx; 2. Hybrid Threats - A Strategic Communications Perspective-compressed.pdf

Dear colleagues,

Please see attached the following report produced by RRM Canada:

**1. Alberta Elections Analysis**

This report analyzes open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019.

Additionally, the following report from the NATO Strategic Communications Centre of Excellence is also attached:

**2. Hybrid Threats - A Strategic Communications Perspective**

This report is the result of a two-year study conducted by the NATO Strategic Communications Centre of Excellence. It is designed to help national authorities understand, prepare for, identify and respond to hybrid threats.

Feedback/comments are always welcome.

Kind regards,

G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique international  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

**Canada**



TOGETHER • ENSEMBLE  
**CANADA**  
UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU  
2021-2022

## Bcc List

\*IOC <D-IOC@international.gc.ca>; \*IOD <D-IOD@international.gc.ca>; \*IOL <D-IOL@international.gc.ca>; \*IOP <D-IOP@international.gc.ca>; \*IOR <D-IOR@international.gc.ca>; \*USS-DMA Advisors <D-USS-DMAAdvisors@international.gc.ca>; \*MINA-Dept Unit <D-MINA-Dept-Unit@international.gc.ca>; Friele, Shawn -IFM <Shawn.Friele@international.gc.ca>; Whiting, Shelley -IOD <Shelley.Whiting@international.gc.ca>; Lévêque, Alexandre -POD <Alexandre.Leveque@international.gc.ca>; Thompson, Graeme -POL <Graeme.Thompson@international.gc.ca>; Higginbotham, Ian -POL <Ian.Higginbotham@international.gc.ca>; Dondey, Laurent -POG <Laurent.Dondey@international.gc.ca>; Bonser, Michael -POG <Michael.Bonser@international.gc.ca>; Jansen, Ralph -PRD <Ralph.Jansen@international.gc.ca>; Mills, Amy -LCBR <Amy.Mills@international.gc.ca>; Lindblad, Anabel -LCB <Anabel.Lindblad@international.gc.ca>; Brisebois, Charles -LDS <Charles.Brisebois@international.gc.ca>; Mojsej, Charles -LCD <Charles.Mojsej@international.gc.ca>; Galligan, Gregory -LCF <Gregory.Galligan@international.gc.ca>; Dunev, Jennifer -LCFA <Jennifer.Dunev@international.gc.ca>; Cranfield, Leilla -LDN <Leilla.Cranfield@international.gc.ca>; Paterson, Robert -LCM <Robert.Paterson@international.gc.ca>; Stéphane.levesque@international.gc.ca; May, Adria -OPB <Adria.May@international.gc.ca>; Lee, Albert -OPC <Albert.Lee@international.gc.ca>; Puxley, Evelyn -OPX <Evelyn.Puxley@international.gc.ca>; Bergeron, Jean-François -OPB <Jean-Francois.Bergeron@international.gc.ca>; Payne, Nichola -OPB <Nichola.Payne@international.gc.ca>; Lu, Tim -OPB <tim.lu@international.gc.ca>; David, Arthur -IOC <Arthur.David@international.gc.ca>; Shapardanov, Chris -IDS <Chris.Shapardanov@international.gc.ca>; Nelson, David -IGR <David.Nelson@international.gc.ca>; Norman, Giles -IGR <Giles.Norman@international.gc.ca>; Therrien, Anne -EUA <Anne.Therrien@international.gc.ca>; Flanagan Whalen, Ann -EUA <Ann.FlanaganWhalen@international.gc.ca>; Grant, Alison -ECE <Alison.Grant@international.gc.ca>; LeClaire, Alison -ECD <Alison.LeClaire@international.gc.ca>; Roma, Giovanna -EUA <Giovanna.Roma@international.gc.ca>; Beloin, Valérie -ECE <Valerie.Beloin@international.gc.ca>; Fry, Robert -EUD <Robert.Fry@international.gc.ca>; Colvin, Richard -EUA <Richard.Colvin@international.gc.ca>; Nouvet, Antoine -IGR <Antoine.Nouvet@international.gc.ca>; BREU (CBSA-ASFC) <BREUCBSA-ASFC@international.gc.ca>; Ebel, Brian -BGRAD -GR <Brian.Ebel@international.gc.ca>; Gibbins, Christopher -WSHDC -GR <Christopher.Gibbins@international.gc.ca>; Senay, Claudie -LDN -GR <Claudie.Senay@international.gc.ca>; Laporte, Eric -BNATO -GR <Eric.Laporte@international.gc.ca>; Gartshore, Geoff -BRLIN -GR <Geoff.Gartshore@international.gc.ca>; Reckseidler, Jarrett -BREU -GR <Jarrett.Reckseidler@international.gc.ca>; Tolland, Jason -HSNKI -HOM/CDM <Jason.Tolland@international.gc.ca>; Blitt, Jessica -BREU -GR <Jessica.Blitt@international.gc.ca>; Reeves, Jordan -TAPEI -HOM/CDM <Jordan.Reeves@international.gc.ca>; Tunney, Kevin -WSHDC -GR <Kevin.Tunney@international.gc.ca>; Sarty, Leigh -DSIR <Leigh.Sarty@international.gc.ca>; Vidal, Maeva -BNATO -GR <Maeva.Vidal@international.gc.ca>; Laflamme, Martin -BEIJING -PA <Martin.Laflamme@international.gc.ca>; Loken, Martin -WSHDC -GR <Martin.Loken@international.gc.ca>; Delisle, Richard -BNATO -GR <Richard.Delisle@international.gc.ca>; Waschuk, Roman -KYIV -HOM/CDM <Roman.Waschuk@international.gc.ca>; Nolke, Sabine -HAGUE HOM/CDM <Sabine.Nolke@international.gc.ca>; Landry, Tristan -PARIS -GR <Tristan.Landry@international.gc.ca>; Alex.Jasperse@tbs-sct.gc.ca; Bianca.Healy@tbs-sct.gc.ca; Bronwyn.Cline@tbs-sct.gc.ca; Dana.Robinson@tbs-sct.gc.ca; Doug.McCallum@tbs-sct.gc.ca; Helene.Potvin@tbs-sct.gc.ca; jonathan.Macdonald@tbs-sct.gc.ca; kirsten.duke@tbs-sct.gc.ca; Lesley.Kiely@tbs-sct.gc.ca; Lucas.Beal@tbs-sct.gc.ca; Mark.Stokes@tbs-sct.gc.ca; Michael.Murphy2@tbs-sct.gc.ca; Nathalie.Dussault@tbs-sct.gc.ca; Sean.Sutton@tbs-sct.gc.ca; Scott.MacIntosh@tbs-sct.gc.ca; Véronique.Gauvreau@tbs-sct.gc.ca; William.McMahon@tbs-sct.gc.ca; Anna.Cichosz@pco-bcp.gc.ca; Ayesha.Malette@pco-bcp.gc.ca; Christos.Sarakinos@pco-bcp.gc.ca; Cloe.Prieur@pco-bcp.gc.ca; Colum.Grove-White@pco-bcp.gc.ca; David.Ott@pco-bcp.gc.ca; Guylaine.hamel@pco-bcp.gc.ca; Jean.Tessier@pco-bcp.gc.ca; Jessica.Kingsbury@pco-bcp.gc.ca; Kate.Binnie@pco-bcp.gc.ca; Michael.Waters@pco-bcp.gc.ca; Philippe-Andre.Rodriguez@pco-bcp.gc.ca; Raymond.Rivet@pco-bcp.gc.ca; Rob.Ammerman@pco-bcp.gc.ca; Sandra.Boudreau@pco-bcp.gc.ca; Valerie.Samaan@pco-bcp.gc.ca; Tracy.Dool@pco-bcp.gc.ca;

David.Ennis-Dawson@canada.ca; Dennis.Giguere@canada.ca; Gillian.Badger@canada.ca; julie.grenier@canada.ca;

lynn.fournier2@canada.ca; mike.ashman@canada.ca; stephanie.sprott@canada.ca;  
Janice.Keenan@forces.gc.ca;  
MARK.FARFANDELOSGODOS@forces.gc.ca; RICHARD.PERREAU@forces.gc.ca; DOUGLAS.ALLISON@forces.gc.ca;  
DESMOND.JAMES@forces.gc.ca; jay.janzen@forces.gc.ca; Stephanie.Kennedy@forces.gc.ca;  
SHANNON.ALFFORD@forces.gc.ca; YVETTE.GRYGORYEV@forces.gc.ca; Amelia.brown@elections.ca;  
anne.lawson@elections.ca; Daniel.fischer@elections.ca; Darrell.Kekanovich@elections.ca; jane.dunlop@elections.ca;  
Melanie.Wise@elections.ca; Rahul.badami@elections.ca; serge.caron@elections.ca; bruno.bosse@elections.ca;  
susan.torosian@elections.ca; Jacinthe.Dumont@cef-cce.ca; Amanda.Bellefeuille@rcmp-grc.gc.ca; Bill.Ricketts@rcmp-  
grc.gc.ca; Christopher.Johnson@rcmp-grc.gc.ca; Rampersad, Dave -RCMP/GRC <dave.rampersad@rcmp-grc.gc.ca>;  
Deanne.Morgan@rcmp-grc.gc.ca; Holly.Richter@rcmp-grc.gc.ca; Maria.Gurina@rcmp-grc.gc.ca; Steve.Strang@rcmp-  
grc.gc.ca;

Gordon, Eric -

RCMP/GRC <eric.gordon@rcmp-grc.gc.ca>; cameron.ortis@rcmp-grc.gc.ca;  
ANGELA.MAXWELL@forces.gc.ca; caitlin.cowan@canada.ca;  
danielbezalel.richardsen@canada.ca; Jack.Branswell@cic.gc.ca; james.lewis@canada.ca; josee.sirois3@canada.ca;  
katherine.snow@canada.ca; Kirstan.Gagnon@justice.gc.ca; Lisa.Scarizzi@cic.gc.ca; marie-eve.lamoureux@canada.ca;  
michael.himsl@canada.ca; paul.piasko@canada.ca; ps.goc-cog.sp@canada.ca; raymond.snow2@canada.ca;  
Ritu.Gill@drdc-rddc.gc.ca; ryan.baker3@canada.ca; samson.kan@canada.ca; taylor.bildstein@canada.ca;  
Tony.Seaboyer@rmc-cmr.ca

## ALBERTA ELECTION ANALYSIS

## PURPOSE

This report analyses open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019. Prepared in support of the [G7 Rapid Response Mechanism \(RRM\)](#), the report was penned by RRM Canada. The RRM is mandated to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

## KEY FINDINGS

Based on primary and secondary research, RRM Canada concludes that there were very likely **no significant foreign interference campaigns** targeting the Alberta election in the online space in April 2019. However, coordinated inauthentic activity was detected:

- **RRM Canada identified accounts that demonstrated coordinated inauthentic behaviour.** RRM Canada judges the activity is very unlikely to comprise one third of the online conversation as reported by [Press Progress on April 11, 2019](#).
- RRM Canada identified cases of social media accounts, which were **likely inauthentic, coordinated behaviour**<sup>1</sup> around online discussions about the Alberta election. However, the majority of these accounts were very likely not foreign.
- RRM Canada identified known national far-right and hate group actors who have previously disseminated material, **using similar tactics as known malign foreign actors.**
- RRM identified **accounts tied to lobbying groups** that were unaffiliated with a political party spreading disinformation online in the run-up to the Alberta election.
- The Alberta election provides an example of a situation where there may be evidence of **coordinated inauthentic behaviour undertaken by Canadian actors**, making the identification of foreign interference more difficult.

## Alberta Election Findings

[1] RRM Canada reviewed social media data to search for obvious cases of coordinated, inauthentic behaviour with the objective of identifying any potential foreign activities. Based on available information, it is very unlikely there was any foreign interference. The two largest components of the graph are made up of supporters of the former Premier Notley and Premier Kenney, as expected in an election campaign [Annex A].

[2] RRM Canada assesses that none of the major communities taking part in online conversations related to the elections are driven by foreign interference. The presence of automated inauthentic activities does not appear central or crucial to the overall conversation or activity.

---

<sup>1</sup> Scale of Estimative Language: Almost No Chance – [0 – 10]; Very Unlikely/Very Improbable – [11 – 29]; Unlikely/Improbable – [30 – 39]; Roughly Even Chance – [40 – 59]; Likely/Probable – [60 – 69]; Very Likely/Very Probable – [70 – 89]; Almost Certainly – [90 – 100]

[3] RRM Canada's findings stand opposite to the [April 11, Press Progress report](#), which claimed that a third of accounts talking about the Alberta election were bots. **RRM Canada's findings, using multiple tools and methods, judges that the online activity is very unlikely to comprise one third of bots.** The article appears to rely only on the online tool mentionsmap as a metric for "bot activity", which is not a proper means of assessment for inauthentic account behaviour or bot activity. RRM Canada therefore does not support the findings articulated in the Press Progress Report.

[4] RRM Canada identified communities that **demonstrated a suspicious account creation pattern that is indicative of troll or bot activity.** Recent spikes in account creation suggest the presence of accounts developed for a specific purpose; however, **the community was determined to very likely be domestic,** as it was mainly comprised of supporters of the United Conservative Party (UCP). A second small community was identified as supporters of the People's Party of Canada, which had similar suspicious patterns of account creation. This pattern was not identified within communities of supporters of the Alberta Liberal Party or Alberta New Democratic Party. The overall number of accounts is a small percentage of a larger collection [Annex B]. This highlights a key point, namely that **domestic actors are also emulating the tactics used by foreign actors, within the context of provincial elections. This behaviour will make it increasingly difficult to distinguish national from foreign interference efforts in the upcoming Federal election.**

[5] The RRM identified a small group of anonymous accounts pushing a pro-separation movement in Alberta and the Prairies. Though Alberta has an official separatist party, <https://albertaindependence.ca/>, these accounts do not appear affiliated with this movement. Creating false separatist movements or amplifying domestic ones is a known tactic in foreign interference. Though unaffiliated, at this time, RRM Canada cannot tie this small group of accounts to any foreign entity.

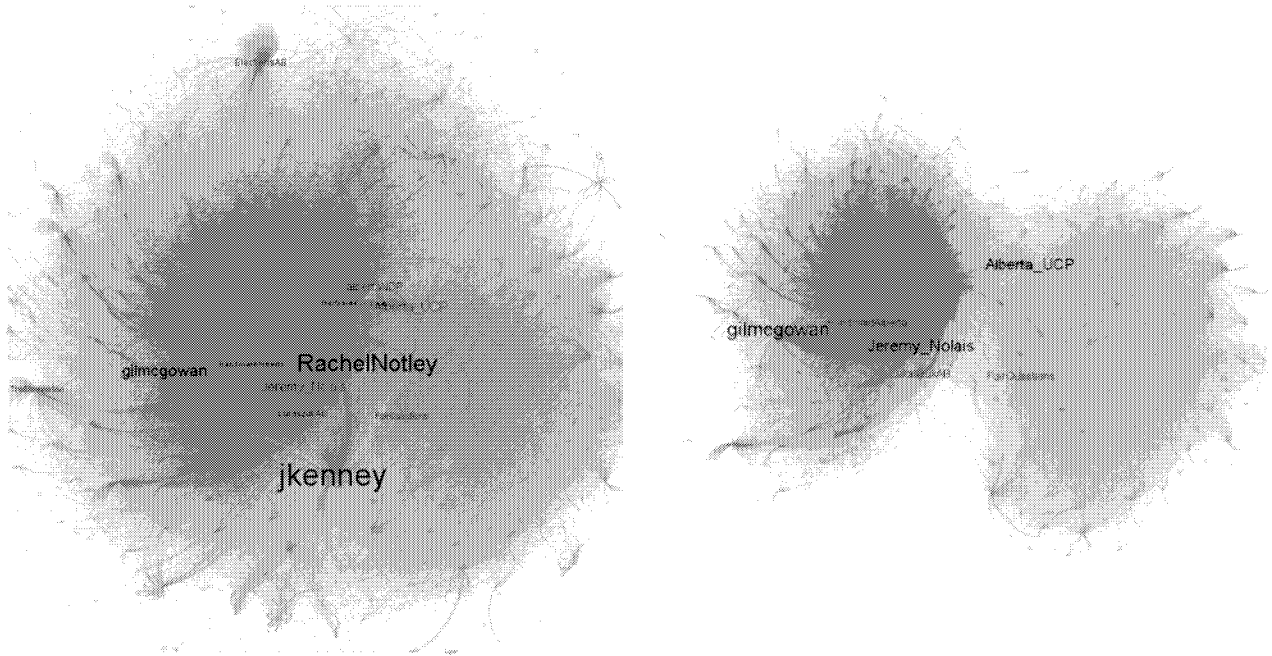
[6] In its review of the data of this election, RRM Canada found no evidence supporting a broad, coordinated campaign to influence the Alberta election. **RRM Canada assesses that automated inauthentic behaviour and trolling activities are very likely domestic in nature;**

Released: May 1, 2019

**Disclaimer:** G7 Rapid Response Mechanism Canada (RRM Canada) monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

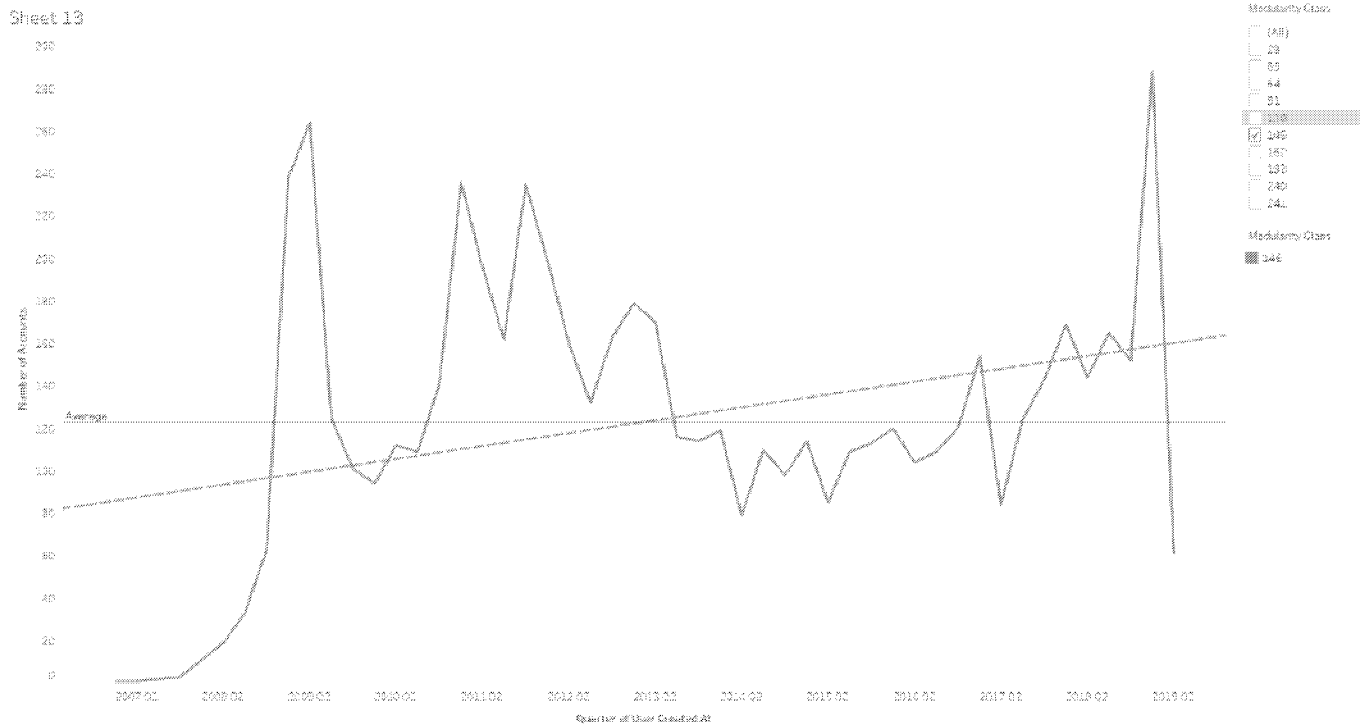
Annex A

This Annex is a visual representation of RRM Canada’s data collection illustrating a high level of normality in the online conversation related to the Alberta provincial election. The analysis of activity would have been noteworthy for RRM Canada if there were other communities that rivaled the main political communities in size, but were predominately unknown actors, or actors from another geographical location.

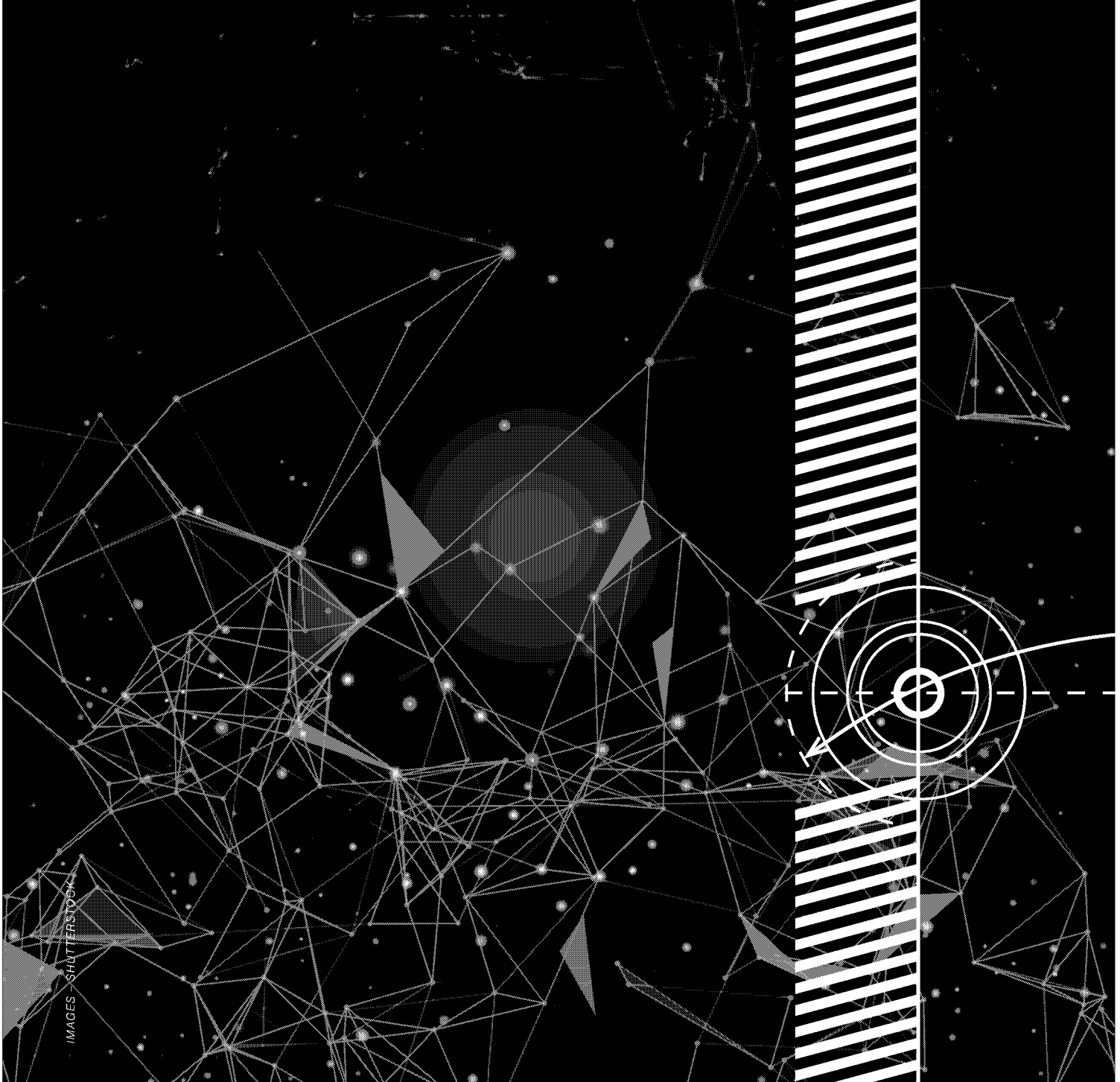


Annex B

A review of the account creation dates of accounts in the community of UCP supporters. The size of the final spike is an indicator of inauthentic activity. One indicator of bot activity is a large number of recently-created accounts. In this case, a large spike in accounts created in Q1 2019 is suggestive of inauthentic activity by either automated accounts or anonymous accounts. This combined with a qualitative evaluation of the accounts by RRM Canada, as well as their posting behaviours and the social network analysis; these are indications of likely inauthentic behaviour.







IMAGES SHUTTERSTOCK

# Hybrid Threats

A Strategic Communications Perspective



ISBN - 978-9934-564-33-8



**DISCLAIMER:**

This document is a research product of the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does not represent the opinions or policies of NATO or NATO StratCom COE.

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. The NATO StratCom COE was initially founded by Latvia, Estonia, Germany, Italy, Lithuania, Poland, and the United Kingdom in 2014. Since then Canada, Finland, the Netherlands and Sweden have joined the Centre. Denmark, France and Slovakia are set to join in 2019.

© All rights reserved by the NATO StratCom COE. Material may not be copied, reproduced, distributed or publicly displayed without permission of the originator.

# Hybrid Threats

A Strategic Communications Perspective

## Acknowledgements

### Project Director

Ben Heap

### Project Assistants

Sophia Krauel, Jente Althuis

### Research Assistants

Alexandra Clifton, Tara Flores, Leonie Haiden, Pia Hansen, Torsten Hertig

### Contributing Authors

Dr Sean Aday, Dr Māris Andžāns, Dr Una Bērziņa-Čerenkova, Dr Francesca Granelli, John-Paul Gravelines, Dr Mills Hills, Miranda Holmstrom, Adam Klus, Irene Martinez-Sanchez, Mariita Mattiisen, Dr Holger Molder, Dr Yeganeh Morakabati, Dr James Pamment, Dr Aurel Sari, Dr Vladimir Sazonov, Dr Gregory Simons, Dr Jonathan Terra

Global Influence, Hersh Consulting, Latvian Institute of International Affairs (LIIA), Norwegian Defense Research Establishment (FFI)

### With thanks to

Henrik Aagardh-Twetman, Devin Ackles, Iona Allan, Vārin Alme, Ruta Apeikyte, Uku Arold, Professor Christina Archetti, Matt Armstrong, Sebastian Bay, Andreas Beger, Gita Bērziņa, Beata Bialy, Dr Neville Bolt, Mira Boneva, Erik Brattberg, Henry Collis, Dr Patrick Cullen, Linda Curika, Thomas Frear, Lucy Froggatt, Melissa Hersh, Brady Hills, Ivars Indans, Jakub Janda, Dr Ivo Juurvee, Alise Krauja, Dr Torbjørn Kveberg, Elina Lange-Ionatamisvili, Dr Andrew Mumford, Piret Pernik, Dr Vladimir Rauta, Dr Sophie Roberts, Connor Seefeldt, Dr Antti Sillanpaa, Bernd Sölter, Zane Štāla, Jan Stejskal, Sanda Svetoka, Dr Claire Yorke, Deniss Žukovs

King's Centre for Strategic Communications, The European Centre of Excellence for Countering Hybrid Threats, European Union External Action Service

### Layout by Inga Ropsa

Media enquiries to Linda Curika: [info@stratcomcoe.org](mailto:info@stratcomcoe.org)

## About this report

### Aim

This report is the product of a research project undertaken by the NATO Strategic Communications Centre of Excellence (NATO StratCom COE), at the request of the governments of Lithuania and Estonia. The project was designed to deepen our understanding of the wide range of measures which come under the umbrella of 'hybrid threats'. Such measures aim to influence the political decision-making of a targeted nation in a way which hurts their national security interests, predominantly conducted in the 'grey zone' between peace, crisis and war.

### Scope

The project broadens the framing of current debates on hybrid threats beyond the most common empirical reference points, which tend to relate to the Russian Federation. A standardised framework is used to analyse case studies which are assessed to offer examples of hybrid threats.

Analysis has been conducted from the perspective of 'Strategic Communications', which is articulated for this report not simply as a suite of capabilities disseminating messages to explain actions or intentions in support of strategy but as a basic function of statecraft. Strategic Communications is therefore considered both as an overarching philosophy to be inculcated into organisational culture and as a cross-government process, central to integrating the instruments of national power.

The research focuses on the national level, where the primary responsibility lies for understanding, identifying and responding to hybrid threats. In this main volume, summaries of 30 cases are provided, of which a representative selection of 10 cases are analysed in detail in a separate annex. In order to limit the scope of the project, this phase of research focuses solely on state actors.

### Purpose

The case studies are not intended to be definitive accounts of a particular scenario or provide templated solutions to similar situations, nor does the inclusion of any particular state actor necessarily conclude malicious intent. The report encourages the reader to take a '360-degree view' of an issue area, deepening their knowledge of factors and considerations relevant to threat assessment.

This report is designed to help the reader develop two complementary viewpoints. First, being agile and adaptive enough to deal with emerging security challenges where the identity and intent of adversaries may be unclear or deliberately deceptive. Threats may also be constituted by the synergy of many different, apparently unconnected measures.

Second, the *Strategic Communications mindset*. This is the notion that *everything communicates*. The key to an effective strategy is therefore to understand actors and audiences, then integrate policies, actions and words across government in a coherent way to build national resilience and leverage strategic influence.

# CONTENTS

<b>EXECUTIVE SUMMARY</b>	7
Executive Summary	8
<b>A STRATEGIC COMMUNICATIONS APPROACH TO HYBRID THREATS</b>	17
About hybrid threats	18
The Strategic Communications mindset	21
Strategic Communications at the national level	22
Research approach	24
<b>KEY FINDINGS AND RECOMMENDATIONS</b>	26
10 key recommendations	27
Analysis of thematic areas	37
<b>CASE STUDY SUMMARIES</b>	47
1. RUSSIAN SNAP EXERCISES IN THE HIGH NORTH	48
2. CONFUCIUS INSTITUTES	50
3. 2007 CYBER ATTACKS ON ESTONIA	52
4. US TRANSIT CENTER AT MANAS	54
5. THE SPREAD OF SALAFISM IN EGYPT	56
6. DISINFORMATION IN SWEDEN	58
7. HAMAS' USE OF HUMAN SHIELDS IN GAZA	60
8. THE 2010 SENKAKU CRISIS	62
9. HUMANITARIAN AID IN THE RUSSO-GEORGIAN CONFLICT	64
10. CHINESE PUBLIC DIPLOMACY IN TAIWAN	66
11. DETENTION OF ESTON KOHVER	68
12. FINNISH AIRSPACE VIOLATIONS	70
13. SOUTH STREAM PIPELINE	72
14. RUSSIAN LANGUAGE REFERENDUM IN LATVIA	74
15. INSTITUTE OF DEMOCRACY AND COOPERATION	76
16. ZAMBIAN ELECTIONS 2006	78
17. SERBIAN ORTHODOX CHURCH	80
18. COMMUNIST PARTY OF BOHEMIA AND MORAVIA	82
19. BRONZE NIGHT RIOTS	84
20. RUSSKIY MIR FOUNDATION IN THE BALTICS	86
21. CRIMINAL NETWORKS IN THE DONBAS	88
22. CIVIL DISORDER IN BAHRAIN 2011	90
23. PAKISTANI INVOLVEMENT IN YEMEN	92
24. OPERATION PARAKRAM	94
25. SNAP EXERCISES AND CRIMEA	96
26. ELECTRONIC WARFARE DURING ZAPAD 2017	98
27. RUSSIAN ESPIONAGE IN SWEDEN	100
28. RELIGIOUS EXTREMISM IN THE NETHERLANDS	102
29. CYBER ATTACKS ON ROK & US	104
30. CASAS DEL ALBA IN PERU	106

# EXECUTIVE SUMMARY

# Executive Summary

This report is the result of a two-year study conducted by the NATO Strategic Communications Centre of Excellence. It is designed to help national authorities understand, prepare for, identify and respond to hybrid threats. The research focuses on state actors and uses a standardised framework to analyse 30 case studies taken from a range of geopolitical scenarios. It does so from the perspective of Strategic Communications, which is articulated not simply as a means of supporting national strategy through coordinated messaging but as a mechanism for integrating all actions taken by a government, central to both the development and implementation of strategy.

## About hybrid threats

- The final communique from the 2018 NATO summit in Brussels stated that NATO nations had “come under increasing challenge from both state and non-state actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict.”<sup>1</sup> The term ‘hybrid’ has been used to describe a wide array of measures, means and techniques including, but not limited to: disinformation; cyber attacks; facilitated migration; espionage; manipulation of international law; threats of force (by both irregular armed groups and conventional forces); political subversion; sabotage; terrorism; economic pressure and energy dependency.
- NATO defines hybrid threats as a ‘type of threat that combines conventional, irregular and asymmetric activities in time and space’.<sup>2</sup> This provides the essence of something produced by the synergy of different measures but used alone it is too broad. Most current definitions of hybrid threats lean heavily on Russian actions in Ukraine and Crimea, but this risks neglecting one of the key aspects of hybrid threats, that of **adaptability**.
- While discussions surrounding the essential nature of ‘hybridity’ are likely to continue, the underlying phenomena the term encapsulates remain very real.<sup>3</sup> This report therefore focuses on the **characteristics of hybrid threats**. These are actions which:
  - Are coordinated and synchronised across a wide range of means.
  - Deliberately target democratic states’ and institutions’ systemic vulnerabilities.
  - Use a wide range of means.
  - Exploit the threshold of detection and attribution as well as the border between war and peace.
  - Aim to influence different forms of decision-making at the local (regional), state, or institutional level.
  - Favour and/or gain the agent’s strategic goals while undermining and/or hurting the target.<sup>4</sup>
- A key aspect of hybrid threats is **ambiguity** – hostile actions that are difficult for governments to identify, attribute or publicly define because the responsible actor or overall intent is unclear or deliberately obscured.<sup>5</sup> The effects from hybrid threats can be diffuse and may only materialise over time.
- **Attribution** is ultimately a political endeavour by individual governments based on an assessment of the measures involved and an understanding of actors and their interests. It is unlikely that governments will find conclusive evidence that ‘proves’ hostile intent, or be able to publish sensitive intelligence. Threat

<sup>1</sup> “Brussels Summit Declaration, issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11-12 July 2018,” *North Atlantic Treaty Organization*, 11 July 2018.

<sup>2</sup> NATO Standardization Office (NSO), *AAP-6, NATO Glossary of Terms and Definitions* (2018 edition), 62.

<sup>3</sup> Elie Tenenbaum, “Hybrid Warfare in the Strategic Spectrum: A Historical Assessment”, in ‘*NATO’s response to Hybrid Threats*’, eds Guillaume Lasconjaras and Jeffrey A. Larsen (NATO Defense College 2017), 95-112.

<sup>4</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018), p10.

<sup>5</sup> Andrew Mumford and Jack McDonald, *Ambiguous Warfare*, report produced for the Development, Concepts and Doctrine Centre, October 2014.



assessments can differ between nations and international organisations (such as NATO or the EU) which can further hamper effective and coordinated responses.

- The way in which hybrid threats are interpreted is complex and significantly affected by **context**. For instance, an airspace violation can be regarded as either accidental or a deliberate act of provocation. Military exercises can be perceived as reassurance or deterrence and a foreign-sponsored political foundation can be seen as fostering intercultural exchange or undermining democratic values.
- The realm of hybrid threats is characterised by the interplay between information, perception, interpretation and decision-making. An appreciation of how actors and audiences interact, form opinions and make decisions should therefore be the basis of understanding the hybrid threat environment.

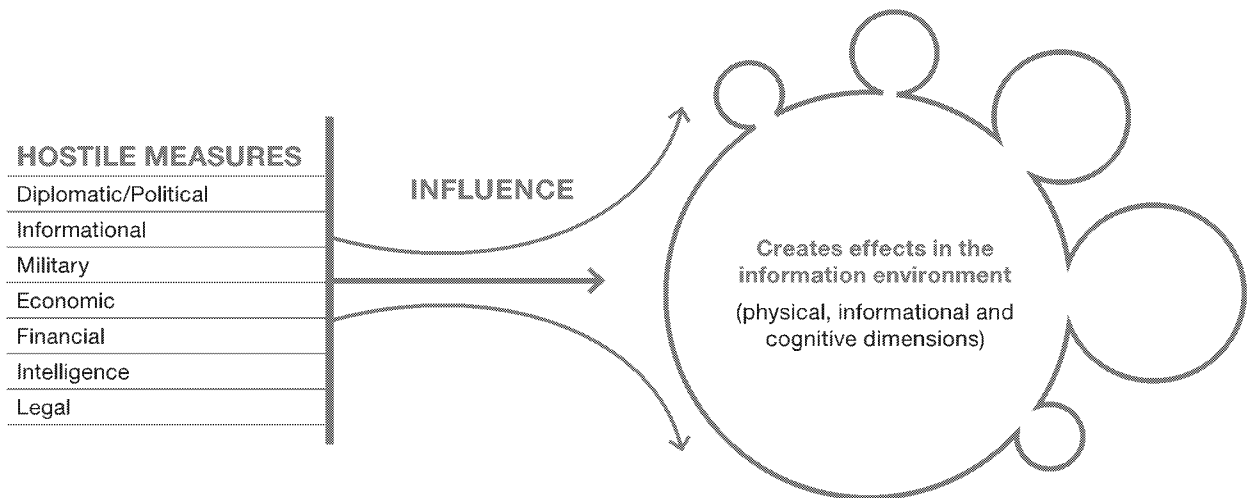
## Hybrid threats as levers of influence

- Hybrid threats have the malign intent of manipulating the **political decision-making processes** of a targeted nation by influencing the behaviours and attitudes of key audiences such as media organisations, the general public and political leaders.
- Hybrid threats can therefore be considered as **information or influence activities**. These are actions which influence audience perception and decision-making. Such activities are not limited to the 'Information' instrument but involve the combination of different instruments of power, including Diplomatic, Economic and Military.
- Understanding the way hybrid threats act as levers of influence requires a shift from focusing on the real, physical world where events and actions occur, to the conceptual realm where information exists and communication takes place. The Information Environment (IE) is a model which enables this.
- The **Information Environment (IE)** is a model for understanding how actors and audiences interact, how people see the world around them and consequently make decisions based on the meaning they deduce from it. It is a *conceptual space* consisting of three interrelated dimensions: **cognitive** (where people think, understand and decide); **physical** (individuals, organisations and infrastructure) and **informational** (facts, knowledge and data).<sup>6</sup> The IE is often used as a shorthand for the media environment but this belies its utility in offering a way to understand the interaction between all activities – ranging from military force posture to the construction of pipelines – and what they communicate to audiences.
- Analysis of the IE can help understand how hybrid threats exploit vulnerabilities, such as cultural divides or grievances, to undermine the targeted nation while benefiting the responsible actor's strategic interests. Addressing domestic issues and building societal resilience is a key component of countering hybrid threats.
- All activities undertaken by an actor affect the IE and influence decision-making in the cognitive dimension. So, while information can be an enabler *to* national power, the ability to influence audiences comes *from* the synergy of national instruments, including diplomatic, informational, military and economic measures.<sup>7</sup>
- The synergy of different hostile measures can exploit vulnerabilities across the full range of state systems of a targeted nation – political, military, economic, social, information and infrastructure (known as the PMESII spectrum).

---

<sup>6</sup> U.S. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations, incorporating change 1* (Washington D.C., 2014), 1-2.

<sup>7</sup> The standard model of the instruments of national power is DIME but in the context of hybrid threats, NATO adds Financial, Intelligence and Legal to make DIMEFIL, which is used for the analysis in this research.



## The Strategic Communications mindset

- Enabled by an understanding of the IE, Strategic Communications as a response to hybrid threats provides a holistic approach to communication, based on values and interests and encapsulating everything a nation can do to achieve strategic objectives in a contested environment.
- The term 'Strategic Communications' is often used interchangeably to refer to both the function which coordinates cross-government activities and the communications themselves. This report focuses on the former and articulates Strategic Communications as being predominantly a philosophy or *mindset* but also a *process* and a *capability*.
- To be effective, the concepts of Strategic Communications need to be endorsed as a guiding principle across all government departments and levels. This is Strategic Communications as a *mindset*, which is an appreciation that **everything – words, actions, images, policies – communicates**.
- Strategic Communications as a *process* can provide a more **effective orchestration of government activity**, integrating activities across the instruments of power to leverage strategic influence and build national resilience.
- Such a process might need resourcing with a *capability* (such as the 'Department of Strategic Communications'), to enable planning and integration of cross-government activities such as media handling, marketing and engagement. However, rather than simply establishing new, specialist structures, governments would benefit from establishing a communication culture at all levels.

## Strategic Communications at the national level

- The first step in the process of Strategic Communications is to **understand the Information Environment**. Considerations of human perception and behaviour should be central in understanding the dynamics of hybrid threats, how they are perceived, interpreted and attributed.
- Communication, including all actions, images, words and policies, should be **collective and integrated**. Every action a government takes (or does not take) communicates something, so all personnel in every department and branch are communicators.
- Actions to address hybrid threats should be guided by a **national strategy** which has consensus of support amongst the population and is endorsed from the top down by political leadership. Communication considerations should be at the centre of the development and implementation of strategy from the outset.
- National authorities need to have structures that are **flexible, decentralised and adaptive**. Hybrid threats are characterised by the synchronisation of different instruments and adaptability to context and vulnerabilities. Preparation, agility and responsiveness should be key considerations in dealing with such activities.

- Attributing hybrid threats to an adversary is a political endeavour by national governments which requires an evaluation of the geopolitical context and the strategic logic underlying adversarial measures. This assessment relies on the trust of the public. **Credibility should be protected as a vital resource.**

## Research approach

- The research attempts to broaden the discussion on hybrid threats beyond the current emphasis on the Russian Federation. It aims to assist the reader understand the factors to be considered when identifying and responding to the full range of hostile measures a nation might face.
- The project identified 250 scenarios from the end of the Cold War until the present day as potential examples of hybrid threats. A representative selection of 30 cases are analysed to understand the ways in which hybrid threats might materialise. The case studies are not intended to be definitive accounts of a particular scenario or provide templated solutions to similar situations, nor does the inclusion of any particular state actor necessarily conclude malicious intent.
- The project uses a standardised analytical framework to align the case study research and ensure comparability of the findings across the different cases. It structures the analysis according to the ways in which adversaries use different channels and means to exploit vulnerabilities and undermine the target's national security interests while advancing their strategic objectives.
- The analytical framework covers the full range of adversarial measures across the DIMEFIL continuum and tries to capture the way in which they might be synchronised and integrated to create effects.
- To understand attribution and interpretation of hybrid threats, narratives, context and an assessment of the underlying strategic logic of adversarial measures are analysed.
- The case studies are grouped together into sixteen thematic areas of threat. In accordance with the 'fog' of ambiguity that characterises hybrid activity, this is not intended to be a categorisation which can be used to objectively define different measures and means. Instead, it is meant to raise awareness for the diverse fields and channels through which hybrid threats can occur, ranging from the exploitation of ethnic identities and energy dependency to espionage and bribery.

### Thematic areas of threat

Territorial violation	Non-Government Organisations (NGOs)	Government Organised Non-Government Organisations (GONGOs)	Espionage and infiltration
Exploitation of ethnic or cultural identities	Media	Lawfare	Agitation and civil unrest
Cyber operations	Religious groups	Academic groups	Coercion through threat or use of force
Energy dependency	Political actors	Economic leverage	Bribery and corruption

- Based on the comparison of the case studies across all thematic areas, the project identified practical lessons and guidelines for decision-makers at the national level where the main responsibility lies for understanding, identifying and responding to hybrid threats. The key findings are summarised and captured in the following top ten recommendations, applying the Strategic Communications mindset to the challenge of hybrid threats.

# Summary of Key Findings and Recommendations

**The findings from this report focus on how to apply the Strategic Communications mindset to the challenge of hybrid threats.**

## **1. Everything communicates.**

All policies, actions and words influence decision-making, therefore communication should be integral to strategy and considered from the outset of planning. National authorities preparing for, and responding to, hybrid threats should appreciate that communication is not limited to words – every action (or inaction) can influence the attitudes and behaviours of key audiences. Strategic Communications is therefore not limited to certain functions and capabilities – such as public affairs and press offices – but is an organisational responsibility, with everyone working to achieve desired outcomes derived from overarching objectives.

## **2. Whole-of-government.**

Hybrid threats are generated from a mix of adversarial measures to influence political decision-making of the targeted nation, therefore an integrated approach across government is needed to effectively identify and address such threats. What works in one situation may not work in another, so governments need to be agile and able to anticipate and identify potential threats, then integrate and coordinate their response across a range of levels and channels. This requires timely decision-making and a coherent, sustained response to reinforce government credibility and legitimacy.

## **3. Understand the strategic logic.**

In order to understand an adversary's strategic logic, national authorities should grasp the underlying thinking and calculation behind adversarial measures. This entails assessing their potential aims, and the way in which different instruments are integrated and synchronised to achieve these objectives. Such an understanding would allow governments to identify potential vulnerabilities and key target audiences, anticipate future developments through horizon scanning, and adjust their preparation and response.

## **4. Determine what you want to protect and identify vulnerabilities.**

Hybrid threats deliberately target and exploit existing vulnerabilities of the target state, often opportunistically. Domestic issues such as systemic corruption and social divisions can be exploited by malign state actors. Weakness in national security institutions and a lack of public confidence in government may be seen as domestic political issues, but these vulnerabilities enhance the ability of hostile actors to affect critical functions and damage national security interests. Nations should continually assess their vulnerabilities in an honest and transparent manner and articulate this in national security policy.

## **5. Build resilience.**

Resilience describes the ability of a state and society to withstand pressure and recover from crises or shocks which may be the result of a hybrid threat. Improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost-benefit calculation. Deterrence through resilience is therefore a key component of reducing a nation's susceptibility to hybrid threats.

**6. Activity should be based on values, with clear objectives.**

Governments need to be clear about their strategic aims and ensure that statements and actions are consistent with core values. They should understand that employing measures or taking positions which appear to be deceptive or inauthentic will undermine their credibility. Democracies should also be aware that appearing to deal harshly with a suspicious actor – such as with civil society or media organisations – might provide the justification for autocratic governments to crack down on disagreeable foreign-sponsored NGOs or media outlets in their own country.

**7. Be proactive.**

A proactive approach would enable governments to maintain dominance over evolving narratives and frame events in a manner favourable to their interests. Instead of merely responding to threats as they materialise, governments should anticipate events and issues that are likely to be exploited by adversaries. This can reduce risk by not merely ‘countering’ an adversary’s activities, but pre-emptively steering public discourse in a preferred direction and building resilience, thus reducing the likelihood of unintentionally reinforcing an adversary’s preferred narrative of events.

**8. Understand the information environment.**

The ultimate purpose of any hybrid threat is to affect the political decision-making of the target nation by influencing key target audiences. Adversarial activity may be undertaken to make a political statement, alter perceptions and attitudes of the general public, degrade levels of trust and confidence in government, or create confusion and a sense of insecurity. This is why consistent, coherent and factual government communications tailored to different key audiences is crucial to maintain trust and cohesion.

**9. Learn to operate in shades of grey.**

Hybrid threats can be complex, adaptive and inflict damage on national security before they are detected. Ambiguity surrounding intent and attribution impairs decision-making and complicates effective responses. Compelling and credible evidence may not be publicly available, and so the role of government communication becomes particularly important. Official statements should be specific and coherent, capture the nuances of the situation and give enough factual, credible information to inspire public confidence in the government. Governments should not spend too much time on trying to decipher deliberately ambiguous messages and actions, but instead frame events in a manner favourable to their aims.

**10. Not every activity is a threat.**

Defining an activity as a threat and attributing it to a state actor is ultimately a political endeavour, and governments should be mindful not to inflate the threat level for political ends, either deliberately or inadvertently. As hybrid threats target a nation’s weaknesses, it is a challenge to distinguish hostile influence from legitimate social grievances or failings of the government. Policy-makers should resist the temptation to blame external actors as a convenient way of shifting blame for domestic failings. Inflating or misattributing hybrid threats can affect the government’s credibility in the long-run and risks unnecessary escalation.

# Summary of case studies

Highlighted cases are covered in detail in a separate annex.

Case Study	Thematic Area	Summary
1 Russian snap exercises in the High North	Coercion through threat or use of force	The Russian military engaged in snap manoeuvres in response to Norwegian military activity in Finnmark and the US Exercise Dragoon Ride, despite both being announced well in advance. Although the Russian snap exercise of March 2015 was not interpreted as a threat by Norway it sparked a wider debate on whether the spirit of the OSCE's Vienna Document had been breached.
2 Confucius Institutes	Government Organised Non-Government Organisations (GONGOs)	The Confucius Institute (CI) is funded by the Chinese government and has secured partnerships with universities in many NATO nations. While the CI presents itself as a non-profit educational institution, it has frequently been described as a Chinese 'soft power' instrument. The institutes' structural integration and funding arrangement with their Western partner universities have led to concern about intellectual freedom and self-censorship on sensitive issues, such as Taiwan.
3 2007 cyber attacks on Estonia	Cyber operations	The first major occurrence of cyber warfare targeted the Estonian government, media, banks and other websites in 2007. This cyber attack coincided with the relocation of the controversial Bronze Soldier Memorial. The malicious network traffic had indications of political motivation and Russian-language origin.
4 US Transit Center at Manas	Economic leverage	The US Transit Center at Manas in Kyrgyzstan was established to support Operation Enduring Freedom in Afghanistan. Being increasingly wary of the prospect of a permanent US presence in Central Asia, the Russian Federation exerted significant pressure on the Kyrgyz government, coupled with offers of economic assistance. Despite generous US lease payments and economic aid, as well as extensive outreach efforts to the Kyrgyz population, the Transit Center at Manas was closed in 2014.
5 The spread of Salafism in Egypt	Political actors; Religious groups	The Kingdom of Saudi Arabia (KSA) has long supported Salafi ideology in Egypt, particularly by funding Salafi TV channels and charities. After the 2011 revolution, Salafism developed a political arm: the Salafi Nour Party's surprising financial advantage and electoral success gave rise to much suspicion of KSA funding, especially since the party has often supported KSA-friendly policies. Support of a friendly ideology allows the KSA to counter the regional influence of the Muslim Brotherhood; dominate the interpretation of Islam; and gain influence in Egyptian politics.
6 Disinformation in Sweden	Media	<i>Sputnik</i> published an article in response to the enhancement of Gotland's defences by the Swedish military. This article misquoted senior Swedish politicians and commentators, and deliberately distorted the truth to support Russia's position. This case provides a typical example of the systematic means by which contentious debates on national security are exploited as part of wider influence strategies by pro-Russian actors.
7 Hamas' use of human shields in Gaza	Lawfare	In an attempt to counter negative opinions of their use of lethal force, in their 2014 Operation Protective Edge, the Israeli Defence Forces (IDF) used a broad range of information activities designed to encourage civilians in Gaza to evacuate from certain areas before conducting military strikes against Hamas. Hamas took advantage of this to encourage 'human shields', which temporarily put Hamas into a win-win situation by restricting the IDF's freedom of action.
8 The 2010 Senkaku crisis	Economic leverage; Territorial violation	China embargoed Rare Earth Elements (REE) following its manufactured Senkaku Crisis with Japan in 2010. A Chinese fishing vessel deliberately rammed the Japanese Coast Guard near the disputed islands, leading to the detention of the Chinese trawler captain by the Japanese. Beijing immediately demanded the captain's release and encouraged anti-Japanese protests across the Chinese mainland. This incident provided a narrative that explained why Chinese customs officials chose to embargo the REE.
9 Humanitarian aid in the Russo-Georgian conflict	Lawfare	In 2008, the Russian Federation used 'humanitarian' assets in support of the separatist populations of Abkhazia and South Ossetia, two regions of Georgia which both declared independence in the early 1990s. The Russian government used what it termed 'humanitarian assistance' as an instrument to pursue broader geo-strategic goals that were not humanitarian in nature.
10 Chinese public diplomacy in Taiwan	Exploitation of ethnic or cultural identities	China's use of public diplomacy to further its 'One China' policy towards Taiwan is addressed to two key target audiences: the Taiwanese population, where they seek to bolster support for unification, and third countries, where the aim is to isolate Taiwan. The results have been mixed: while eschewing military confrontation, it has reduced diplomatic recognition by the international community yet failed to shift Taiwanese opinion, which remains confident of US support.

11	Detention of Eston Kohver	Espionage and infiltration; Territorial violation	Eston Kohver, a member of the Estonian security service, was detained by the Russian Federation in 2014 during an operation to counter organised crime in a disputed border region; he was then portrayed as a Western spy in the Russian media. Not only did this incident risk embarrassing the Estonian government, it increased friction between different groups in the country (e.g. the far right, pro-Russians, and anti-NATO activists).
12	Finnish airspace violations	Territorial violation	From March 2014 there was a marked increase in close military encounters between Russia and NATO aligned nations. These included airspace violations, near-miss mid-air collisions and maritime encounters. In the same year NATO scrambled and intercepted more than 100 airplanes in European airspace, more than three times than it did in the previous year.
13	South Stream pipeline	Energy dependency	Western nations must balance value, reliability, and security in the provision of its energy. This tension was brought into focus by the Russian Federation's South Stream pipeline project, which offered a competitive (if less secure) alternative to the EU-proposed Nabucco Pipeline and hence threatened its viability. Moreover, it encouraged certain NATO/EU member states to contravene EU legislation by supporting South Stream.
14	Russian language referendum in Latvia	Exploitation of ethnic or cultural identities	A referendum on whether to designate Russian as an official language was held in Latvia in 2012. Although unsuccessful, it exposed – and temporarily aggravated – divisions over language, ethnicity and identity in Latvia. While the issue initially came to prominence because of a campaign by Latvian nationalists, the Russian Federation used an existing network of individuals to exploit the situation.
15	Institute of Democracy and Cooperation	Academic groups; NGOs	The Institute of Democracy and Cooperation (IDC) presents itself as an independent think tank, despite an evident bias towards the Russian Federation and antipathy towards many NATO values. Although no formal connection can be proven with the Russian state, the latter is alleged to provide funding and there are informal links with board members and directors.
16	Zambian elections 2006	Economic leverage; Political actors	The Zambian government welcomed Chinese investment in construction and mining, but a significant part of the population was unhappy with China's influence which they saw as privileged and threatening. This anti-Chinese sentiment became a pivotal issue during the 2006 presidential elections, with opposition candidate Michael Sata pledging to expel Chinese investors and making overtures to recognise Taiwan as a sovereign state. China took the position that if Sata won and established diplomatic ties with Taiwan, bilateral relations with Zambia would suffer and further investments put on hold.
17	Serbian Orthodox Church	Religious groups	The Serbian Orthodox Church has an outlook that can reasonably be described as pro-Russian; in particular, it actively organises demonstrations against the independence of Kosovo and "Western liberal values" such as LGBT rights. Most significantly, the Church can lend credibility to political messages towards Orthodox audiences, and may choose to extend such legitimacy and deploy its influence in a way more directly hostile to NATO and the NATO nations.
18	Communist Party of Bohemia and Moravia	Political actors	The Communist Party of Czechia and Moravia (KSČM) mirrors and normalises Russian narratives within the media and parliament of the Czech Republic: specifically, anti-NATO and anti-EU views are kept alive. The party encourages political radicalism and anti-system rhetoric. Two of its MPs visited the Donbas region in 2016 to lend legitimacy to Russian action in Ukraine.
19	Bronze night riots	Exploitation of ethnic or cultural identities; agitation and civil unrest	Violent protests broke out in Estonia after the relocation of the Bronze Soldier statue and the reburial of associated remains in 2007. There are radically different interpretations of the monument throughout Estonia: from the Russian perspective, the monument symbolises their victory in the Great War, while for many Estonians it represents the beginning of Soviet occupation. The riots, which resulted in the death of one Russian protester, were encouraged by Russian media and statements by Russian officials.
20	Russkiy Mir Foundation in the Baltics	Government Organised Non-Government Organisations (GONGOs)	The Russkiy Mir Foundation (RMF) is a cultural and educational institution that promotes Russian language and culture across over 100 countries. RMF has constructed a network of influencers among NATO nations, especially those bordering the Russian Federation. Such organisations are capable of activity which is hostile to the host nation and may contribute to cleavages in those societies.
21	Criminal networks in the Donbas	Bribery and corruption	Russian financial and military support for separatists in Ukraine encouraged organised criminal activity in Donetsk and Luhansk in 2014 – regions considered a safe haven for criminals. This took place alongside more familiar tactics, such as the questionable use of a referendum; unmarked soldiers of Russian origin; and encouragement of civil unrest. The consequent perception of Ukraine as a failed state threatens its territorial integrity, national security, and participation in NATO/EU structures.

22	Civil disorder in Bahrain 2011	Agitation and civil unrest; exploitation of ethnic or cultural identities	In 2011, the Kingdom of Bahrain – a majority Shia nation ruled by a Sunni minority – experienced mass protests which were inspired by the so-called ‘Arab Spring’. Some of the most prominent demands of the protesters included political reform and a stop to systematic discrimination against Shia Muslims. It is likely that deliberate agitation by Iran, particularly by way of overt public statements and media channels, contributed to the escalation. Alleged Iranian interference was used as justification by the Bahraini regime to justify repression in the following years.
23	Pakistani involvement in Yemen	Economic leverage	Pakistan’s decision not to join the Saudi-led intervention in Yemen in 2015 exemplifies a highly dynamic system of alliances and counter-alliances that Islamabad had to navigate while balancing multiple competing interests. Equilibrium was achieved in this case by stationing troops to protect the Saudi border, while refusing to deploy military force within Yemen.
24	Operation Parakram	Coercion through threat or use of force	The India-Pakistan standoff (2001–2002) was one the biggest conflicts between India and Pakistan after 1971, which had a nuclear dimension and several hybrid aspects (e.g., cross-border terrorism, Islamic radicalisation). Operation Parakram was India’s response to terrorist actions as a part of a strategy of coercive diplomacy.
25	Snap exercises and Crimea	Coercion through threat or use of force	Russian snap exercises during the annexation of Crimea were the latest in a string of exercises meant to show that the Russian Federation was ready for confrontation and to deter activity in its sphere of influence. Specifically, it was a case of ‘pressure and shield’ - pressure by indigenous insurgents, shielded by large combat ready forces across the border.
26	Electronic warfare during Zapad 2017	Territorial violation	In September 2017, parts of Latvia experienced a major cellular network outage. At around the same time, commercial aircrafts reported GPS outages while flying over Eastern Finnmark in Norway. Officials of both countries linked these incidents to Russian Electronic Warfare (EW) capabilities which were tested during the military exercise Zapad. Although experts concluded that the jamming was aimed at Russian forces during the exercise, and that spill-overs to neighbouring countries were likely unintended side-effects, officials pointed out that transparency would be desirable to avoid future misunderstandings.
27	Russian espionage in Sweden	Espionage and infiltration	According to the Swedish Security Service, Russian espionage activities in Sweden have been increasing since 2014. In many cases, attribution was not possible, not least due to the challenges attached to reporting on intelligence gathering. A crucial aspect is the (intended or unintended) information effect resulting from espionage activities: many commentators decried the development of what they consider national hysteria surrounding the issue, despite the substantial threat.
28	Religious extremism in the Netherlands	Religious groups	The Dutch intelligence and security service raised concerns in 2017 that, after being mostly stagnant for several years, the influence of extremist forms of Salafism was rising in the Netherlands. This manifested itself in an increase in hate speech and a shift from moderate Islam to fundamentalist teaching in mosques, increasing the threat of radicalisation and violence. The government needed to respond without creating a backlash against all Muslims, and transparently deal with cases of Gulf funding of religious outreach.
29	Cyber attacks on ROK & US	Cyber operations	In July 2009, tweaked versions of extant malware were used by the Democratic People’s Republic of Korea (DPRK) to execute Distributed Denial of Service (DDoS) attacks to flood certain websites in the Republic of Korea (ROK) and the United States (US) with data traffic and make them unavailable.
30	Casas del ALBA in Peru	NGOs	In 2007, Peruvian officials accused the Venezuelan government of using development aid to interfere in its domestic affairs, claiming that in concert with Bolivia, Venezuela was supporting around 58 ‘ALBA Houses’ (Casas del ALBA) in Peru. These houses provided charitable work such as literacy classes and healthcare to impoverished rural Peruvian communities. The Peruvian government argued that the ALBA Houses were promoting the Venezuelan regime, supporting left-wing extremism and inciting protests to subvert the Peruvian government.



# A STRATEGIC COMMUNICATIONS APPROACH TO HYBRID THREATS

This chapter outlines the overall approach guiding the research. It summarises the definitional challenges surrounding 'hybrid' terminology and introduces the concept of Strategic Communications as a function of basic statecraft.

## About hybrid threats

There is nothing new about the idea of using a wide range of instruments to achieve strategic ends without resorting to direct, interstate warfare.<sup>1</sup> Yet the character of warfare continues to evolve – the ongoing information revolution being a significant factor – offering adversaries new opportunities to exploit the spectrum of conflict beyond the utility of force.<sup>2</sup>

NATO understands the need to adapt and address these new modes of geopolitical rivalry but formulating distinctions has proven problematic. This is reflected in the variety of contexts that ‘hybrid’ terms are used in political discourse and the research community’s continued discussions regarding its essential nature.<sup>3,4</sup> Since being introduced to the lexicon of security and defence, the definitions of hybrid ‘threat’ and its close relations ‘war’ and ‘warfare’ have changed in tandem with the conflicts they have been used to describe.<sup>5,6</sup> Despite intense academic inquiry and widespread usage of the terms in NATO and national strategies, a consensus definition of ‘hybridity’ remains elusive.<sup>7</sup> This does not necessarily mean that the term should be abandoned, or that addressing the problem should be delayed until the labels are agreed upon. Despite the lack of conceptual clarity in definitions, the underlying phenomena the term encapsulates remain very real and a matter of urgent concern for the NATO nations.<sup>8</sup>

NATO defines hybrid threats as a ‘type of threat that combines conventional, irregular and asymmetric activities in time and space’.<sup>9</sup> This provides the essence of something produced by the synergy of different measures but used alone it is too broad. Most current definitions of hybrid threats lean heavily on Russian actions in Ukraine and Crimea, but this risks neglecting one of the key aspects of hybrid threats: adaptability. Hybrid threats do not follow a set pattern, and can be generated by a wide range of actors creatively using whatever means and measures available to achieve their strategic objectives. The adversary prefers to stay short of the threshold of conventional warfare but may eventually resort to the direct application of force. It should be expected that future threats will evolve in this way, with adversaries tailoring their means and measures to a targeted nation’s vulnerabilities.

A lack of conceptual clarity has meant that discussions over the nature of hybridity often become mired in narrow and outdated views of conflict, with the terms becoming merely an endeavour of political rhetoric, being ‘exaggerated, demonised and mobilised’ for political purposes.<sup>10</sup> This report takes a pragmatic approach which accepts a degree of conceptual obscurity but addresses the underlying security issues by focusing on the *characteristics* of hybrid threats. For the purposes of this research, hybrid threats are actions which:

- Are coordinated and synchronized
- Deliberately target democratic states’ and institutions’ systemic vulnerabilities.
- Use a wide range of means.
- Exploit the thresholds of detection and attribution as well as the border between war and peace.
- Aim to influence different forms of decision-making at the local (regional), state, or institutional level
- Favour and/or gain the agent’s strategic goals while undermining and/or hurting the target.<sup>11</sup>

Hybrid threats, by their very nature, are about creating effects that influence political decision-making. These effects can be diffuse, developing over a long period of time and not noticeable until it is too late. This ambiguity means that they can be difficult for governments to identify, attribute or publicly define because the responsible actor, or overall intent, is unclear or deliberately obscured.<sup>12</sup> Such activity is often described as taking place in the ‘grey zone’ between peace, crisis and war. It is often unlikely that governments will find ‘smoking gun’ evidence that provides credible and compelling proof of hostile intent, or be able to publish sensitive intelligence to support their analysis.

The way in which hybrid threats are interpreted and attributed is complex and significantly affected by context. For instance, an airspace violation can be regarded as either accidental or a deliberate act of provocation. Military exercises can be perceived as reassurance or deterrence and a foreign-sponsored political foundation can be seen as fostering intercultural exchange or undermining democratic values. These interpretations lead

to threat assessments that shape attitudes among publics and government officials alike. The judgement of whether an activity is considered hostile is ultimately a political decision taken by individual nations, with each nation seeing threats differently based on their own experience. This creates a challenge for how international organisations such as NATO and the EU should respond.

The realm of hybrid threats is therefore characterised by the interaction of information, perception, interpretation, and decision-making. An appreciation of how actors and audiences interact, form opinions and make decisions should therefore be the basis of understanding the hybrid threat environment.

## Hybrid threats as levers of influence

An inherent characteristic of any hybrid threat is a malicious intent to influence the attitudes and behaviours of key audiences, such as populations and political leaders. Mastering the dynamics of these levers of influence provides the basis for any government wishing to develop an effective strategy to protect their security interests and project power. Understanding this system requires a shift from focusing on the real, physical world, where events and actions occur, to the conceptual realm where information exists and communication takes place. This means placing less emphasis on 'real' domains such as land, sea and air, and adopting an approach which gives primacy to understanding actors, information and audiences, of which the physical world is one component. Such an approach would need to enable the analysis of a wide range of subjects, from energy dependency to military exercises.

To provide such a framework, this report proposes that hybrid threats be viewed as 'information' or 'influence' activities. These are actions which influence decision-making by creating changes in the conceptual system known as the *Information Environment* (IE). This is a term which is often used to refer to just the media environment but this belies the utility of it as a way of understanding how all actions (and non-actions) can influence decision-making. The IE is not, as many might understand it, a separate realm of contestation – changes in the IE influence physical actors and systems and vice versa.<sup>13</sup> The IE is a *conceptual space* consisting of three interrelated dimensions: **cognitive** (where people think, understand and decide); **physical** (individuals, organisations and infrastructure) and **informational** (facts, knowledge and data).<sup>14</sup> By this definition there is no limit on the IE and as it does not conform to spatial boundaries it is difficult to conceptualise both visually and verbally.<sup>15,16</sup> In essence the IE is a model for understanding how actors and audiences interact, how people see the world around them and consequently make decisions based on the meaning they deduce from it. Political leaders often instinctively think this way, such as when they refer to deterrence and reassurance measures. It is commonplace for actions to be described as 'sending a message' or a 'strong signal' but what is often lacking is a framework for placing such activities in the broader context of national strategy and integrating them with other measures in a coherent way.

Using the IE as a system to understand adversaries and the audiences they are likely to target is a departure from a more traditional approach which emphasises actions in the physical dimension with information as an afterthought. This challenges the 'DIME' model of national power (Diplomatic, Information, Military, Economic) which places 'Information' as a separate and apparently equal instrument.<sup>17</sup> All activities undertaken by an actor affect the IE and influence decision-making in the cognitive dimension. So, while information can be an enabler *to* national power, the ability to influence audiences comes *from* the synergy of national instruments, including diplomatic, military and economic measures. If these instruments are coordinated and work together harmoniously to achieve strategic objectives, the chances of success are increased and the less risk is assumed. The principles of Strategic Communications can enable this integration by understanding how hybrid threats affect the IE, then in response orchestrating statecraft in a manner that transcends traditional ministerial domains.

## Considerations for the different characteristics of hybrid threats

Characteristics	Description	Considerations
Coordinated and synchronised across a wide range of means.	<ul style="list-style-type: none"> <li>■ Activity which involves all instruments of national power: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal.</li> <li>■ Mixture of overt and covert, military and non-military, conventional and unconventional means; can involve state and/or non-state actors such as criminal groups and extremist organisations.</li> <li>■ Threats can be the result of a combination of different measures which create synergistic effects.</li> </ul>	<ul style="list-style-type: none"> <li>■ Nations should have the ability to continually monitor the Information Environment (IE), identify the use of measures and the reach and effect they have on key target audiences.</li> <li>■ A cross-government effort is needed to identify patterns and changes in adversarial behaviour.</li> </ul>
Deliberately targets democratic states' and institutions' systemic vulnerabilities.	<ul style="list-style-type: none"> <li>■ Vulnerabilities are weaknesses in a nation's system which can be political, military, economic, social, informational or infrastructure-related.</li> <li>■ Vulnerabilities can range from domestic shortcomings in security, infrastructure, or public goods and services, to social vulnerabilities such as cultural fracture lines or grievances.</li> </ul>	<ul style="list-style-type: none"> <li>■ Vulnerabilities should be continually assessed and addressed across the full range of critical functions.</li> <li>■ Build resilience with a whole-of-society approach, including civil society, private sector, media organisations, NGOs, think tanks.</li> <li>■ Nations should be aware that their relationship with other states may be the target.</li> </ul>
Exploits the thresholds of detection and attribution as well as the border between war and peace.	<ul style="list-style-type: none"> <li>■ Attribution of responsibility can be challenging, and the degree of state involvement may be unclear.</li> <li>■ Thresholds of war and peace can be stretched depending on context.</li> <li>■ Blurred lines between peace and conflict and between normality and crisis hamper identification and attribution.</li> </ul>	<ul style="list-style-type: none"> <li>■ Attribution is a political endeavour.</li> <li>■ Attribution should be done on a case-by-case basis and relies on government credibility to be convincing.</li> <li>■ Importance of legal domain in supporting arguments.</li> <li>■ Attribution and monitoring should not impede free speech.</li> </ul>
Aims to influence different forms of decision making at the local (regional), state, or institutional level.	<ul style="list-style-type: none"> <li>■ Can target public opinion or officials on the local or national level.</li> <li>■ Local / municipal level institutions can be especially vulnerable as they often do not receive the same attention as national issues.</li> <li>■ Exploits lack of accountability and transparency or poor governance.</li> </ul>	<ul style="list-style-type: none"> <li>■ Governments should build resilience at all levels of government through awareness building and training.</li> <li>■ Vulnerability assessments need to be comprehensive and conducted on a regular basis.</li> <li>■ Identify potentially vulnerable target audience groups and plan resilience strategies accordingly.</li> </ul>
Designed to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.	<ul style="list-style-type: none"> <li>■ Hybrid activity may be used to directly achieve strategic objectives, but may not necessarily be an end in itself; it may serve to generate influence by investing in actors or networks.</li> <li>■ Aimed at changing the behaviour or attitudes of the government or population in a way that damages national security interests.</li> </ul>	<ul style="list-style-type: none"> <li>■ Understand the overall strategic logic of adversaries.</li> <li>■ Attribution needs to be clear and supported by the maximum amount of releasable information or intelligence.</li> </ul>

# The Strategic Communications mindset

'Strategic Communications' (and Strategic Communication) is a label which is applied to different, yet related functions. It can be used to refer to both the internal machinery that coordinates cross-government communication activities and the communications themselves. This report focuses on the former and for simplicity suggests a generic definition of Strategic Communications as the 'coordination of actions, words and images to influence the behaviour and attitudes of key audiences to achieve strategic goals.'<sup>18</sup> It is understood predominantly as a *mindset* but also as a *process* and a *capability*.<sup>19</sup>

The boundaries between the different facets of Strategic Communications are blurred and this is reflected in the ongoing debate as to whether Strategic Communications should be considered as the "communication of strategy, or communication as strategy".<sup>20</sup> In the former, the role of communication is limited to the implementation of strategy, in a predominantly subordinate role. The strategists decide on the strategy and then coordinated activities such as press conferences and media campaigns message in support, typically as a reactionary measure in times of crisis. It is in this context of a coordination *capability* that policy-makers refer to 'getting the right message out' and 'counter-narratives'. Yet this perspective neglects the ways in which every government activity communicates, including actions, words and policies.

By contrast, communication as a primary instrument of strategy is considered as an integral part of government decision-making from the outset and placed at the heart of strategy development. Strategic Communications when applied as a *process* enables this by focusing on audience insight and providing a unifying lens to understand the full array of adversarial measures, how they are interpreted, affect perceptions and influence decision-making. This forms the basis of a response which incorporates all available means and ways to build societal resilience, forge international coalitions and attribute threats effectively.

The process of Strategic Communications can therefore provide a more effective orchestration of government activity to drive and coordinate decision-making in a way favourable to the national interest. It needs to be endorsed as a guiding principle across all government departments and levels in order to be practiced efficiently. This principle is encapsulated in the articulation of Strategic Communications as a philosophy or *mindset*. This is an appreciation that everything communicates, therefore everyone in government is responsible for what is being communicated.

The application of Strategic Communications as a process can act as the connecting membrane between strategy and action, integrating efforts across government and enabling unity of effort towards common strategic ends. Such an approach would maximise the use of available resources and reduce the risk of failure. This requires a Strategic Communications mindset absorbed into all levels of government and views foreign policy through the lens of communication, identifying relevant audiences and understanding how they form opinions and make decisions. There will inevitably be specialist capability requirements, such as assessment and analysis of the IE, or the planning and integration of cross-government activities such as media handling, marketing, and engagement. However, rather than assigning the responsibility of Strategic Communications to a single entity, governments would benefit from fostering a culture that communication is core business.<sup>21</sup> In this way, when the mindset is stronger, less process is required.<sup>22</sup>

In practice, these two approaches – communication at the core of strategy development or subsequently in the implementation phase – are not mutually exclusive. They are often integrated to varying degrees, either deliberately or as a characteristic of how governments function. This is reflected in the balance that governments need to find between expanding their pool of specialist communications capabilities and encouraging a Strategic Communications culture which is integral to every department, policy and strategy.<sup>23</sup>

# Strategic Communications at the national level

This report does not propose that those working in the field of Strategic Communications at the national level make a bid to take over the functions of government that define the means and ways of strategy. It proposes that every hybrid threat can be considered as an act of communication, ultimately influencing political decision-making in a way which benefits the adversary and hurts the targeted nation. The underlying concepts and principles of Strategic Communications can therefore provide a useful guide to effective statecraft in understanding, identifying and countering hybrid threats.

The most important principle that underpins Strategic Communications is the requirement to **understand the Information Environment**. Considerations of human perception should be central in understanding the dynamics of hybrid threats, how they are perceived, interpreted and attributed. It is clearly not feasible to consider the entirety of the IE, therefore analysis should be focusing on relevant topics and on the constituent parts of a hybrid threat: *actors* (political leaders, civil society, military), *channels* (military, information, law, cyber, economy) and *means* (disinformation, cyber attacks, bribery) and understanding how these might exploit vulnerabilities to damage national security interests. Continuous assessment should establish baselines of normality and identify changes in patterns. This demands information sharing both within and between governments and the ability to synthesise different types of intelligence and information. Implicit in any assessment of the IE is the ability to assess the effectiveness of government activities to inform adjustments to strategy.

Communication should be a whole-of-government activity which is **collective and integrated**. Based on a comprehensive understanding and continuous assessment of the information environment, governments should have a clear understanding of what measures and means are available to reach key audiences. This could be anything from economic sanctions to a change in military force posture. These should be integrated and employed in a coherent manner to achieve desired strategic effects and outcomes.

Actions taken to address hybrid threats should be guided by a **strategy**. Communications considerations should be at the centre of the development and implementation of strategy from the outset and this process should be supported by the availability of appropriate resources, particularly qualified personnel. National strategy should have a broad consensus of support amongst the population and be endorsed from the top down by political leadership. This includes formulating the strategic position a nation wishes to take and how it intends that to be articulated across the whole of government, including ministries such as culture, education and home affairs. Such an approach ensures that whatever 'story' (or national narrative) the government wishes to communicate is empowered at all levels, coherent and consistent.

National authorities need to have structures that are **flexible, decentralised and adaptive** and able to emphasise preparation, agility and responsiveness. The nature of hybrid threats means there are no set playbooks or manuals that can be followed. Adversaries will continue to develop, test and employ measures that target vulnerabilities wherever they materialise. Rather than establishing formal structures, fostering a culture of Strategic Communications across all government departments will allow a nation to retain the initiative.

Attributing hybrid threats to an adversary is a political endeavour which relies on the trust of the public, so **credibility should be protected as a vital resource**. Any government action which needlessly erodes public confidence will limit the courses of action available to both prepare and respond to hybrid threats. Government branches should understand that even if there is no obvious connection between their particular area of responsibility and national security, their actions can weaken national resilience.

---

#### Endnotes

- <sup>1</sup> For background and examples see Frank G. Hoffman, "The hybrid character of modern conflict", in *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict*, Council for Emerging National Security Affairs (2011). Kindle version, locn 716.
- <sup>2</sup> For an overview see Bruce D. Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology* 12, no.1 (1995), 59–66.
- <sup>3</sup> Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism. The Journal of Complex Operations* 7, no. 4 (2018), 31-47.
- <sup>4</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018).
- <sup>5</sup> Most scholars attribute the term to William J. Nemeth in *Future War and Chechnya: A Case for Hybrid Warfare* (Monterey: Naval Postgraduate School, 2002).
- <sup>6</sup> Patrick Cullen and Erik Reichborn-Kjennerud, *Countering Hybrid Warfare Baseline Assessment* (Multinational Capability Development Campaign (MCDC) 2015-2016, October 2016), 5.
- <sup>7</sup> Ibid.
- <sup>8</sup> Elie Tenenbaum, "Hybrid Warfare in the Strategic Spectrum: A Historical Assessment". Chapter in 'NATO's response to Hybrid Threats', eds Guillaume Lasconjarías and Jeffrey A. Larsen (NATO Defense College 2017) p112.
- <sup>9</sup> NATO Standardization Office (NSO), AAP-6, *NATO Glossary of Terms and Definitions* (2018 edition), 62.
- <sup>10</sup> Benjamin Tallis and Michal Šimečka, *Collective Defence in the Age of Hybrid Warfare* (Prague: Institute of International Relations, 2016).
- <sup>11</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018), p10.
- <sup>12</sup> Andrew Mumford and Jack McDonald, *Ambiguous Warfare*, report produced for the Development, Concepts and Doctrine Centre, October 2014.
- <sup>13</sup> Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* (Santa Monica: RAND Corporation, 2018), ix.
- <sup>14</sup> U.S. Joint Chiefs of Staff, Joint Publication 3-13: Information Operations, incorporating change 1 (Washington D.C., 2014), 1-2.
- <sup>15</sup> Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 253.
- <sup>16</sup> Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* (Santa Monica: RAND Corporation, 2018), 3..
- <sup>17</sup> The UK, for instance, defines only three instruments of power – diplomatic, military and economic – with information considered as an enabler for all of them (see UK Ministry of Defence (MOD), *Joint Doctrine Note 1/12: Strategic Communication: The Defence Contribution* (Swindon: The Development, Concepts and Doctrine Centre, MOD, 2012). NATO Standardization Office (NSO), AJP-01, NATO Allied Joint Doctrine (February 2017) considers information as a separate instrument and says StratCom is 'delivered through the instruments of power via policy, words and actions is an important element of operations planning and execution', 1-3.
- <sup>18</sup> Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates* (Santa Barbara: Praeger, 2011).
- <sup>19</sup> For more on this see Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016; Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates* (Santa Barbara: Praeger, 2011) and UK Ministry of Defence (MOD), *Joint Doctrine Note 1/12: Strategic Communication: The Defence Contribution* (Swindon: The Development, Concepts and Doctrine Centre, MOD, 2012).
- <sup>20</sup> Kenneth Payne, "Thoughts on the Psychology of 'Strategic Communication,'" Paper presented at the KCL Insurgency Research Group and CIWAG US Naval War College Conference, 'Strategic communications: the Cutting Edge,' 10 May 2011.
- <sup>21</sup> Paul Cornish, Julian Lindley-French and Claire Yorke, *Strategic Communications and National Strategy: A Chatham House Report* (London: Chatham House, The Royal Institute of International Affairs, September 2011).
- <sup>22</sup> Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 276
- <sup>23</sup> Paul Cornish, Julian Lindley-French and Claire Yorke, *Strategic Communications and National Strategy: A Chatham House Report* (London: Chatham House, The Royal Institute of International Affairs, September 2011).

# Research approach

**Problem statement.** The start point for this research is a requirement for NATO nations to better understand and counter the broad range of threats they face from state actors, which sit in the low-intensity, indirect end of the spectrum of influence. Such threats, in certain circumstances, may be a precursor to the use of conventional military force but are predominantly characterised by the use of different instruments to undermine and weaken the governing authority without resorting to open conflict. National authorities therefore require the ability both to identify when such threats materialise and to integrate and coordinate all measures available in response.

**Purpose.** This publication provides the first large-scale systematic analysis of hybrid threats, covering a wide spectrum of different methods of influence, across a range of geographic regions. It broadens the framing of most previous research beyond the common empirical reference points relating to the behaviour of the Russian Federation. The findings and recommendations aim to assist decision-makers, practitioners and policymakers working at the national level develop an effective approach to prepare for, identify and respond to hybrid threats which is based on the underlying concepts of Strategic Communications.

**Selection of case studies.** Initial research identified over 250 scenarios assessed as featuring activity which was potentially an example of a hybrid threat. These activities may have impacted national security interests by exploiting a vulnerability and affecting a nation's critical functions, i.e. by weakening the military, economic or political strength of a governing authority. The inclusion of an actor in a scenario does not necessarily mean that their actions were intended to be hostile. Part of the research was therefore to interrogate this proposition of hostility and also accept that the results may not necessarily be conclusive.

**Analysis of case studies.** With over 250 scenarios identified, this research is based on a large selection of case studies. However, ambiguity as a key characteristic of hybrid threats impedes a quantitative analysis. The research methodology employs a mixed-methods qualitative approach. Individual case studies have been conducted by experts in the respective regions with the necessary language skills and background information. The researchers conducted interviews with subject matter experts and all case studies have been peer-reviewed. To ensure the comparability of the findings, a standard analytical framework, developed through a series of workshops, has been applied. The different components of the analytical framework cover the analysis of contextual factors, key actors, themes and narratives as well as the range of measures employed, their underlying strategic logic and the potential impact of these activities on national security interests.

**Categorisation of case studies.** Sixteen areas of thematic threat were identified to group case studies together for analysis. The thematic areas are designed as a typology to serve as a framework to help understand the wide range of means and ways that hybrid activity can manifest itself – military and non-military, conventional and unconventional, overt and covert, state and non-state. The thematic areas often overlap, as hostile influence usually involves more than one thematic area.



# OVERVIEW OF ANALYTICAL FRAMEWORK

## CONTEXT

This section provides an overview of background knowledge that needs to be understood in order to appreciate narratives and actor behaviour against the background of broader historical and political developments relevant to the case.

## ACTORS AND NARRATIVES

This section identifies key actors and looks at the core themes and narratives of all parties involved.

## MEASURES

This section looks at all measures employed by an adversary, and the strategic logic behind the application of different instruments of power.

The **STRATEGIC LOGIC** describes the underlying thinking and calculation of adversarial measures. Different measures are broken down into functional components according to the DIMEFIL spectrum: diplomatic, information, military, economic, financial, intelligence and legal.

**Diplomatic.** The principal instrument for engaging with other states and foreign groups to advance values, interests, and objectives, and to solicit foreign support. The credible threat of force reinforces, and in some cases enables the diplomatic process.<sup>1</sup>

**Information.** Information remains an important instrument of national power and a strategic resource critical to national security.<sup>2</sup>

**Military.** The use of military capabilities, predominantly through coercion generates effects through the application of force (to include the threat of force) to compel or deter an adversary. The military also has capabilities that can be used in non-conflict situations.<sup>3</sup>

**Economic.** The use of economic inputs and flows to influence decision-making.<sup>4</sup>

**Financial.** The control of the creation, flow, and access to "stores of value" wields power. Although finance is generally an operation of real and virtual currency, anything that can serve as a "medium of exchange" provides those who accept the medium with a method of financial transaction.<sup>5</sup>

**Intelligence.** Intelligence, as an instrument of national power provides the national leadership with the information needed to realise national goals and objectives while providing military leadership with the information needed to accomplish missions and implement national security strategy. Planners use intelligence to identify the adversary's capabilities and centres of gravity.<sup>6</sup>

**Legal.** The attitude of the population, degree of control provided by competing (non-state government) enforcers of law, and traditions of civic order – or lack thereof – are key components of the overall law enforcement environment. All of these varying conditions will contribute to the degree of lawlessness in any given society.<sup>7</sup>

## NATIONAL SECURITY INTERESTS

This section looks at the outcomes and effects of adversarial measures. This is a series of lenses to facilitate a '360 degree' view of a situation and to assess any impact of adversarial measures. Consideration is given to the different levels (local, regional, national) at which effects are assessed to have occurred. The main area of focus is the effects section, particularly on political decision-making, public opinion and the development of themes and narratives.

A **critical function** is something that the nation is trying to protect or sustain. Critical functions are activities or operations distributed across the PMESII spectrum which if affected could lead to a disruption of services that a working system such as a state and its society depends on. Critical functions can be broken down into a combination of actors, infrastructures (such as national power grids) and processes (for example legal, technical, political).<sup>8</sup>

A **vulnerability** in a critical function presents an adversarial actor with a possible condition for exploitation, depending on the means at its disposal.<sup>9</sup> Any factors associated with a weakness in the critical function of a nation may be considered a vulnerability. Vulnerabilities can therefore be anything from lack of public trust in the government to high reliance on technology.

A **threat** is anything that can exploit a vulnerability and achieve an effect or effects on a critical function. A threat to national security is an action or a sequence of events that 1) threatens drastically and over a relatively brief span of time to degrade the quality of life for inhabitants of a state or 2) threatens significantly to narrow the range of policy choices available to the government of a state, or to private, non-governmental entities (persons, groups, corporations) within the state. A threat is what the nation is trying to protect against.

An **effect** is a change in behaviour or state of a system and is the outcome or impact of a threat. Describes short term effects on target(s) behaviour. Assessing this change requires a baseline or status quo for comparison. Where possible, longer term effects are considered.

<b>Political.</b> Relating to the distribution of responsibility and power at all levels of governance – both formally constituted authorities and informal or covert political powers.	<b>Military.</b> Relating to the military and paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given environment.	<b>Economic.</b> Individual and group behaviours related to producing, distributing, and consuming of resources.	<b>Social.</b> The cultural, religious, and ethnic makeup within a bounded environment and the beliefs, values, customs, and behaviours of society members.	<b>Information.</b> Describes the nature, scope, characteristics, and effects of individuals, organisations, and systems that collect, process, disseminate, or act on information.	<b>Infrastructure.</b> The basic facilities, services, and installations needed for the functioning of a community or society.
--	--	---	--	--	---

<sup>1</sup> "Instruments of National Power," *The Lightning Press*, website accessed 29 October 2018.

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

<sup>4</sup> US Headquarters Department of the Army, *Army Special Operations Forces Unconventional Warfare*, September 2008.

<sup>5</sup> Ibid.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Patrick J. Cullen and Erik Reichborn-Kjennerud, *Understanding Hybrid Warfare*, Multinational Capability Development Campaign Project, January 2017.

<sup>9</sup> Ibid.

# KEY FINDINGS AND RECOMMENDATIONS

This chapter presents the main lessons identified from the research. The findings are cross-referenced to the 30 case studies that follow. This chapter also outlines a typology of different threats.

# 10 key recommendations

## 1. Everything communicates

**All policies, actions and words influence decision-making, therefore communication should be integral to strategy and considered from the outset of planning. National authorities preparing for, and responding to, hybrid threats should appreciate that communication is not limited to words – every action (or inaction) can influence the attitudes and behaviours of key audiences. Strategic Communications is therefore not limited to certain functions and capabilities – such as public affairs and press offices – but is an organisational responsibility, with everyone working to achieve desired outcomes derived from overarching objectives.**

Communication is not just what is said. Images, actions and policies all have an information effect. Actions – both your own, and those of an adversary – can be perceived to ‘send a message’, intended or not. Decision-makers need to recognise the importance of integrating communication into planning from the outset, and be adequately supported and trained by experienced communications practitioners.

- Military force posture and presence can achieve strategic information effects such as deterrence, reassurance or disruption: *Operation Parakram (24), Snap exercises and Crimea (25)*
- When an adversary government does not react to accusations of hostile or disruptive activity, this can imply hostile intent, especially when silence is deliberately used to increase uncertainty and confusion: *Electronic warfare during Zapad 2017 (26)*
- High-profile responses, such as formal investigations into hostile activities, can send a strong political statement and build resilience by deterring malign influence: *Casas del ALBA in Peru (30)*

**Audience insight.** Care must be taken to understand the diversity of audiences, their attitudes, values, motivations and – importantly – where their trust lies. Nations should adequately resource target audience analysis and invest in personnel with language skills and in-depth knowledge of history, religion and cultural norms. This knowledge should be applied to monitoring and analysis, and used to support Strategic Communications planning and the development of credible and resonant narratives.

- Efforts to change audience attitudes and behaviours can be more persuasive and cost-effective when organisations have an in-depth understanding of the issues that people really care about: *US Transit Center at Manas (4)*

**The messenger matters.** Whether a message is promoted by high-ranking politicians, subject-matter experts, academics, celebrities, or religious leaders has a profound effect on how the message is interpreted by an audience. Similarly, the medium chosen for the message – be it an online awareness campaign, a political speech, or a movie – can change the impact of a message. Audience insight is crucial to understand how different messengers might change the way in which a message is interpreted, which specific key groups hold the balance on opinions, and which information channels are the most used and trusted.

- In cases where official channels are likely to have a minimal effect on key audiences, governments should identify and work together with civil society groups that might be more effective messengers: *Religious extremism in the Netherlands (28)*

## 2. Whole-of-government

Hybrid threats are generated from a mix of adversarial measures to influence political decision-making of the targeted nation, therefore an integrated approach across government is needed to effectively identify and address such threats. What works in one situation may not work in another, so governments need to be agile and able to anticipate and identify potential threats, then integrate and coordinate their response across a range of levels and channels. This requires timely decision-making and a coherent, sustained response to reinforce government credibility and legitimacy.

**Work across departments.** To identify and counter hostile measures from malign actors, responses need to be coordinated across government and span the civil-military divide. Different branches of government should establish mechanisms for effective cooperation and use synergies to their full potential.

- Identifying and countering potential threats requires the ability to assess adversarial activity across the full spectrum of military and non-military means to understand an adversary's overall objectives: *US Transit Center at Manas (4)*, *The 2010 Senkaku crisis (8)*, *Bronze night riots (19)*
- Lack of information sharing and cooperation between civilian and military authorities limits the government's ability to effectively determine and pursue its objectives: *Operation Parakram (24)*
- Preparation for disruptive events, such as cyber attacks, should focus on credible, factual responses consistent across national authorities, stressing civil preparedness: *Electronic warfare during Zapad 2017 (26)*

**Empower and enable all levels.** Responsibility for communication does not only lie with high-level officials and spokespeople: in today's fast-paced and networked media environment, statements by regional officials and even by low-ranking soldiers on the ground can be influential or be exploited by hostile actors to legitimise a specific point of view. Governments should consider training officials to refrain from making statements which undermine the overarching narrative, and to be mindful of the impact their individual actions and statements might have.

- Improving awareness of information-based threats and developing media presentation skills through training across government and at the lowest levels of national authorities will help officials make statements that are not open to misinterpretation: *Disinformation in Sweden (6)*

**Consistency.** Aligning words and deeds is of fundamental importance for coherent government messaging. Inconsistent messaging due to a lack of strategy, poor coordination, or attempts to cater to different audiences, can result in a say-do gap which undermines an actor's overall credibility. Messaging (including actions) across national authorities, while tailored to address specific audiences, should consistently reflect overarching themes.

- When information from different official channels contradicts each other, this fundamentally affects trust in government communication and leaves room for doubt and alternative interpretations: *Civil disorder in Bahrain 2011 (22)*
- Balancing competing demands of domestic and international audiences can result in information fratricide, especially when words are not aligned with actions: *Pakistani involvement in Yemen (23)*
- When two or more countries face similar or identical hybrid threats, efforts to align narratives and coordinate approaches would help present a unified front: *Cyber attacks on ROK & US (29)*

### 3. Understand the strategic logic

In order to understand an adversary's strategic logic, national authorities should grasp the underlying thinking and calculation behind adversarial measures. This entails assessing their potential aims, and the way in which different instruments are integrated and synchronised to achieve these objectives. Such an understanding would allow governments to identify potential vulnerabilities and key target audiences, anticipate future developments through horizon scanning, and adjust their preparation and response.

**Long-term aims of adversary.** Taking a '360 degree' approach will help decision-makers situate an activity within larger systematic efforts and strategies, and shed light on an adversary's underlying motivations and goals. By monitoring activities across the full spectrum of adversarial measures, decision-makers will be able to identify how the adversary's aims and information activities align and gauge their success or failure. Once the overall strategic logic is better understood, decision-makers will be able to better develop their strategy accordingly.

- An adversary's long-term goals may be unclear (they might not even be clear to the adversary). Hybrid activity often operates opportunistically and may not have any specific immediate objective other than generating influence in another country by investing in the potential of actors and networks: *Ruskiy Mir Foundation in the Baltics (20)*

**Modus operandi and toolkit of adversary.** Governments should have a thorough understanding of their adversary's capabilities and methods, to develop knowledge of how potential threats fit within their existing toolkit and serve their long-term aims. This includes looking at historical patterns of behaviour, analysing where an adversary might be testing defences, and identifying actors with aligned interests that the adversary could employ as agents or useful allies.

- Examining whether a specific tool – such as ambiguous cyber operations, or the providing of 'humanitarian' assets – has been used systematically by a state actor in different contexts and against different countries can be of use when trying to determine hostile intent: *2007 cyber attacks on Estonia (3), Humanitarian aid in the Russo-Georgian conflict (9)*
- Hybrid threats are often opportunistic. A typical approach might be to create pressure or intensify social divides, and then take advantage of crises once they emerge. Similarly, a small uncalculated incident might be exploited and deliberately escalated into an international incident for strategic gain: *The 2010 Senkaku crisis (8), Bronze night riots (19)*
- Potentially hostile civil society groups are often modelled on Western cultural institutions and soft power approaches, but might be aimed at undermining the cohesion of the host nation: *Institute of Democracy and Cooperation (15), Ruskiy Mir Foundation in the Baltics (20)*

**Identify potential key target audiences for adversarial activity.** Understanding the strategic logic and aims of adversaries will enable decision-makers to better anticipate the potential target audiences of their activities. It is also important to consider that the primary target audience may be local to the hostile actor, such as domestic public opinion.

- Decision-makers should identify actors with aligned interests who could be used by an adversary as agents, channels or mouthpieces: *Serbian Orthodox Church (17)*

## 4. Determine what you want to protect and identify vulnerabilities

Hybrid threats deliberately target and exploit existing vulnerabilities of the target state, often opportunistically. Domestic issues such as systemic corruption and social divisions can be exploited by malign state actors. Weakness in national security institutions and a lack of public confidence in government may be seen as domestic political issues, but these vulnerabilities enhance the ability of hostile actors to affect critical functions and damage national security interests. Nations should continually assess their vulnerabilities in an honest and transparent manner and articulate this in national security policy.

**Physical vulnerabilities in services and infrastructure.** Hybrid threats target a state's physical weaknesses; these can be deficiencies in areas such as cyber security, transport and communication infrastructure, or essential goods and services to the population.

- A common technique to influence foreign populations is to step in where the government has failed to provide services such as healthcare and education. Development aid programmes are then used to promote a particular political system or ideology, while simultaneously delegitimising the target state government: *The spread of Salafism in Egypt (5)*, *Casas del ALBA in Peru (30)*
- Unresolved territorial disputes and insufficient border security open up opportunities for deliberately ambiguous activities: *The 2010 Senkaku crisis (8)*, *Detention of Eston Kohver (11)*, *Finnish airspace violations (12)*

**Vulnerabilities concerning governance and sovereignty.** Shortcomings in a state's ability to exert control over its territory, guarantee law and order, manage crisis situations, or make independent policy decisions can enable foreign actors to exert malign influence.

- Economic or energy-related dependencies on another state can induce or coerce a government into making decisions that negatively affect national security interests: *US Transit Center at Manas (4)*, *South Stream Pipeline (13)*, *Pakistani involvement in Yemen (23)*, *Zambian elections 2006 (16)*
- Domestic vulnerabilities such as pervasive corruption, lack of financial or political transparency, and inadequate legal frameworks, not only invite hostile influence activities, but also impede the government's ability to investigate and counter these activities: *The spread of Salafism in Egypt (5)*, *South Stream Pipeline (13)*, *Criminal Networks in the Donbas (21)*

**Social vulnerabilities.** A lack of social cohesion can expose fracture lines that can be exploited by hostile actors. Vulnerabilities include disagreements on what constitutes national identity, different interpretations of history, sectarianism, or radicalism and violent extremism.

- Existing polarisation between identity groups which is based on religion, political ideology or ethnicity can be exploited by hostile actors; governments face the additional challenge of calling out foreign influence without exacerbating divisions: *Russian language referendum in Latvia (14)*, *Bronze night riots (19)*, *Serbian Orthodox Church (17)*
- Social grievances, such as certain groups feeling excluded or discriminated against, are easily instrumentalised to incite discord and civil unrest: *Bronze night riots (19)*, *Civil disorder in Bahrain 2011 (22)*
- Hostile actors can capitalise on insufficient trust in government and media organisations, or exploit a general sense of insecurity and uncertainty present in public discourse: *Criminal Networks in the Donbas (21)*, *Russian espionage in Sweden (27)*

## 5. Build resilience

Resilience in the context of this study describes the ability of a state and society to withstand pressure and recover from crises or shocks which may be the result of a hybrid threat. Improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost-benefit calculation. Deterrence through resilience is therefore a key component of reducing a nation's susceptibility to hybrid threats.

**Patch 'holes in the fence'.** Countering every hostile measure itself is not a sustainable solution, as hybrid threats are highly adaptable, and might continue to target vulnerabilities in different ways. Tackling these vulnerabilities head-on is the first and crucial step for governments to build resilience and make it harder for hostile influence to gain a foothold. Effective communications can help raise public awareness, get stakeholders to agree on the nature of the problem, and generate sufficient political will-power to address the vulnerabilities in question.

- Depending on the vulnerabilities identified, addressing these root problems often demands a sustained and focused effort, which requires adequate resourcing. Eliminating systemic corruption or making up for deficiencies in healthcare and education takes time and political will. Governments can take the lead by raising awareness of vulnerabilities, threats, and the need for resilience-building – both within different government departments and amongst the wider public: *Casas del ALBA in Peru (30)*
- Countries that feature social groups with historical, ethnic or cultural ties to potentially hostile state actors should avoid the unnecessary politicisation of contentious issues and instead focus on common values, shared historical experience and an inclusive vision of the future. This will increase the overall sense of national belonging and frustrate hostile efforts to hamper integration or promote separatist ideals: *Chinese public diplomacy in Taiwan (10), Russian language referendum in Latvia (14), Bronze night riots (19)*

**Whole-of-society.** To tackle domestic issues and build resilience, governments should work together with the private sector, media, NGOs and academia. This will enable the public to be better informed and contribute to inclusive policy-making, and develop an awareness of malicious influence intended to harm the nation.

- The issue of hostile influence through political actors is best addressed by civil society and independent media rather than the government, to avoid the impression of a biased, politically-motivated persecution of a particular party or politician: *The spread of Salafism in Egypt (5), Communist Party of Bohemia and Moravia (18)*
- A healthy and diverse media, both state-funded and independent, and fact-checking organisations, will be able to provide multiple open-source verifications or validations of incidents and events: *US Transit Center at Manas (4)*

**Work with partners.** Hybrid threats are an international issue. National resilience and deterrence are strengthened by forging strategic alliances with international partners which share a common interest in identifying and countering potential threats. Governments should encourage and enable information sharing between nations and integrate those mechanisms to identify and respond to threats at the international level in a coordinated and united manner.

- Many countries share similar security concerns. Governments should support each other in the face of hybrid threats, encourage information exchange, and create joint expertise-based institutions to build a unified front: *2007 cyber attacks on Estonia (3)*
- Threats can be deliberately aimed at weakening a state's relations with other countries, or its commitment to international organisations and institutions: *South Stream Pipeline (13)*

## 6. Activity should be based on values, with clear objectives

Governments need to be clear about their strategic aims and ensure that statements and actions are consistent with core values. They should understand that employing measures or taking positions which appear to be deceptive or inauthentic will undermine their credibility. Democracies should also be aware that appearing to deal harshly with a suspicious actor – such as with civil society or media organisations – might provide the justification for autocratic governments to crack down on disagreeable foreign-sponsored NGOs or media outlets in their own country.

**Uphold democratic values.** Democracies – due to their commitment to freedom of speech, their respect for national and international law, and their accountability to the population – often find themselves at a disadvantage when addressing hybrid threats. This might be due to lack of evidence connecting a suspicious organisation to a hostile foreign actor or proving hostile intent. Legal obstacles can constrain a government's freedom of action in shutting down suspicious civil society organisations, and rightly so. Governments must therefore align their actions with core democratic values, and conduct any investigation in a transparent manner, to bolster their credibility and legitimacy.

- Shutting down or outright banning a suspicious media outlet, political party, or civil society organisation is often not an option for a democratic government. Governments should instead focus on involving civil society in the surrounding debate, and let it point out anti-democratic ideas and groups: *Confucius Institutes (2)*, *Disinformation in Sweden (6)*

**Listen to critical voices.** Governments should plan to incorporate critical voices from neutral or friendly actors into their communication strategy. Governments should anticipate likely lines of argument and take them into account when formulating strategy, which will both increase trust in democratic processes and leave less room for hostile foreign influence to alienate groups from the government.

- Domestic criticism and protests are a normal and healthy part of democracy. It will only benefit adversaries when governments do not take them seriously or try to dismiss them as foreign-sponsored agitation: *Civil disorder in Bahrain 2011 (22)*
- There is likely to be criticism at how foreign influence is handled by the government – some will claim that the government has reacted too harshly and unnecessarily disrupted bilateral relations, while others will criticise that the government's stance has been too weak. Governments should anticipate these lines of argument, and be able to explain in clear terms which considerations led them to choose a specific course of action: *The 2010 Senkaku crisis (8)*, *Zambian elections 2006 (16)*

**Have specific and achievable end goals.** Having realistic and clearly defined strategic aims is vital for coherent communication and unity of effort. All activities should then be nested under this common purpose. Governments should ensure that both proactive and responsive strategies aimed at countering hybrid threats are based on clear and achievable goals, which will enable measurement of progress and the evaluation of outcomes.

- Without clearly stated objectives which are time-bound, it is difficult to maximise the use of resources, maintain coherence and credibility, and sustain public support for prolonged periods of time: *Operation Parakram (24)*



## 7. Be proactive

A proactive approach would enable governments to maintain dominance over evolving narratives and frame events in a manner favourable to their interests. Instead of merely responding to threats as they materialise, governments should anticipate events and issues that are likely to be exploited by adversaries. This can reduce risk by not merely 'countering' an adversary's activities, but pre-emptively steering public discourse in a preferred direction and building resilience, thus reducing the likelihood of unintentionally reinforcing an adversary's preferred narrative of events.

**Prepare through scenario-based training.** Likely scenarios can be mapped out and possible courses of action evaluated with up-to-date target audience analysis, to get an understanding of the possible information effects and outcomes of different decisions. Scenario-based training should be grounded in a comprehensive analysis of the information environment to identify the most appropriate channels of communication and prepare responses for negative themes that are likely to arise.

- In the event of negative themes such as divisive arguments or disinformation arising, responses with key facts and nuances of the situation explained can be quickly presented to media and disseminated in order to mitigate effects of disinformation: *Hamas' use of human shields in Gaza (7), Electronic warfare during Zapad 2017 (26)*

**Expect the unexpected.** By their very nature, hybrid threats can be complex and adaptive. Therefore, governments need to have the institutional capacity to deal with such evolving security challenges, with systems and processes in place that are agile enough to adapt to different actors and changing tactics. The right mindset – both an understanding of hybrid scenarios, and a Strategic Communications approach – would enable governments to quickly detect threats and act in an adequate and efficient manner.

- Based on existing vulnerabilities and tensions with other states – e.g. unresolved border disputes, or stationing of unwelcome foreign troops in the vicinity – governments should anticipate likely scenarios and themes in order to have response mechanisms and communication strategies in place: *The 2010 Senkaku crisis (8)*

**Beware of reinforcing adversary narratives.** Governments should consider how a proposed action or message might serve an adversary's narratives. Attempting to directly 'counter' hostile narratives can reinforce the particular framing of a situation in a way that lets an adversary set the agenda and supports their objectives. Similarly, debunking disinformation can sometimes be counterproductive, as it will give the narrative in question greater prominence. It is therefore important for governments to consider the appropriate frame, medium and messenger. For instance, whether an action or response is taken by a high-level political actor or by subject-matter experts can have a crucial informational effect.

- By analysing a territorial violation on a purely safety-related and technical level rather than on a political level, governments can try to de-escalate tensions and alter the perception of an incident: *Finnish airspace violations (12), Electronic warfare during Zapad 2017 (26)*
- Governments should consider if their proposed actions and messages could be used to reinforce and amplify an adversary's narrative – for example, of 'Russophobia', 'Islamophobia', or 'East-West status conflict': *Detention of Eston Kohver (11), Russian espionage in Sweden (27), Religious extremism in the Netherlands (28)*
- If a hostile measure is repeatedly used against a state, governments should consider if it is productive to defensively counter and respond to every single incident. It might be more constructive to develop long-term strategies on a different level altogether, and take proactive approaches that promote a government's own narrative: *Humanitarian aid in the Russo-Georgian Conflict (9)*

## 8. Understand the information environment

The ultimate purpose of any hybrid threat is to affect the political decision-making of the target nation by influencing key target audiences. Adversarial activity may be undertaken to make a political statement, alter perceptions and attitudes of the general public, degrade levels of trust and confidence in government, or create confusion and a sense of insecurity. This is why consistent, coherent and factual government communications tailored to different key audiences is crucial to maintain trust and cohesion.

**High-visibility measures.** Some hostile measures are specifically designed to be high profile and generate maximum impact. Such threats might be intended to influence decision-making or public opinion on a specific issue, undermine trust in government by creating uncertainty and confusion, or to provoke a particular response. Government strategic communications should demonstrate – through both words and actions – that it has control over the situation; authorities must also have mechanisms in place to ensure that factual information is distributed to the population to mitigate the spread of rumours and disinformation.

- Disruptive events, such as cyber attacks or electronic warfare activities which target civilian systems, are often not intended to cause severe damage – which is part of the strategy of staying below the threshold of any kind of serious reprisal. Rather, these activities might be aimed at sending a political message, achieving certain psychological effects, or making a statement of capability: *2007 cyber attacks on Estonia (3)*, *Electronic warfare during Zapad 2017 (26)*, *Cyber attacks on ROK & US (29)*

**Reputation and legitimacy.** Public debates on the ethics of ‘right’ and ‘wrong’ are often heavily emotional, which an adversary can exploit by strategically framing a political issue in legal terms. Legal arguments can serve both as a source of legitimacy and as a tool to delegitimise an adversary. For instance, in cases of unclear attribution, an adversary might insist on the principle of ‘innocent until proven guilty’. Similarly, an adversary might seek to repudiate accusations of meddling in the internal affairs of other countries by employing ‘whataboutism’ and calling out hypocritical behaviour. One way of preventing these lines of argument from having damaging effects on a government’s legitimacy and reputation, is to display the importance of legal advisors in decision-making by referencing their counsel in public statements.

- Images and emotions are extremely effective means to influence public opinion and frame the narrative. First impressions – even when not accurate – usually frame the narrative, which can allow an adversary to achieve a public relations victory based on a semblance of legitimacy: *Hamas’ use of human shields in Gaza (7)*, *Humanitarian aid in the Russo-Georgian Conflict (9)*

**Measured response.** In responding to hostile measures, governments need to find a way of taking a public stance vis-à-vis the source nation, while not reinforcing the adversary’s desired information effect. A public response should not only be aimed at the adversary but should be tailored to the adversary’s target audience. Government messaging should not just discuss issues that worry the authorities but should address the concerns of the population.

- Media reporting on suspected espionage activities can quickly cause alarm and public concern, which is complicated by the fact that governments face severe constraints when releasing information on intelligence-related matters. Nations should be careful to avoid cultivating paranoia and make a distinction between general threat assessments and responses to single events: *Russian espionage in Sweden (27)*
- Governments often face the challenge of communicating and acting in a way that addresses a threat without reinforcing in-group vs. out-group perceptions: *Religious extremism in the Netherlands (28)*

## 9. Learn to operate in shades of grey

Hybrid threats can be complex, adaptive and inflict damage on national security before they are detected. Ambiguity surrounding intent and attribution impairs decision-making and complicates effective responses. Compelling and credible evidence may not be publicly available, and so the role of government communication becomes particularly important. Official statements should be specific and coherent, capture the nuances of the situation and give enough factual, credible information to inspire public confidence in the government. Governments should not spend too much time on trying to decipher deliberately ambiguous messages and actions, but instead frame events in a manner favourable to their aims.

Ambiguity can hinder effective responses. Ambiguity surrounding hybrid threats – the difficulty in identifying intent and attributing responsibility – can considerably slow down decision-making. It can also limit the response measures available to any affected government if public support is needed. Authorities may also not be able to release all of the information they have, which inevitably leaves room for doubt and alternative narratives that contest the government's position.

- Attributing a hybrid threat to a state actor can pose significant challenges and it may take time to establish compelling and credible evidence. State involvement is rarely black-and-white; the spectrum can range from state-tolerated to state-encouraged, state-orchestrated, or state-executed activity.<sup>10</sup> For example regarding cyber attacks or civil unrest, the degree of state responsibility can be extremely difficult to assess: *2007 cyber attacks on Estonia (3)*, *The 2010 Senkaku crisis (8)*, *Civil disorder in Bahrain 2011 (22)*, *Cyber attacks on ROK & US (29)*
- Connecting actors and groups to hostile foreign governments can be challenging, especially when financial or political links are not substantial, but interests and goals clearly align: *The spread of Salafism in Egypt (5)*, *Institute of Democracy and Cooperation (15)*, *Communist Party of Bohemia and Moravia (18)*
- Assessing hostility can be as difficult as determining attribution. For instance, snap exercises, which could be interpreted as threatening by neighbouring countries, provide a high degree of plausible deniability: *Russian snap exercises in the High North (1)*, *Snap exercises and Crimea (25)*, *Electronic warfare during Zapad (26)*

**Attribution impacts the perception of hostility.** An activity might not in itself be perceived as hostile or harmful, and only be seen as threatening when it is carried out by a certain actor. Foreign funding of an NGO by a friendly democratic state actor will inevitably be treated differently than foreign funding by an autocratic state actor that has been hostile on past occasions. In the absence of credible and compelling evidence, assessments of hostility and attribution ultimately become a political endeavour.

- Strategic context, history, bilateral relations, and common values with the source nation all impact whether an activity is interpreted as hostile: *The spread of Salafism in Egypt (5)*, *Humanitarian aid in the Russo-Georgian Conflict (9)*, *Casas del ALBA in Peru (30)*

**Counter the threat on your own terms.** When adversaries intentionally only give vague or contradictory information in order to confuse and slow down responses, governments can lose valuable time trying to disentangle and interpret the situation. Governments should not let the adversary dictate the rules of the game, but instead counter the threat on their own terms.

- Constantly being in the defensive, demanding clarity from the state actor in question, and scrambling to piece together different bits of information will let the adversary set the agenda. It will also let the adversary seem more powerful and calculating than they actually might be. Instead, governments should present closed ranks and unity of purpose, and stress resilience and international support: *The 2010 Senkaku crisis (8)*, *Bronze night riots (19)*

<sup>10</sup> Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, 22 February 2012.

## 10. Not every activity is a threat

Defining an activity as a threat and attributing it to a state actor is ultimately a political endeavour, and governments should be mindful not to inflate the threat level for political ends, either deliberately or inadvertently. As hybrid threats target a nation's weaknesses, it is a challenge to distinguish hostile influence from legitimate social grievances or failings of the government. Policy-makers should resist the temptation to blame external actors as a convenient way of shifting blame for domestic failings. Inflating or misattributing hybrid threats can affect the government's credibility in the long run and risks unnecessary escalation.

**Context affects meaning.** Historical context and coinciding events affect how words and actions are interpreted by audiences. An action which is perceived as routine or unremarkable at one moment, can be seen as hostile under different circumstances.

- A change in strategic context, such as the deterioration of relations between the Russian Federation and the West, fundamentally affects how events such as territorial violations and military exercises are interpreted: *Finnish airspace violations (12)*, *Electronic warfare during Zapad 2017 (26)*
- The level of analysis can also affect interpretation: an event can be seen as normal activity from a bilateral perspective, and only be interpreted as threatening when placed in a larger historical and strategic context: *Russian snap exercises in the High North (1)*

**Threat assessment.** Governments need to be able to identify why a particular activity is a threat. Regardless of actual hostile intent behind the activity, governments need to be able to assess if the activity in question has any harmful effect on national security interests, and measure this on a continuous basis.

- As the impact of foreign influence frequently depends on internal factors, governments must be careful not to overemphasise the role of foreign hostile activity. In cases relating to social grievances and civil unrest, too much focus on foreign influence might be perceived as an attempt to deflect from political failings: *Civil disorder in Bahrain 2011 (22)*
- Public diplomacy, i.e. the direct interaction of a government with foreign populations, is a fundamental element of international relations. Governments must therefore be able to articulate precisely how a certain kind of public diplomacy is detrimental to national security interests, and take appropriate measures that are consistent with democratic values and international norms: *Confucius Institutes (2)*, *Chinese public diplomacy in Taiwan (10)*

**Avoid unnecessary escalation.** While hybrid threats can sometimes be designed as precursors to the use of conventional military force, they are usually calculated as an asymmetric method of influencing another state without entering into a costly open conflict. A government's response should find a balance between countering hybrid threats and over-reacting in a way that could escalate the situation.

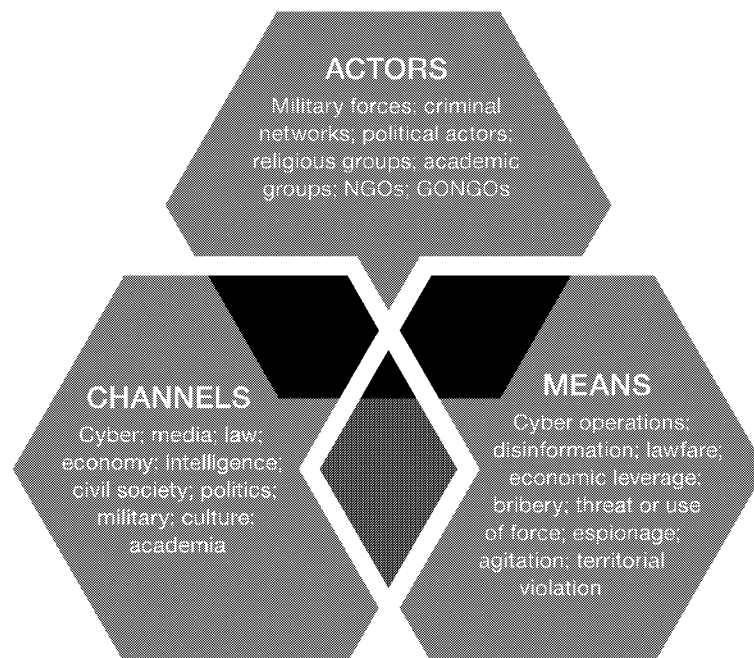
- Particularly when a threat exploits ethnic, cultural or religious divisions in a society, inadequate government responses might easily exacerbate these fractures: *Russkiy Mir Foundation in the Baltics (20)*, *Religious extremism in the Netherlands (28)*
- Factual and nuanced government communication is especially important to avoid threat inflation due to alarmism and a tendency to ascribe every negative occurrence to a hostile foreign actor: *Zambian elections 2006 (16)*, *Electronic warfare during Zapad 2017 (26)*, *Russian espionage in Sweden (27)*
- An apparently hostile activity might be aimed primarily at the perpetrator's domestic audience, for instance to distract from domestic problems, or to reinforce a certain narrative. Overreaction would then either only play into the hands of the source nation, or lead to an escalation that benefits neither party: *Finnish airspace violations (12)*

# Analysis of thematic areas

For the purpose of this project, sixteen thematic areas of threat were identified to group case studies together for analysis. The thematic areas are designed as a typology to help understand the wide range of means and ways that hybrid activity can manifest itself – military and non-military, conventional and unconventional, overt and covert, state and non-state. The thematic areas often overlap, as hostile influence usually involves more than one thematic area.

Grouping the case studies into thematic areas also enables policy-makers and Strategic Communications practitioners to identify case studies relevant to their current problem set. Findings and recommendations from this research that are specific to a thematic area will be covered in this chapter, with an emphasis on the role of Strategic Communications in understanding and responding to hybrid threats.

The thematic areas cover actors, channels and means.<sup>11</sup> In terms of this research – which has limited itself to looking at hybrid threats originating from states – an **actor** might be an institution, political organisation or religious group that is set up, supported, sponsored or somehow inspired by a state. A **channel** is the system or environment that the actor uses – for example, media, cyber, or law – which prescribes certain conditions, principles, and rules of behaviour; every channel has its own dynamics, particularities, strengths and vulnerabilities. The **means** describe the specific measures employed by an actor through a specific channel: this could for instance be disinformation, cyber-attacks or lawfare. Although this might seem like a linear process – an actor employing a channel by using a specific means – it is not always this clear-cut. For example, an actor such as a religious organisation might function as a channel to reach certain audiences in another country.



ACTORS, CHANNELS AND MEANS OF HYBRID THREATS (SOURCE: OWN ELABORATION).

<sup>11</sup> This decomposition into actors, channels and means is based on the diagram of hybrid influencing elaborated by the Hybrid CoE, cf. Atte Harjanne, Eetu Muilu, Jekaterina Pääkkönen and Hanna Smith, "Helsinki in the Era of Hybrid Threats – Hybrid Influencing and the City," (Helsinki 2018: Hybrid CoE), 6.

## THEMATIC AREAS OF THREAT

<p><b>Territorial violation</b></p>	<p><b>Non-Government Organisations (NGOs)</b></p>	<p><b>Government Organised Non-Government Organisations (GONGOs)</b></p>	<p><b>Espionage and infiltration</b></p>
<p>Violation of the internationally enshrined legal principle of territorial integrity which extends across the terrains of land, sea and air. Any such violation is considered an act of aggression by the target nation if carried out without previous consent or knowledge of the target nation.</p>	<p>A not-for-profit organisation that is officially independent from national and international governmental organisations, but is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>A non-governmental organisation which is openly funded, organised and/or directed by a government and may be acting against the national security interests of another nation.</p>	<p>Infiltrating organisations or institutions in order to gain intelligence. Infiltrating organisations or institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to the source nation.</p>
<p><b>Exploitation of ethnic or cultural identities</b></p>	<p><b>Media</b></p>	<p><b>Lawfare</b></p>	<p><b>Agitation and civil unrest</b></p>
<p>Exacerbating existing societal divisions in order to influence identity groups to act in the interests of a hostile state actor against the interests of the target nation.</p>	<p>The deliberate use of media either directly or via an intermediate actor in order to influence audiences and achieve attitudinal or behavioural change which is beneficial to an adversary.</p>	<p>Lawfare describes the hostile use of the legal system against an actor by damaging or delegitimising them, tying up their time, or winning a public relations victory. Lawfare is broadly understood as any exploitation of real, perceived or even manipulated instances of international law violations in order to undermine the target nation.<sup>29</sup></p>	<p>Encouragement of the citizens of a target nation to incite or participate in mass demonstrations and protests with the aim of undermining the government.</p>
<p><b>Cyber operations</b></p>	<p><b>Religious groups</b></p>	<p><b>Academic groups</b></p>	<p><b>Coercion through threat or use of force</b></p>
<p>Organised activity that involves the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."<sup>30</sup> The cyber domain describes an "electronic information (data) processing domain comprising one or several information technology infrastructures."<sup>31</sup></p>	<p>An actor identified as being aligned with a religious institution, movement or group that promotes a religious doctrine or ideology. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>An actor identified as being aligned with an academic institution, think tank or educational interest group. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>The threat or use of force to compel the target nation to act in a particular way or restrict freedom of action.</p>
<p><b>Energy dependency</b></p>	<p><b>Political actors</b></p>	<p><b>Economic leverage</b></p>	<p><b>Bribery and corruption</b></p>
<p>Considered to be a threat when the dependency lies on a source which is considered to be hostile. The target nation is dependent upon a source to the extent that withdrawal would have an immediate and serious effect on the energy infrastructure of the target nation. The dependency can thus be used to economically weaken the target nation or coerce the target nation into acting against its own national interests.</p>	<p>Activity which involves a political figure, party or organisation which is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>The use of economic measures to exert an influence which coerces the target country to act in a way which it otherwise would not. This can be acting to the detriment of the latter's national security or in violation of international law.</p>	<p>The receiving or offering of any undue reward by or to an actor within the target nation in order to influence their behaviour, in particular to induce them to act contrary to their professional obligations and against the national security interests of their own nation.</p>

<sup>12</sup> See: Charles J. Dunlap, Jr., "Lawfare Today: A Perspective," *Yale Journal of International Affairs* 3, no.1 (2008): 146; "Is Lawfare Worth Defining?" *Case Western Reserve Journal of International Law* 43, no.1 (11 September 2010).

<sup>13</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>14</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

## Territorial violation.

**Violation of the internationally enshrined legal principle of territorial integrity which extends across the terrains of land, sea and air. Any such violation is considered an act of aggression by the target nation if carried out without previous consent or knowledge of the target nation.**

**Characteristics.** A territorial violation can be a violation of soil, airspace or territorial waters of a nation. It can range from a limited and temporary violation to a large-scale seizure of territory. While on a technical level, a territorial violation can be clearly identified and defined, there can nevertheless be significant ambiguity surrounding a violation, hampering any assessment on whether or not it was a deliberately hostile act. A territorial violation by a single aircraft, or by a private entity like a fishing trawler, gives the related state actor the ability to plausibly deny any hostile intent or involvement. Unresolved territorial disputes and insufficient border security open up additional opportunities for deliberately ambiguous activities. A territorial violation might be aimed at provoking a certain government response, influencing public debate, testing defences, or actually changing borders.

**Considerations.** In dealing with territorial violations, governments should ensure that the violation is not perceived as a sign of weakness and lack of control, but avoid any unnecessary escalation. Government communication should appreciate that the amount of detail provided, the speed of response and the terminology used to describe an incident can significantly alter how an incident is framed by media coverage and perceived by the wider public. For instance, by analysing a territorial violation on a purely safety-related and technical level rather than on a political level, a government might be able to de-escalate tensions. In determining underlying motivations and the degree of hostility, governments should consider the scale of the violation, the overarching strategic context, historical patterns of behaviour, and the response (or non-response) of the opposite government.

*Detention of Eston Kohver (11), Finnish airspace violations (12), Electronic Warfare during Zapad 2017 (26)*

## Non-governmental organisations (NGOs).

**A not-for-profit organisation that is officially independent from national and international governmental organisations, but is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** NGOs are independent and non-profit civil society organisations, which can be active in areas such as education, healthcare, development work, public policy, religion, environment, or culture. They can perform a variety of charitable or social functions, such as acting as an advocacy group, providing a forum of interaction and debate, or supplying social goods and services that the government is unable or unwilling to deliver. Despite their name, NGOs can receive direct or indirect funding and donations from governments, although funding usually comes from the public, private businesses and other organisations that support their cause. The social work of an NGO is not only a powerful source of legitimacy, but also provides the basis for continuous face-to-face interaction with the public, a vital condition for building trust and influencing public opinion.<sup>15</sup> An NGO can be perceived as threatening by a government if it is deemed to be working in support of a state actor to push an ideology which undermines the ruling authority, promoting antidemocratic values, or challenging national unity by increasing social divisions.

**Considerations.** A vibrant civil society and respect for freedom of speech and cultural exchange are fundamental for a well-functioning democratic society. The ambiguity surrounding links of NGOs to hostile state actors makes it difficult for governments to counter potentially harmful activities. Almost every NGO is reliant upon operational and/or financial support, and governments face the challenge of defining the threshold of hostile interference. Governments should be careful to interfere directly in an NGO's work, as this would likely harm the government's credibility and undermine the very democratic values it aims to protect. In cases where an NGO provides critical services in healthcare or education that the government has failed to deliver, governments should focus on addressing these vulnerabilities and improving their policy performance, rather than closing down NGOs. Before implementing any potential legal regulations of NGOs, such as enhancing financial transparency, governments should carefully consider the second and third order effects that their proposed action could have on the treatment of NGOs in other countries; for instance, countries such as China, India or Russia have recently implemented laws to monitor NGO work perceived to be an instrument of hostile interference.

*Institute of Democracy and Cooperation (15), Casas del ALBA in Peru (30)*

<sup>15</sup> Reza Hasmath, Timothy Hildebrandt, and Jennifer Hsu, "Conceptualizing Government-Organized Non-Governmental Organizations." Paper Presented at Association for Research on Nonprofit Organizations and Voluntary Action Annual Conference (Washington D.C., USA), 17-19 November 2016.

## **Government organised non-governmental organisations (GONGOs).**

**A non-governmental organisation which is openly funded, organised and/or directed by a government and may be acting against the national security interests of another nation.**

**Characteristics.** A GONGO can function as a tool of public diplomacy that enables a government to directly engage with foreign publics and decision-makers. GONGOs can further a government's interests abroad, for example by promoting language and culture, interacting with diasporic communities and expatriates, or promoting certain humanitarian, economic, or political goals. A GONGO's director and management board are often directly selected or approved by the government. Although a GONGO is initiated, directed and/or funded by a government, its institutional set-up mirrors an NGO, meaning that it can often circumvent certain laws of transparency and accountability.<sup>16</sup> Although a GONGO is clearly connected to a state actor, its set-up can provide a degree of plausible deniability for the government, which can take credit for well-received GONGO activities, but still keep the organisation at arm's length when its work faces criticism.<sup>17</sup> A government can perceive a foreign GONGO as problematic, for example if this GONGO promotes antidemocratic thoughts and values, undermines the ruling authority, or discourages the integration process of minority groups with historical or cultural ties to the opposite government.

**Considerations.** Not all public diplomacy is hostile. GONGOs are an essential part of the relationship between states; they promote intercultural dialogue and enrich the civil society landscape at home. GONGOs are officially connected to a foreign state actor, which has an impact on how their activities are perceived by the wider public – they do not have the same amount of authenticity and credibility that organic civil society organisations and independent NGOs have. Governments face the challenge of assessing if a GONGO is damaging the democratic legal order by influencing public opinion or government in a way that undermines the ruling authority. In dealing with GONGOs, transparency and monitoring processes are vital: governments should scrutinise their funding channels, institutional set-up and mandate to assess whether a GONGO is propagating political ideas at odds with democratic values or engaging in other subversive activities.

*Confucius Institutes (2), Russkiy Mir Foundation in the Baltics (20)*

## **Espionage and infiltration.**

**Infiltrating organisations or institutions in order to gain intelligence. Infiltrating organisations or institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to the source nation.**

**Characteristics.** Espionage and infiltration are clandestine acts that usually aim to collect valuable information about the target nation, or infiltrating institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to a hostile state actor. Intelligence work relies on covert actions, and its exposure often has significant consequences for the degree of trust between states as well as between governments and publics. Adversaries can also try to expose intelligence work of the target nations or their partners, such as surveillance operations on citizens and organisations, to decrease public trust in government and intelligence services.

**Considerations.** In dealing with intelligence work, governments face the challenge of balancing the need for transparency with operational security. It is often not possible to report on sensitive information without compromising operational security and disclosing methods of intelligence collection. Governments should therefore work on building public trust in intelligence services. This includes admitting and openly discussing intelligence failures and providing as much information as possible. Speculation beyond the known facts should be avoided as this can affect government credibility, and provoke sensational media reporting, thereby risking unnecessary threat inflation. Moreover, a distinction needs to be made between overall threat warnings and evidence that supports attribution on a case by case basis.

*Detention of Eston Kohver (11), Russian espionage in Sweden (27)*

<sup>16</sup> Stephen W. Kleinschmit and Vickie Edwards, "Examining the Ethics of Government-Organized Nongovernmental Organizations (GONGOs)," *Public Integrity* 19, 2017: 529-46.

<sup>17</sup> Reza Hasmath, Timothy Hildebrandt, and Jennifer Hsu, "Conceptualizing Government-Organized Non-Governmental Organizations," Paper Presented at Association for Research on Nonprofit Organizations and Voluntary Action Annual Conference (Washington D.C., USA), 17 – 19 November 2016.



## **Exploitation of ethnic or cultural identities.**

**Exacerbating existing societal divisions in order to influence identity groups to act in the interests of a hostile state actor against the interests of the target nation.**

**Characteristics.** Hostile foreign actors can target pre-existing divisions in the population of another state. These divisions might be differences in religion, culture, ethnicity, or language. Methods can range from disseminating divisive narratives (either directly, e.g. through public statements, or indirectly, e.g. through media channels, institutions or proxy organisations), to giving material, ideological or organisational support to extremist groups or even separatist movements in another country.

**Considerations.** A key challenge for governments facing foreign exploitation of ethnic or cultural identities is that the core problem – that of social divides or minority grievances – is primarily an internal one. Hostile foreign influence will simply aggravate these problems by targeting vulnerable audiences and framing divisions in a way that is harmful to national unity. A government needs to be very precise in its communications when calling out hostile influence regarding social divisions, as excessive attention to foreign influence might be seen as an attempt to dismiss or discredit legitimate grievances of an ethnic or cultural group. Inconsiderate messaging can also reinforce in-group/out-group perceptions. The messenger used, and the frame selected, can have a considerable effect on how the message is perceived by different audiences. Countries that feature social groups with historical, ethnic or cultural ties to potentially hostile state actors should avoid the unnecessary politicisation of contentious issues, either by accident or for political gain. Instead, they should focus on common values, shared historical experience and an inclusive vision of the future. This will increase the overall sense of national belonging and frustrate malign efforts to hamper integration or promote separatist ideals.

*Chinese public diplomacy in Taiwan (10), Russian language referendum in Latvia (14), Bronze night riots (19)*

## **Media.**

**The deliberate use of media either directly or via an intermediate actor in order to influence audiences and achieve attitudinal or behavioural change which is beneficial to an adversary.**

**Characteristics.** Media is a key channel through which the public is provided with an account of world events, and the means by which most people develop an understanding of an official position. It functions as an array of different institutions, often independent from government, that scrutinise official government positions. Today, traditional media, such as print and television, are increasingly supplanted by new forms of social media, including platforms like Twitter and Facebook, and direct messaging applications, such as WhatsApp. In this networked media environment, journalists have lost their former position as gatekeepers necessary to transmitting political messages to the public. Instead, politicians are now able to directly engage with publics. Adding to this, connectivity allows for instant messaging with a high degree of reach and audience engagement. This has consequences for public diplomacy practices. It facilitates the direct engagement with foreign publics, increases reach and impact and makes it difficult to identify the origin of a message and attribute responsibility. Adversaries can manipulate the media environment through different tactics, such as disinformation, agenda-setting, or information laundering, with the aim to polarise a discussion or confuse the audience. They can also try to buy or set up media outlets to exert influence on a foreign media landscape.

**Considerations.** In a globally-connected networked media environment, government responses are significantly restricted by their bureaucratic systems and democratic decision-making rules and processes which hamper their ability to issue timely, consistent and coherent messages. Statements by regional officials and even by low-ranking soldiers on the ground can be influential or be exploited by hostile actors to legitimise a specific point of view. Governments should consider training officials to refrain from making statements which undermine the overarching narrative, and to be mindful of the impact their individual actions and statements might have. While accepting that from time to time mistakes will be made, improving an awareness of risks in the information environment and developing media skills down to the lowest levels of governments will help officials make statements that are not open to misinterpretation.

*Disinformation in Sweden (6), The 2010 Senkaku crisis (8), Civil disorder in Bahrain 2011 (22)*

## Lawfare.

**Lawfare describes the hostile use of the legal system against an actor by damaging or delegitimising them, tying up their time, or winning a public relations victory. Lawfare is broadly understood as any exploitation of real, perceived or even manipulated instances of international law violations in order to undermine the target nation.<sup>18</sup>**

**Characteristics.** Legal arguments are strongly intertwined with notions of legitimacy and ethics. Adversaries can strategically use these characteristics to legitimise their actions or delegitimise their opponents by framing an action in legal and ethical terms as just or unjust behaviour that requires or impedes a certain course of action, such as an intervention. At the same time, legal conformity does not necessarily lead to the perception of an action as legitimate or just. Media coverage, particularly images or video footage, that portray shocking or compelling scenes such as human suffering, starvation or police violence, often have a strong emotional resonance and can either support or undermine legal arguments. Adding to this, hostile actors can use legal arguments to confuse foreign audiences or simply tie up their time by initiating lengthy legal disputes and processes.

**Considerations.** The legality of an action is often not straightforward, but dependent on a certain interpretation of the applicability of a legal rule to a certain situation. Moreover, legal arguments are often accompanied by emotional messages that can support or undermine claims of legality. Governments should appreciate the functioning of the legal system in defining appropriate behaviour and act in accordance with legal norms, as non-compliance with international law will inevitably undermine their credibility. In dealing with the misuse of legal arguments by adversaries, governments should recognise the ambiguity of law and develop the ability to anticipate different interpretations and possible challenges to their own position. Governments should therefore conceptualise law as a domain to counter the use of legal instruments when employed in a hostile manner. It is important to employ legal advisors and communication experts to address lawfare issues and use their guidance to underpin a line of argument when addressing the public.

*Hamas' use of human shields in Gaza (7), Humanitarian aid in the Russo-Georgian Conflict (9)*

## Agitation and civil unrest.

**Encouragement of the citizens of a target nation to incite or participate in mass demonstrations and protests with the aim of undermining the government.**

**Characteristics.** Civil unrest, in the form of mass protests, strikes or riots, can be caused by political, economic or social grievances. Foreign agitators can incite or aggravate civil unrest in a number of ways, in order to undermine the government. For example, they can use proxies and surrogates, infiltrate disaffected groups, give material or organisational support to allied organisations, or encourage protesters by making public statements that serve to legitimise their cause. They can also use social media to agitate groups and induce protesters into violent behaviour, which is particularly difficult to trace back to foreign governments. Often, the goal of fostering civil unrest is to provoke the government into overreacting and responding in a heavy-handed way, to create a narrative of government repression.<sup>19</sup>

**Considerations.** While peaceful protests are a fundamental part of a healthy democracy, they can affect public order and safety if they escalate and turn violent. Foreign instigators can exploit the concerns and grievances of citizens, especially of vulnerable groups or minorities, and encourage them to channel these in a violent rather than political manner. Governments suspecting a foreign government of having incited or escalated civil unrest should beware of scapegoating a foreign government, while not taking legitimate grievances seriously. Governments should promote political inclusion, and show they are responsive to domestic criticism and address vulnerabilities, such as economic inequality. They should provide channels and means for disaffected groups to voice their concerns in legitimate and constructive ways. Governments should also consider training their security forces to be aware of the information effect of their actions, especially of the effect that images and videos of inordinate use of force can have when distributed quickly over social media.

*Bronze night riots (19), Civil disorder in Bahrain (22)*

<sup>18</sup> See: Charles J. Dunlap, Jr., "Lawfare Today: A Perspective," *Yale Journal of International Affairs* 3, no.1 (2008): 146; "Is Lawfare Worth Defining?" *Case Western Reserve Journal of International Law* 43, no.1 (11 September 2010).

<sup>19</sup> John A. Wickham, Jr., and Mildred E. Hedberg, "Field Manual No. 19-15: Civil Disturbances," *US Armed Forces*, 25 November 1985.

## Cyber operations.

**Organised activity that involves the “employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.”<sup>20</sup> The cyber domain describes an “electronic information (data) processing domain comprising one or several information technology infrastructures.”<sup>21</sup>**

**Characteristics.** As public and private physical infrastructure become more networked and reliant on information technology, they become increasingly vulnerable to cyber attacks. Adversaries can employ cyber operations to target critical infrastructures, such as banking or healthcare systems. Such disruptive attacks are often designed to be overt and aimed at high public visibility, for which they do not need to be particularly sophisticated – such as denial-of-service attacks, computer viruses or website defacements. Covert cyber operations aimed at espionage, by contrast, often remain undetected for a long time.

**Considerations.** The difficulty of attributing a cyber attack hampers a government’s ability to respond in an effective and timely manner. In dealing with the increasing threat of cyber operations, governments should both prepare effective communication strategies for immediate crisis response, as well as enhance their capabilities and methods to investigate and communicate attribution findings.<sup>22</sup> Communication strategies need to be included in civil contingency plans to calm the population and distribute essential information immediately to mitigate the spread of rumours and disinformation. Governments should increase cyber literacy amongst government officials, spokespeople and among the media, to ensure factual, coherent and credible communications.

*2007 cyber attacks on Estonia (3), Cyber attacks on ROK & US (29)*

## Religious groups.

**An actor identified as being aligned with a religious institution, movement or group that promotes a religious doctrine or ideology. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** Religion can be instrumentalised by a state actor in various ways. It might set up, direct and/or give financial or operational support directly to religious institutions, or to civil society groups, political actors, media outlets or other institutions that promote a particular religious ideology. A government might also subsidise or otherwise facilitate the education and training of clerics and religion teachers abroad, or provide foreign audiences with educational materials such as books on the religious ideology it is aiming to promote. Underlying motives of a government could be to further a transnational religious movement out of ideological conviction, or to promote a certain world view that bolsters the government’s legitimacy at home and abroad.<sup>23</sup> A government might also use religious language as a channel to reach and influence certain foreign audiences for political purposes. Religious activity can become a security concern when it threatens the democratic legal order by promoting antidemocratic aims or means, such as the rejection of state authority.

**Considerations.** Freedom of religion constitutes one of the core principles of a pluralist democratic society. Governments face the challenge of balancing the right to freely practice religion with a potential risk to national security interests. A hostile state can use religious groups to undermine the ruling authority. Religious activity is usually built on a strong unifying narrative that promotes a distinct worldview, implicating certain values, beliefs and practices. Messages based on a sense of community and belonging facilitate emotional resonance and positive identification, which adversaries can exploit to exacerbate social differences. In dealing with a potential hybrid threat involving a religious actor, governments should ensure a careful message design that avoids reinforcing social cleavages. It is important that governments de-link religion from the specific threat to avoid the perception that an entire religious group is targeted; they should also try to trace funding flows or an alignment of interests between a religious group and a foreign government.

*The spread of Salafism in Egypt (5), Serbian Orthodox Church (17), Religious extremism in the Netherlands (28)*

<sup>20</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>21</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>22</sup> John S. Davis II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica, CA: RAND, 2017).

<sup>23</sup> Peter Mandaville and Shadi Hamid, *Islam as Statecraft: How Governments Use Religion in Foreign Policy* (Washington, D.C: Brookings, November 2018).

## Academic groups.

**An actor identified as being aligned with an academic institution, think tank or educational interest group. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** State actors can aim to influence academic groups, such as university lecturers or think tanks, within the target nation to co-opt the brand of independent scientific or educational institutions. By setting up or supporting such groups, adversaries can try to influence audiences through the guise of objective and neutral centres of expertise. This provides their messages with a high degree of authority and makes it more likely that domestic publics or policy-makers accept their point of view based on perceived impartiality. Academic groups that are aligned to the source nation can also be used as a channel to exert influence on diaspora student communities that study at foreign universities.

**Considerations.** Independent academic research plays a crucial role in every democratic society by evaluating government policies and providing advice and expertise. International academic exchange is a source of success for high-ranking universities around the world. Many academics receive scholarships or funding from governments, which makes it difficult to assess the threshold of malign interference. It is a challenge to protect higher educational institutions against such influence while safeguarding their independent status and ensuring their role as free centres of advice and expertise. Democratic governments should encourage educational and cultural exchange, while protecting the integrity of their higher educational systems. In cases where an academic group has frequently engaged in promoting opinions at odds with fundamental democratic values, governments should seek dialogue with university leadership or unions. These should encourage that academic groups disclose any partnerships or sources of funding to guarantee transparency. This ensures that their research can be discussed against the background of any potential bias. While the decision of closing down academic institutions should lie with the respective universities, governments can raise awareness and warn against foreign academic groups becoming an integral part of domestic educational institutions, and ask universities to critically engage with their programmes and academic methods.

*Confucius Institutes (2), Institute of Democracy and Cooperation (15)*

## Coercion through threat or use of force.

**The threat or use of force to compel the target nation to act in a particular way or restrict freedom of action.**

**Characteristics.** Military force posture and presence, such as the build-up of troops at an international border, ordering large snap exercises, or the development of certain capabilities such as nuclear weapons, is usually planned with certain information effects in mind to send a message of intimidation, deterrence or reassurance. The threat of force can also be implicit in political statements and can have a significant impact on another country's domestic public debates and decisions related to security and defence.

**Considerations.** Governments face the ambiguity as to whether military measures are aggressive or defensive in nature, and so need the ability to synthesise traditional military intelligence with analysis of the information environment. Snap exercises provide adversary governments with a high degree of plausibility, and an excuse to circumvent the OSCE Vienna Convention's stipulations on transparency and troop numbers. When trying to understand the desired information effect, governments should take into account that timing and context can significantly influence how military activity is perceived. For instance, a snap exercise might be perceived as normal on a bilateral level but be part of a worrying trend on a wider strategic level. An airspace violation can be treated as a purely technical and safety-related matter in one year, and as a clear threat in another, depending on the state of bilateral relations at the time. Government communication – i.e. the frame, the wording, and level of urgency – has a considerable impact on how military posture or threatening comments are received by the wider public, and whether or how they impact security-related debates and decisions, such as NATO membership.

*Russian snap exercises in the High North (1), Operation Parakram (24), Snap exercises in Crimea (25)*

## Energy dependency.

**Considered to be a threat when the dependency lies on a source which is considered to be hostile. The target nation is dependent upon a source to the extent that withdrawal would have an immediate and serious effect on the energy infrastructure of the target nation. The dependency can thus be used to economically weaken the target nation or coerce the target nation into acting against its own national interests.**

**Characteristics.** Energy-related dependencies on another state can be dangerous if this induces or coerces the government into making decisions that negatively affect national security interests. A hostile actor can withdraw the supply of critical energy resources, such as oil or gas, with the aim of coercing the target nation into taking a desired course of action. Moreover, the awareness of a dependency or a credible threat by an adversary can already have an indirect influence on decision-making. Overreliance on a single energy source and a failure to ensure supply diversification can exacerbate energy dependency. Poor governance performance and state capture in energy policies hampers the development of a coherent strategy on energy security.<sup>24</sup> Furthermore, energy dependency is often not just a bilateral issue, as the decisions of single countries can affect the energy security of an entire region. What may not be considered as a threat to an individual state's national security can affect the resilience of broader global governance structures.

**Considerations.** Democratic governments must balance value, reliability, and security in the provision of its energy. Decision-makers should be attentive to the possible vulnerabilities of energy policies and monitor lobbying in this area to make sure that the protection of national security is taken into account when taking decisions on energy supply. Governments face the additional challenge that most critical energy infrastructure is in private hands, which makes it more difficult to regulate and protect energy infrastructure.<sup>25</sup> One way of addressing this issue is the establishment of Public-Private Partnerships (PPPs), which are "long-term contracts between a public agency or public sector authority and a private sector entity."<sup>26</sup> This is not always an easy endeavour, since business and national security interests often diverge, and both public and private entities are reluctant to share information and know-how. In these cases, effective communication can help raise public awareness, get stakeholders to agree on the nature of the problem, and generate sufficient political will-power to develop a joint approach to energy security that balances both business and security interests.

*South Stream Pipeline (13)*

## Political actors.

**Activity which involves a political figure, party or organisation which is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** Adversaries can support ideologically aligned political groups, such as parties, their youth organisations, or individual politicians to influence democratic processes and decision-making. Tactics can range from open support, such as through public statements or high-level visits, to covert actions, such as secret funding, infiltration or bribery.

**Considerations.** In the absence of a clear link between a political actor and an adversary, the line between legitimate democratic debate and subversive activity which damages the national interest may be unclear. It is often difficult to distinguish whether a political actor's alignment of interest or ideology with a hostile state actor is the result of foreign influencing such as funding, or simply stems from independent pragmatic calculations or convictions. Political actors suspected of working against the national interest are often best addressed by civil society and media organisations rather than the government, to avoid the impression of a biased, politically-motivated persecution of a particular party or politician. Governments should avoid directly attacking a political opponent and rather focus on strengthening the legal frameworks around elections to ensure a fair campaign and political debate.

*The spread of Salafism in Egypt (5), Zambian elections 2006 (16), Communist Party of Bohemia and Moravia (18)*

<sup>24</sup> "EU and NATO's Role in Tackling Energy Security," Policy Brief No. 47, *Center for the Study of Democracy*, February 2015.

<sup>25</sup> Tiziana Melchiorre, "Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security," *NATO Energy Security Centre of Excellence (Vilnius 2018)*, 5.

<sup>26</sup> *Ibid.*, 6.

## Economic leverage.

**The use of economic measures to exert an influence which coerces the target country to act in a way which it otherwise would not. This can be acting to the detriment of the latter's national security or in violation of international law.**

**Characteristics.** Economic dependencies on another state can become a threat if this induces or coerces the government into making decisions that negatively affect national security interests of the target nation. Economic leverage can be exerted on the target nation through economic sanctions, such as import and export embargoes or tariffs, or withdrawing the supply of critical goods, but also through incentives, such as trade preferences, development aid, or export of energy resources, high tech products or military equipment.<sup>27</sup> Economic sanctions can also be employed as a tool of 'signalling and deterrence' to communicate discord with the target nation's policies or issue a general statement of capability that is intended to grant credibility to future threats of coercive measures.<sup>28</sup>

**Considerations.** Governments face the challenge of balancing values, business interests and security concerns in their foreign relations. Adversaries that hold economic leverage over another state can affect a change in behaviour even without having to resort to explicit threats, as the sheer awareness of potential sanctions or other hostile measures can suffice to change government's decision-making. Hostile economic measures can often be implemented with a high degree of plausible deniability, as measures such as the imposition of tariffs can be framed as a purely economic decision detached from the political matter at hand. Governments should develop long-term strategies to assess economic and political dependencies, resist 'easy cash' and build strategic alliances with partner nations to reduce the risk of the exploitation of economic leverage by hostile actors.

*US Transit Center at Manas (4), The 2010 Senkaku crisis (8), Pakistani involvement in Yemen (23), Zambian elections 2006 (16)*

## Bribery and corruption.

**The receiving or offering of any undue reward by or to an actor within the target nation in order to influence their behaviour, in particular to induce them to act contrary to their professional obligations and against the national security interests of their own nation.**

**Characteristics.** Pervasive and systemic corruption in a state poses a significant vulnerability to hostile foreign influence. An adversary might attempt to destabilise or weaken another country by systematically promoting corrupt behaviour and criminal networks, thus making the country harder to govern and decreasing trust in the government. Corruption can also function as an enabling factor for other hostile measures: a kleptocratic government is more likely to make decisions that undermine the country's national security interests for the personal gain of a few politicians, for example on matters related to energy security.

**Considerations.** Corruption is first and foremost a domestic problem, which is often merely exploited by foreign actors. As corruption is fundamentally intertwined with a lack of transparency and poor governance, it can be difficult to trace these types of hostile foreign influence. The fact that the very institutions designed to counter these types of hostile foreign influence – including security forces, the judiciary and elected politicians – may themselves benefit from the corrupt system or otherwise be under the influence of criminal networks, hinders the effective countering of such threats. Systemic corruption decreases public trust in democratic institutions in the long run, as it causes frustration with the lack of accountability and transparency, and disillusionment with political processes. A key issue for a government is to muster enough political will to fight corruption in earnest, and tackle this domestic vulnerability to foreign influence. Governments also need to credibly display this political resolve to the public, for example by using show cases of high-level punitive action for their information effect, to regain credibility and trust among the population. This should be accompanied by sincere efforts to increase transparency and create a robust legal framework. Government should also consider allocating higher salaries to judges and conducting amnesty programmes for lower-level corrupt business-people.

*Criminal networks in the Donbas (21)*

<sup>27</sup> Richard N. Cooper, "Is 'Economic Power' a Useful and Operational Concept?," *Weatherhead Center for International Affairs*, Working paper series no. 04-02, 2004, 7.

<sup>28</sup> Chen-Yuan Tung, "Cross-Strait Economic Relations: China's Leverage and Taiwan's Vulnerability," *Issues & Studies* 39, no. 3, (September 2003): 137-175, 136-7.

# CASE STUDY SUMMARIES

This section contains summaries of 30 case studies analysed using a standardised framework. Cases were selected because they were assessed as featuring behaviour which could be considered as having the characteristics of hybrid threats.

# RUSSIAN SNAP EXERCISES IN THE HIGH NORTH

## SUMMARY

On 16 March 2015 the Russian Federation began a *combat readiness test* ('snap exercise') of its Northern Fleet and force elements located in its Western Military District. The scale of the exercise was much larger than originally announced, and coincided with the Norwegian exercise Joint Viking in Finnmark (the northernmost part of Norway) and the US exercise Drogone Ride. Since both of these exercises were announced well ahead of time, it is reasonable to assume that the Russian snap exercise was timed as a defensive move or as a response to these exercises.

There remains considerable debate as to whether the readiness exercise violated the Vienna Document, a confidence and security-building measure agreed upon with the OSCE. Norway stated at the time that it was monitoring the situation, and did not submit a complaint to the OSCE. However, the consistent use of such snap exercises to circumvent requirements for notification runs counter to the spirit of the agreement and undermines its provisions.

Readiness tests are often assessed as being a threat to national security, since they have precluded a number of past conflicts, most notably in Ukraine.<sup>1</sup> In this case it is assessed that the exercises did not pose a threat to Norwegian security interests, but rather they were part of conventional geopolitics in the High North. While there seems to be a discrepancy between Norway and NATO's position on the exercises, this ostensible discrepancy is itself part of the conventional balance of power in the region.

## KEY POINTS

- The case study highlights the importance of strategic context: whether one considers the exercises in the context of NATO activities and the conflict in Ukraine or just as a bilateral issue has an impact on how different audiences understand events.

- From Norway's perspective, a high level of military activity, including the conduct of such exercises in the High North, was considered to be routine. Norway treated this series of events as part of accepted normality and did not identify the combat readiness tests as an exceptional or significant threat.

- NATO, by contrast, regarded the increase in Russian snap exercises as a breach of the spirit of the Vienna Document. This highlights the need to consider the differences between NATO narratives and national strategic interests, which in turn reinforces the importance of messaging which is coherent and mutually supportive at the international level.

- An effect does not necessarily have to be a change in behaviour, but could also be the maintenance of the status quo, i.e. considering a high level of military activity to be 'normal'.

## CONTEXT

- **The High North.** The 'High North' is of significant geostrategic value to Russia; home to the Northern Fleets' strategic nuclear submarines and supporting base infrastructure. Beyond its immediate geostrategic importance, the High North is rich in mineral, energy, and marine living resources. In any conflict, it would be expected that Russia would defend this region by deploying forces into northern parts of Norway, the Barents Sea, and the Norwegian Sea.

- **Increase in exercises.** Russian snap exercises, also referred to as readiness exercises, have increased in number since 2013, as part of Russia's military reform and modernisation plans, as well as the turn to (and reintroduction of) power politics and great power competition. Russia has previously used such exercises as a deception tool prior to the use of offensive military operations.<sup>2</sup>

- **Cooperation.** The Vienna Document<sup>3</sup> is a Confidence and Security-Building Measure (CSBM) agreed upon with the OSCE in 1990, which requires participating states to notify each other ahead of time about major military activities such as exercises. According to a strict application of the text, exercises carried out without prior notifications to the troops involved are an exception to this rule.



Baltic Fleet repels simulated missile attack near Kaliningrad on 18 March 2015. IMAGE – Ministry of Defense of the Russian Federation.

## KEY ACTORS

Russian Ministry of Defence  
Norwegian Ministry of Defence  
Norwegian Parliamentary Foreign Relations and Defence Committee  
Norwegian Intelligence Service  
Norwegian Joint Headquarters

General Sergey Shoygu Russian Minister of Defence (since 2012)  
Alexey Meshkov Russian Deputy Foreign Minister (2012 – 2017)  
Colonel-General Vladimir Shamanov Commander Russian Airborne Troops (2009 – 2016)  
Ine Eriksen Søreide Norwegian Defence Minister (2013 – 2017)  
Jens Stoltenberg NATO Secretary General (since 2014)



# NARRATIVES

## Russian government

- New challenges demand exercises, particularly of Russian strategic formations in the north.
- The purpose of this exercise is to test the Northern Fleet's readiness and capability to protect Russian interests in the Arctic region.
- Russia is concerned about the number of NATO exercises, particularly in the north-eastern region of Europe, which increase tensions and destabilise the region.<sup>4</sup>

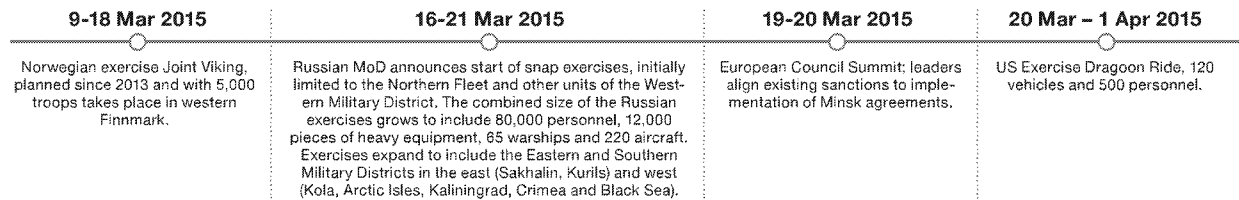
## Norwegian government

- All nations periodically conduct military exercises, including readiness exercises.
- This exercise, although large, was within the scope of what is considered normal, and thus not considered a threat.
- Norway will register any deviation from what is considered to be normal, although it does not seem as though Russia should have provided advance notification for this exercise.<sup>5</sup>

## NATO

- These Russian snap exercises run counter to the spirit of the Vienna Document, and are a serious concern (exercises are discussed in context with Russian aggression in Ukraine).<sup>6</sup>

# KEY EVENTS



# STRATEGIC LOGIC

It is reasonable to assume that Russia factors the timing of Norwegian and NATO exercises into their planning process ahead of snap exercises. Hence, this exercise in particular can be understood as a response to exercises Joint Viking and Dragoon Ride – all of which are part of the continual 'dialogue' of exercises between actors. In addition to the obvious and immediate benefits of improving military capability, this particular readiness exercise might have had other underlying strategic logics, such as also being a domestic show of force to boost national pride, a part of Russia's strategic deterrence against what it sees as NATO aggression, or as a reminder to neighbouring states not to stray too far from Russian interests. Exercises can also be part of an effort to normalise military activity at this scale. At a time of discord between Russia and the West, the underlying core logic could arguably be to demonstrate Russia's determination not to alter their course under Western pressure.

# MEASURES

**DIPLOMATIC.** Strategic deterrence of NATO; typical power politics (High North).

**INFORMATION.** Frequent updates about exercises after commencement; portrayal of exercise as a natural response to NATO behaviour.

**MILITARY.** Conducting a snap exercise to test readiness levels without prior notification and expanding the scope of the exercise. Conducting exercises for which the would-be adversary can only be NATO and/or the US.

**INTELLIGENCE.** None, but it is reasonable to assume that they were attentive to NATO nation responses during the exercises.

**LEGAL.** Taking advantage of the flexibility and room for interpretation in the terms of the OSCE's Vienna Document.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- High North as Norway's most important strategic area of responsibility.<sup>7</sup>
- Maintenance of the international rule of law, institutions, regulations and norms that regulate behaviour (e.g. Vienna Document).
- Predictability and consistency of relations with Russia, as well as further cooperation with Russia based on common interests.

## VULNERABILITIES

- Asymmetry of Russian-Norwegian relations in terms of military capability, which is why Norway aims to make the High North an area of multilateral cooperation.
- Unresolved border disputes in the High North, especially regarding the delimitation of littoral states' Exclusive Economic Zones (EEZs) and the definition of extension of their continental shelves beyond the EEZs. Norway and Russia, however, reached an agreement on a maritime boundary in the Barents Sea in 2010.

## THREATS

- This snap exercise can be interpreted as a demonstration of Russia's ability to achieve dominance in the Kola Peninsula and environs, particularly against the type of force concentration demonstrated in exercise Joint Viking.
- Exercises might be perceived as threatening, because Russia has previously used exercises to shape the operational environment for offensive operations against neighbouring states.
- Norway's official position at the time was that the exercises posed no direct threat to Norway.

## EFFECTS

- This snap exercise did not force Norwegian authorities to deviate from 'business as normal.'
- An effect does not necessarily have to be a *change* in behaviour, but also the maintenance of the status quo. Russian intent might simply have been to *normalise* these kinds of snap exercises in the High North.
- Discrepancy between Norwegian reactions (exercises do not pose a threat to national security) and NATO reactions (snap exercises as serious concern and at odds with the spirit of the OSCE Vienna Document), as NATO considers not only bilateral relations but overall regional trends.

# CONFUCIUS INSTITUTES

## SUMMARY

The Confucius Institutes (CIs) are non-profit educational institutions funded by the Chinese government, with the stated purpose of promoting Chinese language and culture. They were brought forward as a means to tell China's story to the world, but also to demonstrate to the domestic population how China is welcomed and respected globally. Since the launch of the Confucius Institutes programme in 2004, the large-scale initiative has been described as a Chinese 'soft power' success. The Confucius Institutes have secured a number of partnerships with universities in 146 countries around the world, including in NATO member states. In 2017, there were 525 Confucius Institutes at colleges and universities, as well as 1,113 Confucius classrooms at primary and secondary schools.

The CI initiative resembles other cultural institutes like the United Kingdom's British Council or the German Goethe Institut in the ways it provides language training and promotes culture (e.g. through cooking courses or calligraphy classes, and celebrating Chinese holidays). Unlike these other cultural associations, however, the CIs are set up as

a structural unit within a host university, and employ a system of double directorship.

However, the motives behind this large-scale initiative and the procedures of installation in host countries have attracted criticism, in particular the lack of transparency concerning the university contracts, hiring policies and financial aspects. Moreover, reports of self-censorship on sensitive political and historical topics (such as Tibet, Taiwan, or the Tiananmen Square protests of 1989) by both Chinese teachers and local university professors have raised concerns about intellectual freedom. Several scandals in 2014 involving instances of censorship cast light on the hard-line approach applied by the previous Director General, and the tight control exerted by the CI's governing body Hanban and the Chinese Ministry of Education. The controversy resulted in the non-renewal of CI contracts in several universities in the US and Europe and greatly contributed to the perception of CIs as an instrument of Chinese influence.

## KEY POINTS

- Institutions such as the CI should not be seen as inherently hostile – public diplomacy remains a key component of increasing understanding and cooperation between nations. Concurrently, attention should be paid to instances where national security interests might be affected – such as audiences being exposed to a world view at odds with democratic values. The Confucius Institutes should be viewed as acting in accordance with the official Chinese position and in line with larger Chinese strategies of soft power.

- The domestic goals of the Confucius Institutes are as important as the effects desired through the use of public diplomacy to influence foreign audiences. China's government is trying to spin the 'World Welcomes China' narrative in order to legitimise its rule through the image of acceptance and sympathy abroad.

- Such organisations must be treated solely as sources for language and cultural exchange; the lack of academic freedom precludes any claims to wider expertise. A stricter administrative and financial division within the host universities should be applied in order to ensure academic freedom. Sources of funding, as well as underlying political objectives, should be made transparent to the public, media and academia.



## CONTEXT

- **Worldwide presence.** The first Confucius Institute was established in 2004 in Seoul, South Korea,<sup>2</sup> although the first pilot project was launched earlier that year in Tashkent, Uzbekistan.<sup>3</sup> In the following 13 years, the number of CIs globally reached 525 Confucius Institutes at colleges and universities, as well as 1,113 Confucius classrooms at primary and secondary schools in 146 countries (2017). 173 of the Institutes are located in Europe and 110 in the United States of America.<sup>4</sup>

- **Calls for closure.** Both the Canadian Association of University Teachers and the American Association of University Professors (AAUP) called for the closure of all Confucius Institutes, with the AAUP stating in 2013 that the CIs "function as an arm of the Chinese state" and "advance a state agenda in the recruitment and control of academic staff, the choice of curriculum, and in the restriction of debate."<sup>5</sup> In a 187-page report analysing

the work of the CIs in the US, the National Association of Scholars also recommended an immediate closure of all Confucius Institutes in 2017.<sup>6</sup>

- **China and Soft Power.** 'Soft Power', as defined by American political scholar Joseph Nye in the late 1980s, "occurs when one country gets other countries to want what it wants [...] in contrast with the hard or command power of ordering others to do what it wants."<sup>7</sup> President Xi Jinping said in 2014 that "we should increase China's soft power, give a good Chinese narrative, and better communicate China's message to the world," although it is unclear whether they refer to Nye's concept of soft power or have their own definition. China's soft power tools include infrastructure and aid programmes, but also more traditional tools like educational exchanges and international media outlets, as well as the Confucius Institutes.<sup>8</sup>

## KEY ACTORS

**Confucius Institute Headquarters (Hanban)** a corporate body affiliated to the Chinese Ministry of Education

**Xu Lin** former Director General of Hanban, left in 2014 after censorship scandal

**Ma Jianfei** Secretary of the Party Committee of Hanban (Director General level); the Director General position has been empty since the censorship scandal)

# NARRATIVES

## Chinese government

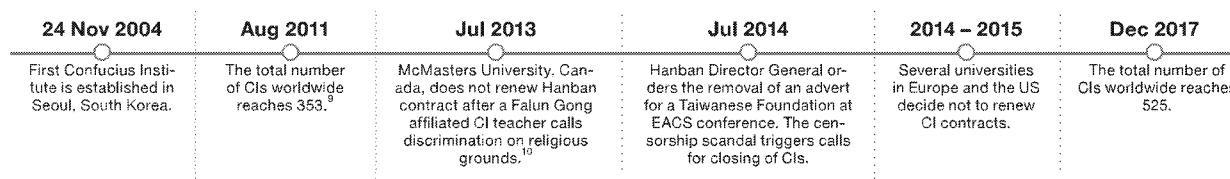
- 'The world welcomes China': Confucius Institutes are much welcomed across the globe.
- Host institutions are the primary initiators in setting up the CIs.
- The CI initiative is the biggest international legacy of President Hu's rule.

## Critics of the Confucius Institutes

From various Western NGOs, think tanks, government officials and academics:

- Suspicion of CIs, 'better-safe-than-sorry' approach.
- Academic institutions can become too dependent on Hanban money, which can lead to (self-)censorship on sensitive political issues, and thus limit freedom of expression.
- By decreasing the outreach of competing narratives (e.g. from Taiwan, Tibet), the CIs have the potential to influence public opinion in the long run.

# KEY EVENTS



# STRATEGIC LOGIC

In order to establish a Confucius Institute, Hanban requires the host institution to establish a partnership with an educational institution in China, making it appear more as a local initiative than an organisation established by an outside actor. Once the partner institution is approved by Hanban, both organisations appoint a director of the soon-to-be established Confucius Institute, thus abiding by the principle of double directorship stipulated by China. It is likely that the Chinese side initially viewed the cooperation

between the universities and the principle of double directorship as a means of reassuring the partners abroad.<sup>11</sup> Ironically, this policy resulted in almost instant suspicion from the Western partners. Drawing on the image of universities as the beacons of freedom of expression and academic thought, the partner institutions may risk becoming a point of entry for Chinese political agenda in the West.

# MEASURES

**DIPLOMATIC.** The work of CIs is intertwined with that of the diplomatic corps, especially the Cultural Affairs Office. Almost every event organised by CIs (festivals, concerts, language competitions) is attended by representatives from the Chinese Embassy at the Ambassador or Consul General level. The establishment of a CI requires an official application from the host institution: when the host institution is reluctant, the initiative of the establishment is unofficially expressed by the Chinese side, lobbying for the institution to apply for CI status. In more strategic cases, the Ministry makes use of diplomatic channels to convey the message that an application for establishment coming from a local entity would be highly appreciated.<sup>12</sup>

**INFORMATION.** Teaching and opportunity marketing (e.g. scholarships) contribute to the CI's successful informational impact. The space for China-related discussion is very narrow, as no meaningful exchange on China's interior or international problematic issues is allowed.

**FINANCIAL.** CIs typically receive a minimum of USD 100,000 in annual support for programming.<sup>13</sup> The CIs are obliged to report their annual projects and accounts to Hanban for approval. The CIs are jointly financed by the Chinese Ministry of Education and the host university. Most of the CIs are not self-sustainable.

**INTELLIGENCE.** Speculation over industrial espionage have been made in the US, and universities with cutting-edge technology were encouraged to exercise caution when cooperating with CIs. Hanban has strongly denied this.

**LEGAL.** The degree of integration of the Confucius Institutes into the everyday academic work of the universities is determined by contracts signed between the involved institutions. In some cases, the legal framework gives the Institutes influence over academic goal-setting, potentially endangering academic freedom.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Sovereignty of foreign policy and internal mechanisms making the foreign policy decisions.
- Integrity and consistency of internal public opinion of external actors (countries).
- Integrity and consistency of academic thinking related to research on China.

## VULNERABILITIES

- Academic institutions often face severe financial constraints. They will therefore often welcome the generous funding from Hanban to provide educational training they would otherwise not be able to offer.
- The policy of establishing a CI within an existing university and injecting the funds and the management into the host university make the university more vulnerable towards a Chinese political agenda.

## THREATS

- The boundaries of what CIs should and should not promote in terms of Chinese culture abroad are rigorously predetermined in operational guidelines, and are politically non-neutral. The agenda of Hanban, if not analysed critically, has the potential to influence the host country's public opinion on China's sensitive political issues.

- The asymmetry of resources invested by the CIs in the popularisation of China's official world view decreases the outreach of competing narratives (e.g. those of Taiwan).
- Potential self-censorship on the side of the host university (e.g. in 2013, Sydney University cancelled a lecture by the Dalai Lama, reportedly to avoid damaging its ties with China, including funding for its CI).<sup>14</sup>

## EFFECTS

- General aim of the popularisation of Chinese culture and especially Chinese language has been achieved, as CI courses reach hundreds of thousands of people worldwide.
- Increased visibility of China in host countries.
- Minimisation of the cultural impact of opposing organisations by monopolising the narrative on Chinese culture.
- Hanban is facing massive public relations challenges following suspicious attitudes towards CIs that have dominated both the Western media as well as academia since the 2014 scandals.

# 2007 CYBER ATTACKS ON ESTONIA

## SUMMARY

In April and May 2007, Estonia was the target of a coordinated cyber attack. Over a three-week period, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by a Distributed Denial of Service (DDoS). The cyber attack coincided with the Estonian government's decision to relocate the Soviet-era 'Bronze Soldier Memorial' in Tallinn, which led to significant civil disturbance in both Estonia and Russia.

Much of the malicious network traffic showed signs of political motivation and Russian-language origin. The Russian government denied any involvement, blaming 'patriotic' pro-Russian groups and individuals. However, the cyber attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and a refusal

to cooperate with the Estonian investigation in the aftermath of the attacks, which likely encouraged the perpetrators.

The attacks caused some disruption and economic cost to Estonia. Perhaps more importantly, though, they exposed Estonia's vulnerabilities, and demonstrated the *potential* of cyber attacks to cause far more lasting damage if intended. However, the incident also demonstrated Estonia's capabilities and resilience in countering the cyber attacks. Ultimately, the shock caused by the cyber attack led to a significant strengthening of cyber defence capabilities, institutions and legislation in Estonia, the European Union, and NATO.

## KEY POINTS

- Ambiguity was a key feature of this cyber attack. As the attacks were apparently carried out independently by individuals using their own resources, any state sponsor responsible for orchestrating the attack was able to disguise themselves and deny involvement. This underscores the requirement for governments to achieve political consensus on attribution in a timely manner based on the available evidence and be able to communicate this in a clear and understandable way to the general public.

- In addition to the physical effect on infrastructure, cyber attacks have a significant psychological dimension. In this case, attackers could have inflicted significantly more damage within the cyber domain if desired, but it was highly likely that a key objective was to test the responses of

the Estonian government and EU and NATO allies, as well as to damage the reputation of the Estonian government in the eyes of Estonia's Russian-speaking population and global public opinion. The cyber attacks almost certainly targeted the government's ability to provide effective and calming strategic communication to domestic and foreign audiences during the crisis.

- In this case, as well as in similar cyber attacks on Lithuania (June 2008), Georgia (July/August 2008), and Kyrgyzstan (January 2009),<sup>1</sup> cyber activity was integrated and synchronised with a wide spectrum of other measures, such as economic or diplomatic pressure, with the result of increasing strategic effects.

## CONTEXT

- **Distributed Denial of Service (DDoS).** DDoS attacks are one of the most common forms of cyber attacks. The attacker will spread malicious software to vulnerable computers, e.g. through infected emails and attachments, and so create a network of infected machines (called a botnet). The attacker can then command the botnet to bombard a certain website or online service with traffic, until the site crashes under the sheer load of requests.<sup>2</sup> DDoS attacks, by their nature, do not usually cause extensive or even irrecoverable damage, but can cause considerable disruption.

- **The Bronze Soldier Memorial.** The Bronze Soldier is a controversial Soviet-era war memorial built at the site of a number of war graves. For many Estonians, the memorial symbolises a time of occupation, deportation and grief. The government stated that moving the statue and the remains from the centre of Tallinn to a cemetery was more suitable and would help societal unity.

## KEY ACTORS

**Ministry of Defence of Estonia**  
**CERT-EE** Estonia's Computer Emergency Response Team  
**NATO**

**Toomas Hendrik Ilves** President of Estonia (2006 – 2016)  
**Urmat Paet** Minister of Foreign Affairs of Estonia (2005 – 2014)  
**Andrus Ansip** Prime Minister of Estonia (2005 – 2014)  
**Vladimir Putin** President of the Russian Federation (2000 – 2008, 2012 – present)  
**Sergei Ivanov** First Deputy Prime Minister of the Russian Federation (2007 – 2008)  
**Sergey Lavrov** Foreign Minister Russian Federation (since 2004)  
**Jaap de Hoop Scheffer** NATO Secretary General (2004 – 2009)

## NARRATIVES

### Estonian government

- The Bronze Soldier memorial is divisive due to different interpretations of history; its relocation to a cemetery will help national unity.
- The cyber attacks are a blatant attack not only on Estonia's sovereignty, but also on the entire EU and NATO.<sup>3</sup>
- The Russian government is at least indirectly responsible for these cyber attacks.<sup>4,5,6</sup>
- Estonia countered the attack very effectively.
- There is an urgent need to adapt and expand national and international law to address new threats such as cyber attacks.

### NATO

- Cyber attacks are a serious security issue.<sup>7</sup>
- NATO is providing technical assistance and political solidarity for Estonia.<sup>8</sup>

### Russian government

- The Estonian government's decision to move the Bronze Soldier memorial is disrespectful and sacrilegious, and will have serious consequences for bilateral relations.<sup>9,10</sup>
- Claims that the Russian government orchestrated the cyber attacks are false.<sup>11</sup> Independent 'patriotic' Russian groups and individuals were involved in the cyber attacks.

## KEY EVENTS

10 Jan 2007	26 – 27 Apr	27 Apr	28 Apr	4 May	9 May	19 May	Jan 2008
Government announces plan to relocate Bronze Soldier Memorial.	Excavation works begin around the Bronze Soldier Memorial. Peaceful protests soon turn into violent riots.	First wave of uncoordinated cyber attacks on high-profile websites begins (targeting major political websites and media outlets).	Coordinated fight-back effort of MoD together with CERT-EE begins, supported by other CERTs around Europe.	Second, more sophisticated and coordinated wave of cyber attacks, this time also targeting banks (esp. Hansabank and SEB Eesti Uhisbank). <sup>12</sup>	Attacks peak on Russian 'Victory Day.'	Cyber attacks abruptly and simultaneously cease.	Estonia indicts one of the responsible hackers.

## STRATEGIC LOGIC

The attacks appeared to be spontaneous and self-organised, with 'patriotic' non-state actors claiming involvement. If the attack was indeed orchestrated by a state actor, the difficulty of attributing responsibility for cyber attacks made it easy for a state actor to credibly deny involvement. However, the synchronisation of the cyber operations with other strategically ambiguous measures, hostile statements by Russian officials, and the

Russian government's lack of support for Estonia's efforts to resolve the attacks indicate that this was very likely a coordinated act of hostility, and that the cyber attacks – if not directed by the state – were at the very least not discouraged. It is reasonable to assume that there was a strong focus on how Estonia (and its partners) sought to manage a response to the attack.

## MEASURES

**DIPLOMATIC.** Public statements by President Putin and other officials harshly criticised Estonia's plans to relocate a Soviet-era war memorial. Protesters besieged Estonia's Embassy in Moscow for a number of days.

**INFORMATION.** By targeting media and many other websites, the cyber attack aimed to prevent Estonian citizens from obtaining information (i.e. news, updates from the government, bank balance) in the way they were accustomed. By interrupting, or making less reliable and instant, the access to information, the attack targeted Estonia's reputation as a digitally-advanced state.

**MILITARY.** There were no accompanying military exercises, movement of forces, or provocative actions. Falling short of the threshold for invoking Article V was likely a strategic imperative.

**ECONOMIC.** Increased friction at the Russian-Estonian border included lengthening of border checks, the severing of rail links due to unscheduled 'repairs' and the cancellation of orders from Russian businesses. The Russian First Deputy Prime Minister called on Russians to boycott Estonian goods and services in response to the relocation of the monument.<sup>13</sup>

**FINANCIAL.** Targeting banks and other financial institutions indicated that attackers were aware of the vulnerability of e-services to DDoS disruption. The web-interfaces for internet-based services of the two biggest banks in Estonia were offline for up to 90 minutes, and foreign money transfers were temporarily unavailable.<sup>14</sup>

**INTELLIGENCE.** It is reasonable to assume that intelligence gathering on vulnerabilities and specific target identification occurred, as the attacks were disciplined in nature, and effects were restricted inasmuch as they did not cause existential or irrevocable damage. Given the likely involvement of organised criminal networks, the identification and clearance of these individuals, as well as monitoring and payment would have required reliable intelligence activity.

**LEGAL.** Ambiguity was a key characteristic of this attack. Although it was clearly illegal under national and international law, the aftermath of such an attack is almost impossible to prosecute given the difficulty of identifying responsible individuals living in Russia – even if such evidence were gathered, it would likely be inadmissible because of the way it was obtained, and would reveal intelligence collection capability.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Actual and perceived political stability, good governance, and security. Public confidence in the government, military and security structures.

- Liberal democratic systems such as Estonia depend upon the free flow of information.

- Estonia was, and is, one of the world's most digitally connected societies,<sup>15</sup> and is critically dependent on the internet and related services.

- It is critical to national security to minimise the vulnerability of information systems, and ensure the security of national databases and registries.<sup>16</sup>

- Estonia's reputation as a business-friendly state, where inner- and inter-state movement of funds is safe and reliable, is an important resource for the country.

- National unity, minimisation of friction between different societal groups, especially regarding the significant Russian-speaking community.

### VULNERABILITIES

- Estonia's highly developed information infrastructure simultaneously made the country vulnerable to disruption from cyber attacks.

- DDoS attacks, the predominant form of attack used here (although other attack types were employed as well), exploit the vulnerability of unprotected websites and web-enabled resources to succumb to the direction of massive amounts of internet traffic. Automated and reactive measures could have been put in place to prevent this vulnerability.

- Around 330,000 of Estonia's 1.3 million inhabitants are ethnic Russians,<sup>17</sup> many more have Russian as their first language. The Russian Federation has a history of manipulating this community to strategic benefit by promoting instability.

### THREATS

- Exploitation of identity politics, different understandings of history, a largely symbolic act to cause civic unrest.

- Use of hijacked resources, and criminal networks with smart command and control. In the 2007 cyber attack, a combination of professional attackers and entry-level users of DDoS and other tools created a smokescreen.

- Disrupted information flow, which threatened to have a psychological effect on citizens and the confidence of businesses and investors.

### EFFECTS

- Although the direct effects of the cyber attacks were contained, the incident demonstrated the ability of hostile state actors to inflict asymmetric damage and disruption without needing to draw on conventional and escalatory forms of force. The attack was first and foremost an act of communication.

- Polls showed that public confidence in the government actually increased after the Bronze Soldier riots,<sup>18</sup> although trust of Russian-speakers in the government decreased and social divisions increased.

- Increased resilience, capability and capacity of Estonia (as well as other states and international organisations such as NATO). Increased international cooperation over cyber defence.

- Implementation of a national cyber security strategy 2008-2013. Establishment of a 'Cyber Defense League' and the NATO Cooperative Cyber Defence Centre of Excellence (both initiatives had been planned before the attack, but gained new importance in the aftermath).<sup>19</sup>

# US TRANSIT CENTER AT MANAS

## SUMMARY

In 2001, the US established an air base<sup>1</sup> at Manas International Airport in Kyrgyzstan as an air mobility hub to support Operation Enduring Freedom – Afghanistan (OEF-A). This base was of strategic importance to the US and its allies, with responsibility for the aerial refuelling of coalition aircraft, airlift of supplies and equipment, movement of coalition personnel and building partnerships with the Kyrgyz population.<sup>2</sup> Although the facility was costly, it provided much safer and more reliable access to Afghanistan than the routes available through Pakistan.

Kyrgyzstan received significant remuneration for the lease, securing USD 318 million in direct investment,<sup>3</sup> as well as indirect financial and non-financial benefits. Russia, however, increasingly pressured Kyrgyzstan to close to the Transit Center at Manas (TCM), wary of a long-term US military presence in the region. Russian offers of financial and economic assistance were intertwined with verbal threats to restrict US-Kyrgyz relations, especially concerning economic cooperation.

Russia also attempted to shift Kyrgyz public opinion against the US facility, in particular through Russian media channels, which focused extensively on accidents related to the base and frequently fabricated or exaggerated negative aspects of the Transit Center.

Kyrgyzstan was thus caught in an apparent dilemma between US and Russian assistance. For over a decade, the Kyrgyz government balanced these opposing pressures with some success. Successive Kyrgyz Presidents used the increasing Russian pressure and growing anti-American public opinion in Kyrgyzstan as bargaining chips in their efforts to increase US payments. However, mostly as a result of rampant corruption prevalent in the national government, Kyrgyzstan failed to use this cash injection to minimise its economic vulnerabilities. Despite intense efforts by the US to keep the Transit Center open, including a wide range of outreach efforts towards the Kyrgyz population, a parliamentary vote in 2013 ended the lease with the US government and the facility was closed in 2014.

## KEY POINTS

- While the Russian Federation used primarily economic instruments as leverage, this was integrated with diplomatic and informational measures. Identifying and countering any potential threat requires the ability to assess adversarial activity across the full spectrum of military and non-military means.
- Economically vulnerable states should pursue long-term strategies that minimise their economic vulnerabilities or be prepared to accept risk concerning their national security interests. Earning “easy cash” without further positive implications can escalate into further economic and political dependence on external powers.
- It is likely that public opinion was a significant factor in the political decision to close the base. If a country is assessed to be vulnerable to outside influence, every effort should be made to identify and understand those key target audiences which hold the balance on domestic consent for government policy.



Photo by Staff Sgt. Travis Edwards, U.S. Air Force/Released

## CONTEXT

■ **Kyrgyzstan.** Like all former Soviet territories, Kyrgyzstan was subject to Soviet policies of collectivisation, Russification, and economic integration with the wider USSR. These policies left a legacy of Russian language and by extension, consumption of Russian-language mass media, as well as close political and economic links with Russia. Kyrgyzstan is one of the poorest countries in the region. The state has been heavily dependent on Russia, although Chinese economic influence has been growing in recent years.

■ **The Transit Center at Manas.** The Transit Center was located at the Manas International Airport, a civilian installation situated 20km north of the capital, Bishkek. The US base shared the airport's 4,200-metre runway. On average, 1,200 to 3,500 coalition troops passed through Manas every day, and between 6 and 13 million pounds of cargo passed through the base every single month.<sup>4</sup>

■ **Financial Aspects.** The Kyrgyz government negotiated with the US to increase payments from the agreed figure of USD 2 million to USD 17.4 million in 2006, rising to USD 60 million annually from 2009.<sup>5</sup> The airport also collected a fee of USD 7,000 for every take-off and landing, and all of the fuel was purchased locally. The US provided assistance to Kyrgyzstan, such as infrastructure improvements, economic development, and counter-terrorism initiatives.<sup>6</sup> Overall, the Transit Center at Manas contributed about USD 40 million per year to the Kyrgyz economy from its first year, and employed around 500 Kyrgyz nationals.<sup>7</sup>

■ **Corruption surrounding the TCM.** Most of the US payments were syphoned off by the regime, flowing to private companies with close links to the Kyrgyz government, and never reached the Kyrgyz population. Technically, these contracts did not violate any US laws or procedures,<sup>8</sup> but the lack of transparency in these financial transactions had a significant impact on domestic political discourse.

## KEY ACTORS

Russian Ministry of Foreign Affairs  
US Department of Defense  
US Department of State

Askar Akayev *President of Kyrgyzstan (1991 – 2005)*  
Kurmanbek Bakiyev *President of Kyrgyzstan (2005 – 2010)*  
Almazbek Atambayev *President of Kyrgyzstan (2011 – 2017)*  
Vladimir Putin *President of Russian Federation (2000-2008, 2012-present), Prime Minister (1999 – 2000, 2008 – 2012)*  
Dmitry Medvedev *President of Russian Federation (2008 – 2012), Prime Minister (since 2012)*

# NARRATIVES

## Kyrgyz government

- Kyrgyzstan receives substantive economic advantages from allowing the US to use the Manas facilities (since 2001).
- The US needs to provide more economic incentives if it wants to continue using the Manas facility (since 2006).
- Kyrgyzstan needs Russia politically and economically; therefore Russia's interests have to be respected (since 2011).
- There is no requirement for US troops to be at a civilian airport just outside the capital (since 2011).

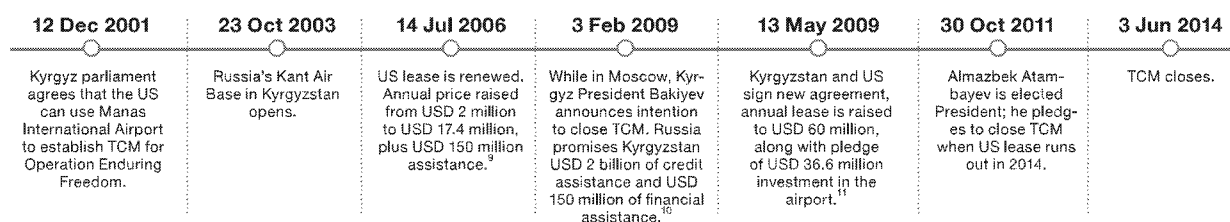
## Russian government

- The base at Manas is destabilising regional security.
- Kyrgyzstan needs to choose between the US and Russia. Economic cooperation with Russia will far outperform closer cooperation with the US.
- The US has hidden and hostile intentions with the facility.

## US government

- The TCM is crucial for the US and its mission in Afghanistan.
- The TCM has no negative impact on Kyrgyzstan, but actually contributes to regional stability.
- Kyrgyzstan receives meaningful economic aid in exchange for allowing the use of the Manas facilities.

# KEY EVENTS



# STRATEGIC LOGIC

Russia used a number of measures to pressure Kyrgyzstan to close the US base at Manas. It employed both carrots and sticks – financial and economic assistance combined with hostile rhetoric – to further its interests,

especially concerning economic cooperation. Russia also attempted to influence Kyrgyz public opinion against the US base through Russian-language media.

# MEASURES

**DIPLOMATIC.** Kyrgyzstan announced significant decisions regarding the TCM preceding or following visits of Russian officials or during visits to Russia. Russian officials publicly criticised Kyrgyz decisions that contradicted Russian positions.

**INFORMATION.** Russian state and private media are widespread in Kyrgyzstan. The closure of the TCM was a popular topic amongst Russian-language media, much more so than in the Kyrgyz media.<sup>12</sup> Russian and Russian-language media often fabricated or exaggerated negative aspects of the US Manas facility, emphasising accidents, the negative impact on the environment, and focused on rumours surrounding fuel dumping, US espionage, and drug-trafficking from Afghanistan via Manas.<sup>13</sup> One incident, in particular, was widely reported by Russian media: in 2006, a local truck driver was fatally shot at an entry control point by a US serviceman, which caused outrage among the population. In 2009, there were also

reports of possible Russian cyber attacks against Kyrgyzstan,<sup>14</sup> but linkage to the TCM is not proven.

**MILITARY.** In 2003, Russia established its own air base (Kant) in Kyrgyzstan, likely as a symbolic counterbalance to the US base.

**ECONOMIC/FINANCIAL.** Economic and financial instruments were primary elements of Russian influence. Kyrgyz decisions relating to a possible closure of the TCM were preceded or succeeded by announcements of Russian assistance (in 2009, Russia agreed to provide a USD 2 billion credit and financial aid worth USD 150 million,<sup>15</sup> and in 2012 Russia agreed to write off Kyrgyzstan's debt of USD 489 million<sup>16</sup>). Russia also pressured Kyrgyzstan to join the Eurasian Economic Union (EEU), which would compensate for the loss of US financial aid and further integrate Kyrgyzstan into a Russian-centred economic space.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Consolidation of democracy and the values associated with it.
- Peace and security in the country and the surrounding region.
- Economic sovereignty, economic sustainability and development.
- Sovereignty of the information space.

## VULNERABILITIES

- Corruption of political elites, which also affected the money flows surrounding the TCM.
- Regional instability, terrorist activity in the wider region.
- Weak national economy, economic dependence on Russia (close links in trade, investment, ownership of assets, and workplaces for Kyrgyz expats).
- Poor journalistic standards; strong presence of Russian-language mass media in Kyrgyzstan, which might decrease the reach of alternative points of view.

## THREATS

- Risk of democratic backsliding.
- Closure of the Russian market to Kyrgyz companies and individuals; reduction or halting of economic and financial assistance from Russia; further dependence on Russia.
- Influencing of public opinion through misinformation (either deliberate or due to lack of journalistic standards).

## EFFECTS

- Democratic backsliding: Kyrgyzstan's participation in the War on Terror provided international legitimacy, and the international community noticeably muted human rights concerns.<sup>17</sup>
- Despite extensive outreach efforts to the local population by the Mission Support Group at Manas, Kyrgyz public opinion gradually tilted against the TCM over the years (likely resulting from dissatisfaction over corruption, negative reporting on the TCM, and the context of deteriorating US-Russian relations).
- Increased bargaining power of Kyrgyz government vis-à-vis the US due to pressure from Russia and domestic public.
- Cooling of US-Kyrgyz relations after the closure of the TCM; Kyrgyzstan has since re-approached Russia, which partly compensated Kyrgyzstan for the loss of US payments.

# THE SPREAD OF SALAFISM IN EGYPT

## SUMMARY

The Kingdom of Saudi Arabia (KSA) has supported Salafite charities, websites and media channels as well as the Salafite Nour Party in Egypt. This support has taken various forms, ranging from ideological guidance to material assistance. Money is believed to come mainly from members of the Saudi royal family, businesspeople, or religious leaders via Muslim charities, rather than through official state channels.<sup>1,2</sup> The KSA likely pursues two main goals in promoting a sympathetic religious ideology in its neighbouring country – firstly, countering the Muslim Brotherhood, which it perceives to be a domestic and regional threat, and secondly, influencing Egypt's internal debates and political processes. This dynamic should be seen in the broader context of Egypt-KSA relations, as well as the interconnectedness of political power struggles and religious movements in the region.

In the years before the revolution in 2011, the spread of Salafism in Egyptian society was greatly facilitated by a number of Salafite TV

channels, reaching people more easily than local mosques and organisations, and the work of Salafite charities, which reached millions of poor Egyptians by providing them with essential services such as food, healthcare and literacy classes. Although KSA support of these media outlets and charities was not originally perceived as a national security threat by authorities, the Egyptian government started to take measures to control foreign funding from 2008 onwards.

After the revolution, the previously apolitical Salafite movement developed a political arm, the Nour Party, which was surprisingly successful in the country's first democratic elections, coming second after the Muslim Brotherhood's party. Accusations of covert funding from the KSA have been frequent (although not yet backed by hard evidence), and the Nour Party has openly supported or pushed for policies favourable to the KSA (e.g. handover of two Egyptian Red Sea Islands to the KSA; position on Syria).

## KEY POINTS

■ Existing divisions in society are a vulnerability which can be readily exploited by malign influence. In the case of Egypt, widespread poverty and youth unemployment have provided a key target audience for KSA-sponsored Salafite ideologues. Their vulnerability to Salafite jihadism also provides a national security threat to Egypt.

■ Tracking money flows presents a significant challenge since donations often come from private individuals, and Egypt suffers from a severe lack of transparency and widespread corruption.

■ Foreign funding is not always perceived as a threat. Foreign funding debates in Egypt usually revolve around western funding, rather than funding from the Gulf.

## CONTEXT

■ **Egypt-KSA relations.** For much of the latter half of the 20th century, Egypt and the KSA have had a close relationship; this was mainly due to the fact that Egypt relied on the KSA for security, political and economic support, while the KSA have counted on Egypt as a strong and experienced military force to counter what they perceive to be an expansionist Iran.<sup>3</sup> The KSA supported President Mubarak until he was deposed in 2011. Bilateral relations took a downturn after the Muslim Brotherhood came to power in Egypt, and the Saudi government allegedly gave General Sisi USD 1 billion to overthrow the Morsi government.<sup>4</sup>

■ **Salafism in Egypt.** Contemporary Salafism originated in Egypt in the late 19th century as an intellectual movement aiming to rediscover a purer and more literalist interpretation of Islam which adherents believe the early Muslims practised.<sup>5</sup> Salafism has many similarities to Saudi Arabian Wahhabism. Salafism in Egypt draws its support mainly from the poor.<sup>6</sup> Some estimates indicate that Salafites control around 4,000 mosques in Egypt (3.5 per cent of all mosques) and have over three million followers (3.2 per cent of Egypt's population).<sup>7</sup> Salafites are often described as an apolitical, "quietist" movement<sup>8</sup> – unlike the Muslim Brotherhood, which has strong political aspirations – which may be a key reason why the Egyptian government tolerated Salafism for a long time to counter the influence of the Muslim Brotherhood.<sup>9</sup>

## KEY ACTORS

**Salafite Call** *Egypt's largest Salafite society*

**Nour Party** *the 'Party of Light'; political party founded by Salafite Call after the 2011 revolution*

**Muslim Brotherhood** *transnational Sunni Islamist organisation*

**Egyptian Ministry of Awqaf** *in charge of religious endowments, has administrative control of Egyptian mosques and regulates religious discourse through state-approved imams and sermons*

**Hosni Mubarak** *President of Egypt (1981-2011)*

**Mohamed Morsi** *President of Egypt (2012-2013)*

**President Abdel Fattah al-Sisi** *President of Egypt (since 2014)*

**Abdullah bin Abdulaziz Al Saud** *King of Saudi Arabia (2005-2015)*

## NARRATIVES

### Major Egyptian Salafite groups

- Promotion of ultra-conservative positions, but renouncement of violence.
- Denying receiving financial support from Gulf states.
- Call for non-participation in the 2011 protests during the 'Arab Spring'.

### Salafite Nour Party

- Frequent support of KSA-friendly policies (even when these contradict Egyptian policies).
- More recently, maintaining that Sisi's government is conducting a hostile media campaign against the Nour Party.

### Egyptian government

- Foreign funding of political parties is illegal and undermines national security.
- The KSA is hardly mentioned in the context of foreign funding; discussions usually revolve around western funding.
- Promotion of moderate Islam, especially the teachings of Al Azhar University.
- Wariness of ultraconservative Salafite teachings.

### KSA government

- Support for the coup that removed Mohamed Morsi from power; antipathy towards Muslim Brotherhood.
- Denial of government funding for Egyptian Salafites.



## KEY EVENTS

2005	2006	25 Jan 2011	11 Feb 2011	5 Jun 2011	Nov 2011 – Jan 2012	3 Jul 2013	Sep – Nov 2013	Oct – Dec 2015
Muslim Brotherhood (MB) wins 20 per cent in parliamentary elections.	Government grants licenses to air to Salafi TV channels, likely to counter MB influence. <sup>10</sup>	Egyptian Uprising begins; 'Salafi Call' society discourages its followers from taking part in protests.	Mubarak steps down. Many new media companies and satellite channels (many of them Salafi) are founded in the following months.	Salafi Nour Party is officially licensed.	Parliamentary elections, MB's party wins 47.2 per cent, Nour Party wins 24.3 per cent. Both enter into an uneasy 'marriage of convenience'.	The MB's Morsi is deposed in a coup led by General Sisi; the Nour Party supports the coup.	The Nour Party unsuccessfully tries to preserve Islamic references in the Egyptian constitution.	Parliamentary elections, Nour Party wins only 11 seats and accuses government of arresting its members and conducting a hostile media campaign

## STRATEGIC LOGIC

The KSA's likely aim of promoting Salafi ideology in Egypt and other countries is "to consolidate their political and ideological influence by establishing a network of supporters capable of defending the kingdom's strategic and economic interests."<sup>11</sup> Another motivating factor for promoting Salafism might also be the KSA government's fear of the growing strength of the Muslim Brotherhood, which it perceives as both a domestic and regional threat and which is supported by Qatar, as well as regional rivalry with Iran. Egypt's Salafis have taken up many of the tactics of the Muslim

Brotherhood to spread their ideology, by building public trust and support through providing basic services such as food and education to the poor. The rural poor have been the main constituency of the Salafi Nour Party, which promotes many KSA-friendly policies. Money rarely flows via official government channels, but mostly comes from Salafi charities and private individuals residing in the KSA, usually in the form of "zakat" (alms to the poor, one of the five pillars of Islam).

## MEASURES

**INFORMATION.** Egyptian Salafi groups benefit from a combination of educational, scholarly, and ideological support from the KSA. A large amount of free Wahhabi literature is distributed in mosques and other public institutions.<sup>12</sup> Adnan al Khtiry, a well-known KSA cleric, gave a speech in Egypt in 2011 in which he urged Egyptian voters to support the Nour Party and other Islamist candidates.<sup>13</sup> Satellite channels have become very popular and effective in spreading Salafism, featuring prominent preachers that often reach a celebrity-like status. Many of these Salafi-themed TV channels are believed to receive private funding from Gulf states, or are owned by Saudi investors.<sup>14,15</sup>

**MILITARY/INTELLIGENCE.** Some Salafi Jihadist groups re-emerging in the Sinai Peninsular since 2011 have been accused of receiving financial support from the KSA's intelligence service and certain Wahhabi charities.<sup>16</sup>

**ECONOMIC/FINANCIAL.** 'Salafi Call', the Nour Party's parent organisation, is believed to be the biggest Egyptian recipient of funds from the KSA, and it is estimated that 30 per cent of these funds were/are transferred to the Nour Party to win political votes.<sup>17,18</sup> While direct financial ties have not been proven, there are many recorded instances of unusually high spending by the Nour Party (in particular during election campaigns) which have given rise to that suspicion. Many Egyptian Salafi NGOs and charities, which provide essential social services and education to the population, receive funding from Gulf countries, especially the KSA.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Political self-determination, independent political processes free from foreign interference.
- Domestic security, especially since one of President Sisi's main sources of legitimacy lies on his pledge to eradicate terrorism.
- Economic development and stability, which President Sisi is attempting to achieve through some reforms.
- Economic independence and energy security.
- Cohesion and unity between different societal groups.

### VULNERABILITIES

- High unemployment rate and lack of opportunities, especially for young people. Over a quarter of Egyptians live under USD 2 per day.<sup>19</sup> Poverty and unemployment are fertile ground for religious extremism.
- Crippled economy since the Arab Spring, which makes Egypt more vulnerable to outside influence, and KSA offers of support become more attractive.
- Shortage of foreign exchange (not least due to loss of tourism income due to instability).
- High levels of corruption and a lack of political will to fight it (many Egyptians believe that Salafi political parties would be less corrupt).
- Rapid population growth (but decrease of resources and arable land).

### THREATS

- Growth of Salafi and other militant jihadi groups (terrorist attacks have steadily grown in numbers and have become more sophisticated).
- Regional instability, especially in neighbouring Libya and Sudan. Arms smuggling across the Libyan border.
- Growing sectarianism: extremist Salafi ideology contributes to growing divisions in society and encourages anti-Shia and anti-Coptic sentiments.
- Foreign sponsoring of a political party is a threat to any country's independent decision-making process.

- Over-reliance on Gulf money. Easy cash allows the government to put off highly necessary but painful reforms. Economic dependency has also been used as leverage by the KSA on several recent occasions (e.g. territorial bargaining in 2017: planned handover of two Egyptian Red Sea Islands to the KSA in exchange for aid and investment).<sup>20</sup>

### EFFECTS

- Growing popularity of Salafism in Egypt, presumably achieved in part thanks to the work of Salafi charities, and the wide reach of Salafi TV channels and websites.
- Development of political Salafism after the 2011 revolution. The astounding success of the newly formed Nour Party in the first free elections is likely due to hidden sources of funding which allowed it to compete in almost every district with significant resources. The Nour Party's declining influence since then can be attributed to internal fighting and splits within the party, and President Sisi's efforts to keep the party at arm's length.
- Gradual and visible increase in religious conservatism over the last twenty years in Egypt, as well as increased sectarian violence.<sup>21</sup>
- Growing awareness of the Egyptian government of the threat posed by Salafi extremism. Counter-efforts include the promotion of more moderate alternatives, closure of some Salafi TV channels, investigations of NGOs over foreign funding, and removal of certain Salafi books from Egyptian mosques.

# DISINFORMATION IN SWEDEN

## SUMMARY

In June 2015, a Swedish government proposition for a new National Defence Policy triggered a nation-wide debate about rebuilding Sweden's 'total defence' capacity and the remilitarisation of the strategically important island of Gotland. During this domestic debate, a report by a US think tank, the Center for European Policy Analysis (CEPA), also stimulated pro-NATO discourse, claiming that Sweden was not able to defend itself against a qualified opponent without NATO support. Joining the debate, *Sputnik* published the English-language news article "Sweden Getting Ready to Fire Missiles at Russian Troops from Gotland Island", suggesting that Sweden intended to attack Russia.

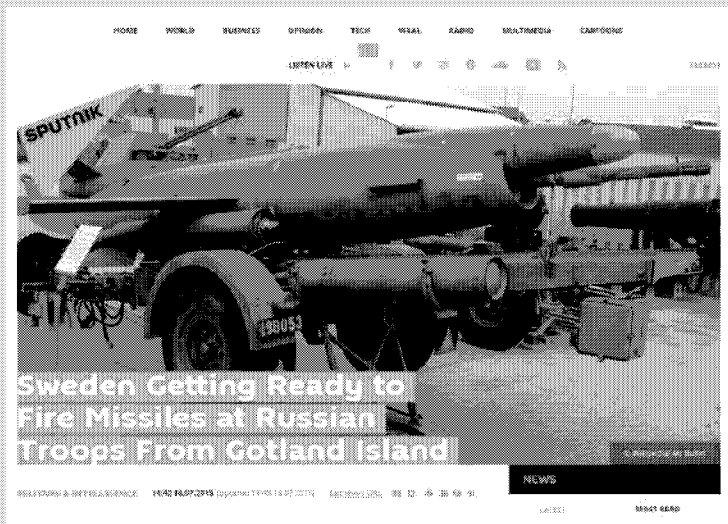
The report used statements from the County Governor of Gotland and a well-known military commentator, but removed context, and mistranslated and distorted their remarks. *Sputnik* did not quote the original source but instead referred to third-party sources in different languages. Although *Sputnik*'s low readership figures suggest that this article had no wider effect in itself, the incident provides an excellent example of the systematic means by which Swedish domestic media debates are used as part of wider influence strategies by pro-Russian actors.

## KEY POINTS

- The *laundering of information* describes the technique of taking original source material and 'laundering' it through intermediaries to obscure their origins. Typical methods include the deliberate mistranslation of key statements and the removal of context. Misquoting is commonplace in news media, but in this case, it is almost certain that the distortion of the source was not a product of an editorial process, but a deliberate attempt to deceive and part of a systematic effort to further polarise Swedish debates on national security.

- Through *framing and agenda setting*, single incidents of disinformation can be used to influence a country's public debate about national security and should be understood within the longer-term development of strategic narratives.

- In this case, officials repeated many lines that – in the context of systematic disinformation activities – were open to exploitation by hostile actors. Minor changes to original quotes are enough to alter their meaning significantly. This underlines the need for training across government to improve awareness of information-based threats and develop media presentation skills at the lowest levels of national authorities.



## CONTEXT

- **Sweden and NATO.** Although Sweden is not a NATO member, it actively cooperates in peace and security operations and exercises with NATO and NATO nations. Discussions about formal membership regularly resurface and are heavily polarised in public debate. In 2014, public support for membership increased to almost 50 per cent,<sup>1</sup> likely in response to Russian aggression in Ukraine.

- **Swedish defence policy 2016–2020.** The government's proposition 2014/15:19 on defence measures was approved by the Swedish parliament with a majority of 75 per cent on 16 June 2015. The proposal outlined a series of measures aimed to strengthen Sweden's defence – alongside political, diplomatic, and economic tools under the rubric "total defence" – against a perceived threat from Russia. It includes an increase in defence expenditure of 10.2 billion SEK (around USD 1.3 billion).

- **Gotland.** The island of Gotland occupies a strategically important location along shipping lanes from St. Petersburg, Helsinki, Tallinn, Riga and Stockholm to Copenhagen and the North Sea. In June 2015, the Swedish government announced that a permanent battle group would be based at Gotland beginning in 2018.

- **Pro-Kremlin media.** *Sputnik* is a media organisation established in 2014 by the Russian government-controlled news agency *Rossiya Segodnya* and operates in over 30 languages. It is widely considered to be a major source of systematic disinformation.<sup>2</sup> The Swedish language site was launched in April 2015 and closed in March 2016. Stories are often re-writes of existing material from major bureaus and other national news outlets, with alternative narratives drawn from right-wing sources.<sup>3</sup>

## KEY ACTORS

**Swedish Ministry of Defence**

**Sputnik News**

**Center for European Policy Analysis (CEPA)** a non-profit think tank dedicated to the study of Central and Eastern Europe; partly funded by NATO

**Peter Hultqvist** Swedish Minister for Defence (2014 – present)

**Cecilia Schelin Seidegård** County Governor of Gotland (2010 – present)

**Peter Mattsson** Lecturer at the Swedish Defence University; one of the foremost commentators for the Swedish press on Russian military

**Viktor Tatarintsev** Russian Ambassador to Sweden (2014 – present)

# NARRATIVES

## Swedish government

- Russia is a potential threat to Sweden, but should not be exaggerated.
- NATO membership is a multifaceted issue.
- Swedish defence of Gotland is important for regional security in the Baltic Sea.

## CEPA

- US involvement is vital for regional security in the Baltic Sea.
- Russian military activity in the Baltic Sea is a security threat.
- Allied defence of Gotland is vital for regional security in the Baltic Sea.

## Russian government

- There is an irrational fear of Russia in Sweden; key communicators in Sweden are aggressive and warmongering.
- The US is demonising Russia to encourage Swedish NATO membership.
- Sweden's increased defence spending is destabilising the Baltic Sea.

# KEY EVENTS

16 Jun 2015	24 Jun 2015	28 Jun 2015	30 Jun 2015	15 Jul 2015	16 Jul 2015	17 Jul 2015
Swedish Parliament approves total defence measures policy.	CEPA publishes report on Baltic security, claiming that Russian military exercises had included scenarios for the seizure of Gotland. This report stimulates public debate in Sweden.	Governor of Gotland is quoted in <i>Expressen</i> : "It's very necessary to have a permanent defence here. We need people on the ground prepared for a possible invasion."	Governor of Gotland speaks on a panel at Almedalen: "We usually say that we are an aircraft carrier. You can launch a war [on mainland Sweden] from Gotland."	<i>Sverige Radio</i> quotes Governor of Gotland (articles in Russian and German): Gotland "could be used as an aircraft carrier in the middle of the Baltic Sea, which could be used by Russia during a possible invasion of the Baltics." Summary of article appears in Russian news agency <i>Regnum</i> .	<i>Sputnik</i> (in French): "Swedish Official: The Island of Gotland is Well-Placed to Bomb Russia."  <i>Sputnik</i> (in English): "Sweden Getting Ready to Fire Missiles at Russian Troops from Gotland Island."	Governor of Gotland issues clarification of her comments.

# STRATEGIC LOGIC

The technique used in this case study of disinformation is the *laundering of information*. This describes a process similar to money laundering – the process of legitimising dirty money by obscuring its illegal origins – adapted to the information environment. In this case, the process is reversed, by taking information and laundering it through intermediaries to deliberately distort the original meaning. These intermediaries cite authentic sources but do so with minor changes to the text and by

removing the original context and meaning. *Sputnik* then refers to these intermediaries as its sources for the falsified quote. The result is a "dirty" quote that has been "laundered" via intermediaries to appear legitimate. Fake news and disinformation sources may also be legitimised through this process and the *Sputnik* article should be seen as part of a broad range of disinformation techniques.

# MEASURES

**DIPLOMATIC.** Russian politicians and diplomats frequently intervene in Swedish domestic affairs regarding NATO and Baltic Sea security.<sup>4</sup> The Russian President and Foreign Minister have openly warned Sweden against NATO membership.<sup>5</sup>

**INFORMATION.** *Sputnik* is one example of how disinformation is used with the aim of undermining Swedish society and weakening confidence in public and private sector institutions.<sup>6</sup>

**MILITARY.** Russia has a long history of violating Swedish airspace and waters. This has contributed to an increased sense of threat to national security that places public concerns about Russia at only a marginally lower level than the threat from international terrorism.<sup>7</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

■ Public debates surrounding political decision-making on defence matters. In this case, the debates concern the level of threat from Russia, Sweden's relationship with NATO, the level of funding of the Swedish military, and the relationship between Gotland and the Swedish mainland.

■ Effective Swedish defence, outlined the government's proposition 2014/15:19, which emphasises the concept of "total defence" to stress the necessity of collaboration between military and civilian defence, with a particular focus on the roles of government agencies and local government.

## VULNERABILITIES

■ Open and democratic debate can also turn into a weakness when actors deliberately seek to leverage pre-existing ideological divisions (e.g. sentiments regarding immigration or NATO) to suit other ends. Polarised domestic debates are fertile ground for foreign influence.

■ The territorial vulnerability of Gotland and the debate about remilitarising the island is exploited in the *Sputnik* article discussed here.

## THREATS

■ Hostile influence on domestic political debates by spreading disinformation (here: through mistranslation and removing statements from their original context) by news sources like *Sputnik*. This is especially concerning when debates surround issues of national security.

■ Skewing of debates also threatens to lead to stronger social divisions regarding polarised topics.

## EFFECTS

■ Increased government and public awareness of the threat posed to national security by Russian information warfare. Many initiatives related to countering disinformation and fake news, bursting filter bubbles, and source criticism have been launched in Sweden or have been supported by Swedish actors.

■ This specific *Sputnik* article discussed here does not seem to have had any effect in influencing debates or decisions (except for potentially reinforcing certain minority opinions). CEPA's report was far more effective in setting the agenda for Swedish discussions on NATO membership by increasing public awareness. *Sputnik* lifted a narrative that may fit with conspiracy theories about Swedish aggression against Russia and re-militarisation.

# HAMAS' USE OF HUMAN SHIELDS IN GAZA

## SUMMARY

Hamas, an Islamist militant group and the de facto governing authority of the Gaza Strip, has been using 'human shields' both defensively and offensively in conflicts with Israel since 2007. According to the Statute of the International Criminal Court (ICC), the war crime of using human shields encompasses "utilizing the presence of a civilian or other protected person to render certain points, areas, or military forces immune from military operations."<sup>1</sup> Hamas has launched rockets, positioned military-related infrastructure-hubs and routes, and engaged the Israeli Defense Forces (IDF) from, or in proximity to, residential and commercial areas.

The strategic logic of human shields is based on an awareness of Israel's desire to minimise collateral damage, and of Western public opinion's sensitivity towards civilian casualties. If the IDF uses lethal force and causes an increase in civilian casualties, Hamas can utilise that as a legal instrument, accusing Israel of committing war crimes, which could result in the imposition of a wide array of sanctions. Alternatively, if the IDF limits its use of military force in Gaza to avoid collateral damage, Hamas will be less vulnerable to Israeli attacks. Moreover, despite the Israeli public's high level of support for the Israeli political and military leadership during operations, civilian casualties are one of the friction points between Israeli left-wing and right-wing supporters.

Israel's efforts to avoid civilian casualties have been multifaceted: the IDF imposed restrictions on the use of force in the vicinity of civilians and focussed on precision airpower to reduce the risk of collateral damage. Moreover, the IDF has taken to warning residents to evacuate prior to an impending air strike (by dropping leaflets, phoning residents, or firing missiles without explosive warheads onto the roof), although in doing so they lose the element of surprise, and Hamas frequently used the warning to encourage civilians to gather at the targeted site. As part of a wide range of legal safeguards within the IDF's operational chain of command, the IDF's international law unit (the "Dabla") has to approve each target to ensure compliance with international law.<sup>2</sup> Moreover, the IDF has taken pains to explain their targeted strikes to both internal and external audiences, in particular via social media.<sup>3</sup> Nevertheless, Israel has not managed to dominate the narrative, with many international organisations and foreign governments accusing Israel of using disproportionate force.

## KEY POINTS

- The use of human shields can be considered an example of 'lawfare' – i.e. the use of the legal system against an enemy by damaging or delegitimising them, tying up their time or winning a public relations victory.<sup>4</sup>
- Even if a targeted strike may be justifiable from a legal perspective, first impressions frame the narrative. Public opinion tends to be influenced more by images depicting the suffering of innocent civilians than by well-thought-out legal arguments.
- National governments should be able to justify their position publicly and reveal their adversary's use of civilians in combat. This can only be accomplished by thoroughly documenting incidents, preparing supportive messages, and working across multiple channels to convey those messages.
- Priority should be given to information activities aimed at the very civilians who are used as human shields, in order to undermine the adversary and convince civilians to actively or passively refuse to serve as human shields. Such activities need to be coherent and consistent and coordinated.



## CONTEXT

■ **Use of human shields.** Hamas is not the only militant organisation using human shields – it was in fact inspired by Hezbollah's strategy in Lebanon.<sup>5</sup> Other Palestinian organisations such as the Islamic Jihad Movement in Palestine, the Popular Resistance Committees (PRC), or the Humanitarian Relief Foundation (IHH) have also resorted to human shields. Even the IDF have used human shields in the past; however this practice

was declared unlawful by the Israeli Supreme Court, and several officers were court-martialled for applying the technique.<sup>6</sup> Typical uses of human shields include launching attacks from densely populated civilian areas, locating military infrastructures in civilian areas, or protecting terrorists' houses and military facilities.

## KEY ACTORS

**Hamas** *Palestinian fundamentalist Sunni organisation that has been designated by the US, the EU and other countries as a terrorist group*  
**Israeli Defense Forces (IDF)**  
**Israel Security Agency (Shabak / Shin Bet)** *monitors terrorist activity in the Gaza Strip and the West Bank*  
**Israel Ministry of Foreign Affairs**

**Ismail Haniyeh** *former Prime Minister of the Palestinian National Authority, current head of Hamas Political Bureau in Gaza, has frequently encouraged Palestinians to act as human shields (e.g. to climb to the roofs of houses targeted by the IDF)*

**Khaled Mashal** *head of Hamas Political Bureau (1996 – 2017)*

# NARRATIVES

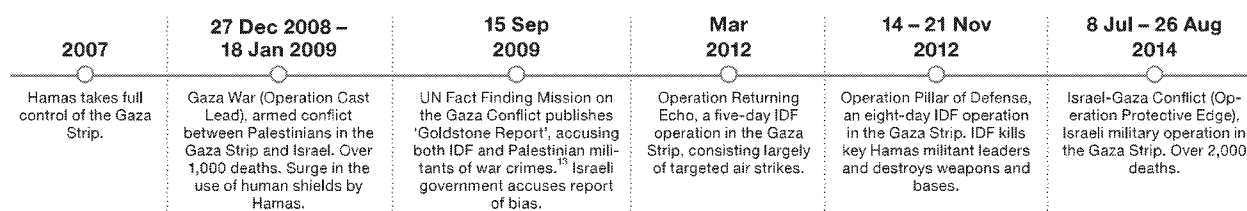
## Hamas

- Israel commits war crimes and is indiscriminately killing Palestinian civilians.
- The Palestinian people support Hamas unconditionally, even if that means risking their lives.<sup>7</sup>
- It is the Palestinian people's religious and national duty to serve as human shields, in order to serve the resistance and support its cause.<sup>8</sup>
- Israel's early warning messages before an airstrike are psychological warfare.<sup>9</sup>

## Israeli government

- Israel uses military force to protect its citizens in light of Hamas' aggression. It only targets Hamas' military facilities and militants.<sup>10</sup>
- Civilian casualties are caused by Hamas' use of human shields to protect its assets. Israel actively engages in all possible efforts to avoid harming civilians, including alerting them before strikes.<sup>11</sup> The IDF often cancels planned strikes when there is a risk to civilians.
- The Palestinian population in the Gaza Strip is subjected to Hamas' terror and does not support the movement's use of human shields.<sup>12</sup>

# KEY EVENTS



# STRATEGIC LOGIC

The dense, heavily populated Gaza Strip provides the ideal setting for a terrorist and paramilitary organisation. The region consists of a variety of populated areas both organised and unorganised, temporary and permanent, aboveground and under the surface. Those areas, comprising of cities and refugee camps (which are even more densely populated), enhance the defender's advantage. Hamas' defensive and offensive strategies are based

on leveraging these advantages in combat with the IDF, inspired by Hezbollah's strategy in Lebanon.<sup>14</sup> The objective of this strategy is to maximise the IDF's casualties while protecting Hamas' forces and infrastructure from the IDF's military supremacy. This strategy accepts the possibility of civilian casualties, and even leverages these for internal and external propaganda.

# MEASURES

**DIPLOMATIC.** Incidents of civilian casualties are recorded by Hamas, and the (frequently manipulated) footage disseminated across a wide array of media channels (esp. social media, satellite TV channels).<sup>15</sup> During the fighting itself, Hamas' aims its communications efforts mainly at the local Palestinian population to build resilience; post-conflict communications are aimed primarily at the international community to cause reputational damage to Israel and limit its strategic choices by controlling the narrative. The use of human shields is aimed at earning points in the global arena, by delegitimising Israel's use of force, creating continuous pressure through international institutions (e.g. UN and EU) and NGOs, and promoting sanctions and prosecution by international tribunals. Since the international community does not recognise Hamas as the political representative of the Palestinian people, its diplomatic activities are usually carried out by third-party states and pro-Palestinian organisations (e.g. presenting 'proof' of alleged war crimes).

**MILITARY.** Use of primary military force from within densely populated areas (e.g. launching of rockets and mortar shells), from which Hamas conducts operations while blending in with the local population (e.g. wearing civilian clothing). Hamas thus responds to the IDF's military and technological supremacy by creating an asymmetric equation, leveraging terrain advantages and using civilian populations to protect their military assets.

**ECONOMIC.** Hamas uses the damage caused to civilians and civilian infrastructure as a justification to raise funds from its donor nations (e.g. Qatar, Turkey) and other allies. Hamas also uses (and pays) civilians to dig tunnels, which are a primary source of revenue, commodities, arms and fighters for Hamas, and conceals their entry points beneath civilian buildings.<sup>16</sup>

**LEGAL.** Hamas aspires to exploit Israel's commitment to normative and explicitly defined international law. Using human shields provides Hamas with a win-win scenario: if the IDF uses kinetic force and the number of civilian casualties surges, Hamas can accuse the IDF of committing war crimes; if the IDF limits its use of force to avoid collateral damage, Hamas will be less susceptible to Israeli attacks. Hamas operates effective mechanisms to gather any potentially incriminating information that could prove that the IDF committed war crimes in Gaza. Once evidence is gathered, Palestinian supporters (usually lawyers) will file complaints against Israel in courts of European nations. Hamas skilfully manages to prolong reputational losses for Israel through the time it takes to have cases heard and adjudicated to their advantage.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Effective defence of Israeli territory and the lives of its citizens.
- International reputation as a country that abides by international law.
- Good relationships with Israel's allies.
- Unity within Israeli society during and after military operations.

## VULNERABILITIES

- From a purely military perspective, Israel's commitment to international law limits its ability to freely terminate the threats posed by Hamas.
- Civilian casualties are one of the friction points within Israeli society: although the Israeli public generally supports its political and military leadership during operations, left-wing groups will usually question the outcomes of the operations.
- Dependency on international support as a cornerstone of Israel's foreign policy.

## THREATS

- Human shields limit the IDF's ability to effectively combat Hamas with their technological and military supremacy. The launching of attacks from heavily populated areas also makes critical Israeli infrastructure more vulnerable to rockets and mortar shells.
- Increased divisions within Israeli society over civilian casualties.
- Increased tension between Israel and its allies over excessive force.

## EFFECTS

- Over the years, Israel's public image has suffered tremendously due to reports and images of civilian casualties. Hamas efforts in controlling the narrative have been successful. Almost every large-scale conflict in the Gaza Strip resulted in an international investigation committee, usually led by the UN, to examine whether IDF operations were lawful. Even Israel's closest allies (e.g. UK, Germany, France) have widely criticised Israel's actions.
- The IDF put certain limitations on the use of force<sup>17</sup> and developed more accurate means to strike individuals and infrastructure. It has also taken to warn civilians residing in the proximity that an attack is approaching, thus allowing civilians to evacuate, but limiting the effect of a surprise attack.<sup>18</sup>

# THE 2010 SENKAKU CRISIS

## SUMMARY

The Senkaku Islands are a group of five uninhabited islands and three islets located in the East China Sea. They are under the administrative control of Japan, but are also claimed by China and Taiwan. The Senkaku Islands are of great economic value due to rich fishing grounds and significant oil and gas deposits in the surrounding exclusive economic zone (EEZ). The islands are also of great geostrategic value, facilitating control over the East China Sea.

In September 2010, a Chinese fishing trawler refused Japanese Coast Guard (JCG) requests to leave Senkaku territorial waters. After a stand-off, the trawler rammed two JCG vessels and after a 40 minute chase, the JCG boarded the Chinese trawler and arrested the 15 man crew and captain. The captain was later tried under Japanese domestic law. In response, China drastically curbed its rare earth elements (REE) exports to Japan, whose high-tech oriented economy is very dependent on Chinese REE imports. These hostile economic measures were accompanied by a number of other escalatory measures, including

rhetorical threats, the encouragement of popular protests across China, and the arrest of four Japanese nationals in China for allegedly photographing military targets. All these measures were implemented with various degrees of ambiguity. Short-term, China wanted to force Japan to release the detained trawler captain; long-term, China wanted to demonstrate its ability to use a potent economic instrument as deterrent and as coercive measure or for punishment.

The Japanese government came under strong domestic criticism for the way it dealt with the crisis, in particular for releasing the Chinese captain after several weeks without indicting him. Citizens took to the street to protest both China's behaviour and the "weakness" of the Japanese government. Video footage proving the deliberate nature of the boat ramming was not released to the wider public, likely out of fear of further diplomatic clashes with Beijing.<sup>1</sup> The footage was eventually leaked online and led to increased criticism of the Japanese government for keeping details of the incident from the public.

## KEY POINTS

- This was an example of a small incident which escalated into an international diplomatic crisis. While it is highly unlikely that the Chinese fishing trawler was acting under direct command of Beijing, the incident was still readily exploited for strategic gain.
- Adversarial measures relied heavily on ambiguity. The two key aspects included the informal nature of the embargo on REE and the involvement of a non-state actor (civilian fishing vessel) as catalyst for the conflict.

- In response to such flexible and adaptive StratCom approaches, nations should focus on the consistency and coherence of government messaging, rather than trying to decipher deliberately ambiguous statements and actions.

- Analysing the 2010 Senkaku crisis from the perspective of 2017, it very much resembles an initial engagement used to test the opponent's defences and potential international reaction. The political tensions between China and Japan resurged in 2012 and remain elevated, with the islands as one focal point of the confrontation.

## CONTEXT

- **The role of the US in the dispute.** The US-Japan Treaty of Mutual Cooperation and Security (TMCS) provides a legal framework for stationing of US military bases in Japan, and commits both parties to assist each other in case either of them is attacked on Japanese territory. However, the Senkaku Islands are only covered implicitly in treaty, and the US does not formally take sides in the Senkaku dispute. In August, just before the crisis, Japanese media reported unverified sources claiming that the Obama administration was unwilling to include the Senkaku Islands under the protection of the TMCS, which prompted speculation in Japan about the strength of US security guarantees.<sup>2</sup>

- **EEZ violations.** Japan treated past territorial violations by illegal fishing in the exclusive economic zone of the islands as a criminal matter rather than a political issue. Occasional stunts by anti-Japan activists to

reach the islands by sea have sometimes reignited bilateral tensions; Tokyo committed to a "deport-not-detain" policy. In the months prior to the September 2010 crisis, violations by illegal fishing increased considerably.

- **Rare Earth Elements (REE).** REEs, a set of 17 chemical elements, are a critical component in the production of a wide range of technologically advanced civilian and military products. Since the early 2000s, production has been dominated by China: in 2009, Japan depended on China for around 90 per cent of its REE needs.<sup>3</sup> From the mid-2000s, China began to impose production and export quotas on the domestic REE industry, citing environmental concerns. In July 2010, the amount of planned REE exports for H2 2010 was slashed by 72 per cent compared to the same period in the previous year.

## KEY ACTORS

### Ministry of Foreign Affairs of China

**Baodiao Movement** A social movement in China, Hong Kong and Taiwan that defends Chinese sovereignty over the Diaoyu/Senkaku islands

### Ministry of Foreign Affairs of Japan

### Japanese Coast Guard (JCG)

### Ministry of Foreign Affairs of Taiwan

### US Department of State

**Wen Jiabao** Premier of China (2003 – 2013)

**Naoto Kan** Prime Minister of Japan (2010 – 2011)

**Seiji Maehara** Foreign Minister of Japan (2010 – 2011)

**Wu Den-yih** Premier of Taiwan (2009 – 2012)

**Barack Obama** President of the United States (2009 – 2017)

**Hillary Clinton** Secretary of State of the United States (2009 – 2013)

**Robert M. Gates** Defense Secretary of the United States (2006 – 2011)

## NARRATIVES

### Chinese politicians and state-controlled media (unified front)

- Japan's actions are illegal and unreasonable.
- The Senkaku Islands are rightfully China's.
- China has not imposed any REE embargo.
- Both parties should be careful not to escalate this situation; Japan and China need each other and should work together to compromise.

### Japanese political elite (divided, criticised each other)

- Reaffirmation of Japan's right to the Senkaku Islands; fervent anti-Chinese rhetoric.
- Underlining the necessity to prevent escalation and find a solution.
- Criticism of Naoto Kan's handling of the crisis, "national humiliation."

### Taiwanese government

- Criticism of Japan's actions in the Senkaku/Diaoyu area; calling for de-escalation and calm approach.
- Assertion of Taiwan's claims to the islands as part of greater Chinese territory, while also distancing Taiwan's diplomatic position from that of China.

### US government

- Proposing US as potential mediator; bilateral talks to solve the dispute.
- No public confirmation of US obligation to defend the Senkakus under TMCS, but reaffirmation of general support for Japan.

## KEY EVENTS

7 Sep 2010	7-14 Sep	8-18 Sep	11 Sep	19 Sep	20 Sep	21 Sep	24 Sep	2 Oct	29 Nov
Chinese fishing trawler rams two Japanese Coast Guard vessels. JCG detains captain and crew.	Japanese Ambassador is summoned 6 times to meet high-level Chinese officials.	Anti-Japanese protests across China (Beijing, Shanghai, Hong Kong).	China suspends talks with Japan on joint exploration of gas and oil resources in East China Sea.	China suspends ministerial and provincial-level contacts with Japan.	4 Japanese nationals are arrested in China for allegedly trespassing military zone and taking photos.	China unofficially restricts shipments of unprocessed REE exports to Japan (e.g. salts, oxides, metals).	Japan releases Captain Zhan Qixiong.	Large protests across Japan against the gov's handling of crisis and China's behaviour.	REE shipments to Japan are fully restored.

## STRATEGIC LOGIC

China's behaviour was characterised by a significant degree of escalation both *vertically* (the severity of measures) and *horizontally* (the number and diversity of measures).

China's actions were highly ambiguous. As the captain of the civilian fishing trawler was reportedly drunk<sup>1</sup> at the time of the incident, the Japanese were unable to attribute political responsibility to China for the incident, nor prove that the action was a result of a planned hostile political action conducted

by a proxy. The detention of four Japanese individuals was arranged so that there was no direct evidence of a connection with the detention of the Chinese captain. The disruption of REE shipments to Japan was also highly ambiguous, as it was (a) officially denied by Beijing, (b) a manipulation of the work pattern of the customs officials, (c) introduced in circumstances conducive to supply disruption (i.e. post drastic reduction of REE export quotas).

## MEASURES

**DIPLOMATIC.** Frequent summoning of the Japanese Ambassador by the Chinese MFA. Suspension of bilateral contacts on ministerial and provincial level. Tolerance of anti/Japanese protests across China.

**INFORMATION.** Coordinated anti-Japan campaign by Chinese state-controlled media.

**MILITARY.** No use of conventional military capabilities, but use of paramilitary units (vessels belonging to the Fisheries Law Enforcement Command) to challenge Japanese control over Senkakus. Vessels reached contiguous zone, but did not violate territorial waters.

**ECONOMIC.** Restriction of REE export quotas (2 months before the crisis, Beijing announced a massive reduction of REE export quotas for H2 2010 by 72 per cent compared to H2 2009, which created a fragile situation for Japanese importers). Disruption of REE shipments to Japan from 21 September<sup>2</sup> (Chinese customs officials refused to process new orders and prevented dockers from loading shipments which were already processed; Chinese authorities repeatedly denied having imposed any additional re-

strictive measures). Variety of threats to Japanese economic interests (including calls for boycotts of Japanese products and for the disruption of Japanese business operations in China through blockades or even vandalism of Japanese-owned assets).<sup>6</sup> Suspension of several bilateral economic initiatives (including joint exploration of natural resources in East China Sea). Transport of equipment to offshore platforms located in disputed part of the EEZ in the East China Sea.<sup>7</sup>

**INTELLIGENCE.** Given the extensive links between the China state security apparatus and various Chinese nationalist groups, it is likely that Beijing played an instrumental role in supporting and organising anti-Japanese protests in Hong Kong and Taiwan, in particular the Baodiao movement.<sup>8</sup>

**LEGAL.** Detention of four Japanese nationals on 20 September for allegedly trespassing into a military zone (the dubious nature of the charges and the coincidence with Japan's 19 September decision to extend the arrest of the Chinese captain indicate that this was a component of Beijing's countermeasures).

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Coverage of Senkaku Islands by the Japan-US security treaty (TMCS).
- Enforcement of effective control around the Senkaku Islands, demonstrating Tokyo's de facto ownership. Ensuring desired geostrategic position of Japan in the East China Sea.
- Stability of the high-tech manufacturing sector.
- Maintenance of public order and cohesion of Japanese society.
- Maintaining credibility of the official narrative regarding the Senkaku Islands ("Senkakus are legally part of Japanese territory," "no territorial disputes exist," "Japan is capable of effectively enforcing control over area").

### VULNERABILITIES

- Weakened domestic position of PM Kan and the ruling DPJ party (barely survived leadership challenge in August). Presence of militant pacifist and nationalist factions in Japanese society, both groups could be exploited by a potential adversary to impose political cost on the Japanese government.
- Trilateral and asymmetric nature of the territorial claims (Japan's claims are contested by both China and Taiwan; anti-Japanese sentiment could bring China and Taiwan closer together).
- Deterioration of US-Japanese relations following the DPJ's victory in the 2009 elections: DPJ had demanded more equal relations with US. Ambiguity surrounding US commitment to defend Senkaku Islands.
- Anti-Japanese sentiment in the region due to Japan's WWII history. Significant constraints on use of military force (i.e. Article 9 of Japanese Constitution). Lack of permanent military or administrative infrastructure on the islands. Private ownership of three out of five Senkaku Islands, which may prevent Tokyo from exercising optimal level of control.
- Significant economic reliance on China.<sup>9</sup> High and quasi-structural dependence on Chinese supply of REE.

### THREATS

- The Japanese government was put in a delicate position where potential (real or perceived) under- or over-reaction would likely provoke a domestic political crisis. Social unrest due to perceived weakness of government.

- Demonstration of Tokyo's lack of effective control over the area by increased number of incursions and maritime confrontations. Tolerance of Chinese incursions might result in Beijing establishing a quasi-permanent presence of para-military units of fishermen militias and coast guard.
- Formation of a unified anti-Japanese front between China and Taiwan over Senkaku Islands.
- Disruption of Japan's high-tech manufacturing sector.
- Drainage of gas reserves from the disputed EEZ in the East China Sea.
- Mishandling of the crisis might create a political precedent, negatively affecting Japan's position in its other territorial disputes.

### EFFECTS

- Transformation of the Senkaku issue into a domestic political problem that severely weakened the government (PM Naoto Kan eventually resigned in 2011). The Senkaku Islands became an emotionally-loaded issue for the Japanese public. The 2010 crisis set a chain of events in motion which led to the 2012 Senkaku crisis (which was much more severe than the 2010 crisis).
- Significant deterioration of China-Japanese relations. Strengthening of nationalist anti-Chinese sentiment in Japanese society.<sup>10</sup>
- Short-term disruption of the Japanese manufacturing sector due to REE shortage. Massive short-term global REE price increase, followed by a medium-term decrease. Implementation of a variety of REE supply diversification strategies (e.g. increased REE recycling, seeking alternative sources of supply and substitutes, developing further strategic reserves). However, China managed to maintain its position as dominant REE supplier to Japan. Relocation of REE processing operations of several large Japanese companies to China, to limit the risk of supply disruptions.
- Domestic and international press coverage of the Japanese government during crisis was more negative than positive. The vague rationale of releasing the Chinese captain was perceived as sign of political inconsistency or even diplomatic incompetence.

# HUMANITARIAN AID IN THE RUSSO-GEORGIAN CONFLICT

## SUMMARY

During the Russo-Georgian conflict of 2008, the Russian Federation used 'humanitarian' assets in support of the separatist populations of Abkhazia and South Ossetia, two regions of Georgia which both declared independence in the early 1990s. The Russian government provided "significant quantities of food, water, medications, water purification facilities, diesel power plants, tents and other material resources,"<sup>1</sup> and set up refugee camps. On 11 and 12 August 2008, two large convoys were sent to South Ossetia's capital, transporting, amongst other things, "two mobile field hospitals [...], 58 tons of food supplies, 31 power generating stations, potable water and more than 200 rescue workers."<sup>2</sup>

The Russian government used what it termed 'humanitarian assistance' as an instrument to pursue broader policy goals that were not humanitarian in nature. Moscow relied on relief efforts and the language of humanitarianism to present itself as a neutral and impartial actor and to justify its continued support for the residents and de facto authorities of Abkhazia and South Ossetia, despite Georgian protests against its continued involvement. Russia thus exploited the tensions

between the laws surrounding territorial sovereignty and the imperative to provide effective relief to civilians.

In the larger context of the Russo-Georgian conflict, Russia's provision of humanitarian assistance played merely a secondary or indirect role, since other measures adopted by Russia (e.g. 'passportisation', economic assistance, arms supplies and eventually full military intervention) presented a direct and far more severe challenge to Georgia's national security. However, humanitarian assistance was of great diplomatic and information value, as it enabled Russia to portray itself as a neutral actor motivated by considerations of civilian protection. The humanitarian activities were also used to strengthen the political and social ties between Russia and the Abkhaz and South Ossetian populations and to weaken their allegiance to the Georgian state. Russia's 'humanitarian' activities demonstrated Georgia's incapability to prevent Russian intervention in its domestic affairs and physical territory, as well as its inability to assert its authority over Abkhazia and South Ossetia.

## KEY POINTS

- The instrumental use of law is not limited to armed conflict but also occurs in peacetime. The term 'lawfare' may be too narrow, if applied to describe the (mis)use of law as a substitute for conventional military means, to capture the instrumental use of legal arguments outside of armed conflict and the military context.

- There is a close link between legality and legitimacy, and between legal justifications and broader strategic narratives. Legal arguments can serve both as a source of legitimacy and as a tool to delegitimise an adversary. In the Georgian scenario, Russia used the law in an instrumental manner as part of a broader narrative, and its arguments were

designed to promote a narrative of legality and legitimacy, rather than to make a compelling legal case.

- Western nations and institutions should conceptualise law as a domain to counter the use of legal instruments when used in a hostile manner. This would also foster a more dynamic approach to the use of law and legal argument to counter hybrid threats.

## CONTEXT

- **Secessionist regions in Georgia.** Georgia gained independence from the USSR in 1991, although it immediately faced armed secessionist movements in the regions of South Ossetia and Abkhazia, which were actively supported by Russia. Particularly since the so-called Rose Revolution in November 2003 led to a pro-Western political environment in Georgia, Russian support of the secessionist regions is widely understood to be motivated by geopolitical considerations aimed at countering Western influence. The Russian Federation has a long history of providing humanitarian aid and assistance to the separatist regions, stretching back to the conflicts of the early 1990s.

- **The 2008 conflict.** From 2004 to 2008, relations between Georgia and the two separatist regions deteriorated sharply, as did Russo-Georgian relations. Violence intensified in the first half of 2008, followed by mutual accusations of preparations for war. Large-scale hostilities broke out between the Georgian and South Ossetian sides on 7 August, leading to

Russian intervention on 8 August and to active hostilities in the Abkhaz zone from 9 August. Armed conflict between Georgia and Russia lasted until 12 August. Approximately 850 people were killed and up to 3,000 wounded;<sup>3</sup> around 138,000 people were internally displaced.

- **International legal framework of humanitarian assistance.** The international community has not developed a single overarching legal regime to regulate the provision of humanitarian aid and assistance in a comprehensive manner. Different legal rules and considerations apply in times of peace and under the law of armed conflict. In the absence of armed conflict, the legal regulation of humanitarian assistance is caught between two competing imperatives: respect for the sovereignty of the affected state and the need to provide effective relief to the civilian population. A key question is whether or not humanitarian assistance falls foul of the principle of non-intervention in the absence of the territorial state's prior consent.

## KEY ACTORS

**United Nations Security Council**  
**EMERCOM** *Russia's Ministry for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters*

**Dmitry Medvedev** *President Russian Federation (2008 – 2012)*  
**Sergey Lavrov** *Foreign Minister Russian Federation (since 2004)*  
**Vyacheslav Kovalenko** *Russian Ambassador to Georgia (2006 – 2008)*  
**Vitaly Churkin** *Russian Permanent Representative to the UN (2006 – 2017)*  
**Mikheil Saakashvili** *President of Georgia (2008 – 2013)*  
**Irakli Alasania** *Ambassador of Georgia to the UN (2006 – 2008)*



# NARRATIVES

## Russian government

- Russia is acting for humanitarian reasons as an impartial and neutral actor.
- Georgia is an aggressor in this conflict and Russia is acting in self-defence. Russia is acting in conformity with international law, Georgia is not.<sup>4</sup>

## Georgian government

- Russia is an aggressor in this conflict and is violating international law.
- Russia's humanitarian motives and its claim to be an impartial actor are false.<sup>5</sup>
- Russia's core justification for intervention – a commitment to protect Russian citizens living in Georgia – are a pretext for other strategic aims.
- Russia is striving for de facto absorption of South Ossetia and Abkhazia.

## Western states and IOs

- Russia is failing to respect Georgia's political independence and territorial integrity and is violating international law.<sup>6</sup>
- Rejection of Russia's claim that it was acting in and against Georgia for humanitarian reasons or in the capacity as an impartial facilitator.<sup>7</sup>

# KEY EVENTS

Dec 1990 – Jun 1992	Aug 1992 – Sep 1993	Jun 2004	Jun 2005	Nov 2006	7 Aug 2008	8 Aug 2008	11 Aug 2008	12 Aug 2008
Armed conflict between Georgian government and separatists, after South Ossetia declares itself an independent republic within the USSR. Ends with Sochi agreement and peacekeeping operations.	Armed conflict between Georgian government and Abkhazian separatists, after Abkhazia declares its secession. Ends with ceasefire and CIS peacekeeping force.	Russia delivers humanitarian aid at the request of the South Ossetian authorities.	The mayor of Moscow sends a humanitarian convoy to South Ossetia.	Referendum in South Ossetia reaffirming independence from Georgia (backed by 99 per cent of voters). Russia begins granting Russian citizenship to South Ossetians.	Georgian forces attack South Ossetia's capital.	Russia launches a large-scale invasion of Georgia.	First Russian humanitarian convoy reaches South Ossetia.	Second Russian humanitarian convoy reaches South Ossetia. Russia and Georgia agree to a cease-fire.

# STRATEGIC LOGIC

Russian humanitarian assistance to Abkhazia and South Ossetia reinforced its image as a neutral arbiter both domestically and internationally, and reinforced its standing among the Abkhaz and South Ossetian populations. The scale of Russian aid indicates it was not simply a token gesture. Many aid agencies, including UNICEF,<sup>8</sup> credited EMERCOM with responding to the urgent needs of the South Ossetian population quickly and in a reasonably

effective manner.<sup>9</sup> However, several indicators suggest that Russia's humanitarian efforts were not motivated exclusively by humanitarian concerns, but fed into its diplomatic and legal justification for military intervention. Humanitarian assistance thus enabled Russia to create a narrative of impartiality and preoccupation with civilian protection, reinforcing its claim to be acting in self-defence and in accordance with an international mandate.

# MEASURES

**DIPLOMATIC/INFORMATION.** Russia's Permanent Representative to the UN claimed that Russia's actions against Georgia were necessitated both by the dangers faced by Russian citizens as well as by the need "to provide humanitarian assistance to refugees and other innocent civilians in desperate situations."<sup>10</sup> This narrative of purely humanitarian assistance was somewhat undermined by actions that cannot be seen as humanitarian, such as Russia's deployment of railway troops as part of its assistance to the Abkhaz authorities.<sup>11</sup> Russia's broader narrative of protecting Russian nationals living in Georgia and of self-defence are reflected in Russia's citizen and passport policy, which enabled the majority of Abkhaz and South Ossetian residents to become Russian nationals en masse through a simplified procedure.<sup>12</sup> The protection of nationals and the provision of humanitarian assistance thus formed mutually reinforcing strands.

**MILITARY.** Following the outbreak of hostilities in 2008, Russia deployed several thousands of regular forces into Georgia. Nothing suggests that Russia abused humanitarian aid to obtain a military advantage.

**ECONOMIC.** Russia has long played a vital role in the economic sustainability of Georgia's breakaway regions. In April 2008, President Putin ordered the strengthening of trade, economic, social and cultural ties with the authorities in Abkhazia and South Ossetia.

**LEGAL.** Russia employed legal arguments to support its actions in Georgia, including to justify humanitarian assistance. It repeatedly acted without the full consent of Georgia when providing aid to the secessionist regions. Russia thus exploited the tensions between the laws surrounding territorial sovereignty and the imperative to provide effective relief to civilians. The dividing line between the instrumental use and abuse of law is narrow; moreover, the law of belligerent occupation, to the extent that it applies to Russia, compelled Moscow to carry out humanitarian relief action.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

■ Excerpt from Georgia's National Security Concept (2006): "Infringed territorial integrity, that is, the existence of uncontrolled territories within Georgian borders, hampers Georgia's transformation into a full democracy. Therefore, reintegration of the state and restoration of the rule of law on the whole territory of Georgia is one of the top priorities of the national security policy. The state reintegration policy envisages participation of Abkhazia and the former Autonomous District of South Ossetia in developing the constitutional order of Georgia."<sup>13</sup>

## VULNERABILITIES

- The unresolved political status of Abkhazia and South Ossetia, and especially the fact that Georgia never established its full authority over these regions, rendered Georgia particularly vulnerable to Russia's actions.
- The Georgian government could not stop Russia from providing humanitarian aid without running the risk of escalation, or playing into the hands of Russia by strengthening Russian narratives.

## THREATS

- Strengthening of political and social ties between Russia and the separatist regions at the expense of weakened allegiance to the Georgian state.
- Undermining of Georgia's international standing by demonstrating its inability to prevent Russian interference in its internal affairs.
- Worsening of Georgia's relationship with Russia by increasing tension and carrying the risk for violent confrontation.
- Legitimation of Russia's actions in the eyes of third parties.

## EFFECTS

- Moscow's humanitarian actions demonstrated Georgia's incapability to prevent Russian intervention and its inability to assert its authority in the secessionist regions.
- Before 2008, the Georgian government responded to similar humanitarian activities by issuing official protest, or taking practical action (e.g. subjecting a Russian convoy to customs procedures in 2004).
- In 2008, Georgia did not take any action to stop Russian humanitarian relief efforts, but continued to call Russia's narrative of humanitarianism and neutrality into question. Georgian efforts seem at least to have convinced third parties, such as Western nations, which questioned Russia's narrative.

# CHINESE PUBLIC DIPLOMACY IN TAIWAN

## SUMMARY

The People's Republic of China's 'One China' principle – which sees Taiwan as an integral part of China – is a fundamental part of its foreign policy. China makes its 'One China' principle a non-negotiable aspect of its relations with other countries, part of a campaign to isolate Taiwan diplomatically in an attempt to force the Taipei government to negotiate. The aim of reunification with Taiwan is included in the Communist Party of China's 2049 'National Rejuvenation' centenary goals.<sup>1,2</sup>

In parallel to a number of more coercive measures (including employing diplomatic pressure and economic leverage), China pursues its 'One China' policy through public diplomacy – the means of engaging with foreign publics in service of the national interest – in an attempt to persuade the Taiwanese public of the benefits of 'One China' subordinated to Beijing. This public diplomacy includes promoting cross-Strait ties

through exchange programmes, workshops and expositions, providing economic and legal incentives making it easier for the Taiwanese public to invest or work in the Mainland, encouraging your people to study in the Mainland (for example through subsidised housing), as well as various efforts at influencing Taiwanese media.

In recent years, Taiwanese opinion polls indicate the results of these efforts have been mixed.<sup>3,4</sup> While Chinese efforts do not seem to have increased public support for reunification or curbed Taiwan's growing sense of national identity, this should be viewed within the context of China's broader presence on the international stage, its increasing economic and military might; ambitions to 'rejuvenate and reunify the great Chinese nation'; and continued refusal to rule out the rule of force to achieve reunification.

## KEY POINTS

- Opinion polls in Taiwan have shown that Chinese public diplomacy and soft power efforts in Taiwan have not led to more support for unification, nor a growing sense of pan-Chinese identity. A reason for this might be the generational gap: in particular the younger generation no longer have strong family and cultural ties to the Mainland. Some segments of the Taiwanese population might find China attractive from a pragmatic point of view – young people in particular are more open to studying and working in the Mainland – but China's political culture and socialist market economy are lacking appeal.

- Mainland China, not least due to its autocratic system, is able to pursue its coercive measures and public diplomacy efforts with governmental coherence and a unifying narrative of 'One China'. In contrast,

Taiwan has no such domestic consensus on national identity. Political parties in Taiwan differ over where Taiwan's roots lie, disagreeing on whether Taiwanese identity and language should mirror that of Mainland China, or whether a distinctly Taiwanese identity should be nurtured.

- Public diplomacy is a process of 'government to people' communication through engagement with foreign publics, using words and deeds to shape public opinion, but there should be boundaries. Such activities should be deemed hostile if they attempt to influence the population in a way that threatens to be hurtful to the target nation or undermines the ruling authority.

## CONTEXT

- **Taiwan and Mainland China.** Ever since the Chinese Civil War resulted in the incumbent Kuomintang (KMT) fleeing to the island of Taiwan while the victorious Communist Party set up a communist state in 1949, Taiwan and China have operated under two different authorities, each claiming to be the legitimate ruler of greater China. In 1992, a historic meeting took place in which leaders from each side of the Taiwan Strait met and forged an agreement on the existence of one China which became known as the '1992 Consensus.' While China's commitment to the principle of 'One China' has been unwavering since the founding of the People's Republic of China in 1949, Taiwan's successive governments have been more ambivalent, most especially in recent years.

- **Chinese coercive measures.** In addition to the public diplomacy efforts discussed in this case study, China has long employed more coercive measures in pursuit of its 'One China' policy: China actively pressures countries to formally accept the 'One China' principle as a prerequisite for official relations with China, leaving Taiwan increasingly isolated on the world stage. The 'One China' policy is also promoted in global civil society and business; for instance, multinational corporations such as airlines or hotel chains have faced strong pressure from Beijing not to list Taiwan as an independent country.<sup>5</sup> Taiwan is also heavily dependent on China economically (China receives 40 per cent of Taiwan's exports), giving China leverage over Taiwan. China's strong and growing military presence and refusal to rule out the use of force if peaceful means fail provide a threatening backdrop to its public diplomacy efforts.

## KEY ACTORS

**State Council Information Office (SCIO)** *the 'nerve centre' of China's public diplomacy apparatus, monitors Chinese media/internet as well as external communications*  
**Public Diplomacy Division** *located within the Chinese Ministry of Foreign Affairs' Information Department*

**Taiwan Affairs Office** *Chinese agency which implements Taiwan-related policy dictated by the State Council, including trade, media and cultural activities*

**Kuomintang (KMT)** *major Taiwanese political party (currently in opposition), leading Pan-Blue coalition parties which support eventual unification with Mainland China with the ROC as the legitimate government, advocates a Taiwanese identity rooted in Mainland China*

**Democratic Progressive Party (DPP)** *current majority ruling party, anti-communist and pro-independence, advocates a distinct Taiwanese identity*

**Mainland Affairs Council** *Taiwanese government agency tasked with Mainland-related affairs*

**Taiwanese Ministry of Culture** *promotes Taiwanese cultural and creative industries*

**Xi Jinping** *President of the People's Republic of China (since 2013)*

**Hu Jintao** *President of the People's Republic of China (2003 – 2013)*

**Tsai Ing-Wen** *President of Taiwan (since 2016), DPP, advocates maintaining the status quo in cross-strait relations*

**Ma Ying-Jeou** *President of Taiwan (2008 – 2016), Kuomintang, largely pro-unification*

**Chen Shui-Bian** *President of Taiwan (2000 – 2008), DPP (first non-Kuomintang President), pro-independence*

# NARRATIVES

## Chinese government

- China will never allow any part of Chinese territory to separate from the Mainland in any form.<sup>5</sup>
- Taiwan is an inalienable part of China and recognition of this is vital for any country wishing to maintain official relations with China.
- The Chinese government has the right to resort to any means necessary to safeguard territorial integrity and achieve the reunification of the two sides of the Strait.<sup>7</sup>
- Reunification is part of 'the great rejuvenation of the Chinese nation' (President Xi's vision for China).<sup>9</sup>

## Taiwanese Kuomintang (Pan-Blue coalition)

- Mainland China and Taiwan are both parts of the Chinese nation, and the government in Taipei is the legitimate ruler of this territory.<sup>9</sup> Status quo is favoured for now.<sup>10</sup>
- Taiwanese identity is of Mainland Chinese origin; the official Mandarin language brought over in 1949 should remain.

## Taiwanese DPP (Pan-Greens)

- Taiwan is a separate country from Mainland China and should be recognised as such.<sup>11</sup>
- Taiwanese identity is distinct from Mainland China (e.g. indigenisation policies of 2000-2008). Why should Beijing Chinese be spoken in a non-Mainland nation? What about dialects of Southern Chinese spoken in Taiwan by the settlers from the 17th century onwards, and languages of the original inhabitants and tribes pushed into the mountains by the settlers?

# KEY EVENTS



# STRATEGIC LOGIC

China's efforts of achieving reunification by winning the 'hearts and minds' of the Taiwanese people take various forms. First, China directly targets the Taiwanese public with public diplomacy to promote a latent pan-Chinese identity and increase public support for reunification. Secondly, China uses economic incentives to boost economic ties between China and Taiwan

and Taiwanese reliance on the Mainland as well as showing the Taiwanese public the benefits of closer relations with China. Finally, China has implemented various legal measures to better facilitate Taiwanese engagement with China.

# MEASURES

**DIPLOMATIC.** China's Taiwan Affairs Office (TAO) frequently makes public statements on the 'One China' principle, and – in place of official diplomatic visits – senior TAO personnel pay official visits to Taiwanese nationals studying or working in the Mainland.

**INFORMATION.** China encourages pro-Mainland businesspeople to buy Taiwanese media outlets, exerts pressure on Taiwanese media outlets which have investments or plan to invest in the Mainland, and purchases advertorials in Taiwanese media to promote pro-China narratives.<sup>12</sup> China also organises programmes and exchanges to develop closer ties between the Chinese and Taiwanese public and promoting a pan-Chinese identity, directed by the TAO.<sup>13</sup>

**ECONOMIC/FINANCE.** China has created a range of incentives and programmes aimed at bringing Taiwanese businesses and citizens to the Mainland to open up businesses and work, including sponsored workshops in the Mainland, subsidised housing, tax breaks, and even financial grants for Taiwanese youths.<sup>14</sup> There have also been alleged financial links between the Mainland and the pro-China 'Chinese Unity Promotion' party via the Triad gangs; investigations on this are ongoing in Taiwan.<sup>15</sup>

**LEGAL.** In March 2018, China implemented 31 legal measures making it easier for Taiwanese people to study, work and invest in the Mainland.<sup>16</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Deterrence and defence against any hostile military action.<sup>17</sup>
- Ensuring US presence and commitment to Taiwan and the region.
- Good cross-Strait relations to ensure peace and stability, and avoiding actions that Beijing could regard as provocative and use as an excuse to react.<sup>18</sup>
- As many international allies as possible, and a strong economy to balance against China.

## VULNERABILITIES

- Reliance on other countries for political support against potential Chinese assertiveness and in favour of Taiwanese autonomy.
- Taiwan's military is far smaller than China's and is heavily reliant on the US for protection.
- Economic reliance on China, which is Taiwan's largest trading partner. China's economic superiority enables China to leverage influence with Taiwan and third-party countries.
- Small, yet vocal, pro-Beijing and pro-reunification political parties and civil society groups. Social, familial ties between Taiwan and China.
- Taiwan's free press is vulnerable to outside financial and editorial influence, e.g. through sponsored content.

## THREATS

- Further isolation on the world stage.
- Continued refusal of China to rule out the use of force against Taiwan, and risk (however unlikely) of abandonment by the US.
- China's economic clout presents a threat as China increasingly focuses on the commercial and business interests of unification, or at least of encouraging closer ties with the Mainland.
- Influencing of public opinion through the Chinese strategy of encouraging pro-Mainland businesspeople to buy Taiwanese media outlets and purchasing advertorials in Taiwanese media.<sup>19</sup> This renders the public more susceptible to pro-Mainland narratives and could reverse the maturing sense of Taiwanese national identity.

## EFFECTS

- The number of countries recognising Taiwan has decreased due to targeted Chinese efforts (five switched allegiance in the last two years).
- China's policies and economic incentives have successfully increased Taiwanese economic dependence on China and facilitated greater numbers of Taiwanese people working in the Mainland. Especially young people are more pragmatic in their views of China-Taiwan relations and are open to working in the Mainland.<sup>20</sup>
- Despite China's public diplomacy efforts, polls have not shown an increase in pro-reunification views. Instead, a growing sense of national identity has been discernible, with an increasing number of people identifying as 'Taiwanese' rather than 'Chinese' or both 'Taiwanese and Chinese'.<sup>21</sup>

# DETENTION OF ESTON KOHVER

## SUMMARY

On 5 September 2014, Eston Kohver, an employee of the Estonian Security Service (KAPO),<sup>1</sup> was abducted at gunpoint by unidentified assailants in the border region between Estonia and Russia. The Estonian government maintained that a group of people had come across the border into Estonian territory to detain Kohver while he was working on an investigation into cross-border smuggling and a corruption case in the Pskov region.<sup>2</sup> He was later formally detained by the authorities of the Russian Federation and transferred to a prison in Moscow, where he remained prior to trial proceedings in Pskov. On 19 August 2015, Kohver was sentenced to 15 years in prison. 13 years of the sentence was judged for espionage and 2 years for illegal crossing of the border and carrying a weapon in Russian territory. According to the Estonian Ministry of Interior, Kohver met with Federal Security Service (FSB) officials several times at the border control point due to the investigation he was working on, therefore it is highly likely

that the FSB was aware of his duties and location.<sup>3,4</sup> Based on publicly available information, it is almost certain that Kohver was detained during a planned operation by professionals who targeted him at a specific location, and that at some point there was an incursion into Estonian territory from the Russian side of the border.<sup>5,6</sup> Meanwhile, the Russian Federation maintained that Kohver had crossed the border into Russian territory and was engaged in espionage activity.<sup>7</sup> The different versions of events put forward by both sides caused confusion and escalated an isolated local event into a diplomatic row.

A month later, in September 2015, Kohver was exchanged for Alexei Dressen, a convicted Russian spy and former official of the Estonian Secret Service. The swap took place some days before the visit of President Vladimir Putin to the United States on a bridge over the Piussa river which separates Russia's western Pskov region and Estonia's Põlva county.<sup>8</sup>

## KEY POINTS

- The Russian government framed events as that of a 'Cold War' status conflict with the West, portraying Western countries, especially NATO nations, as being hostile to Russia. This narrative of status conflict supported the interests of the Russian political establishment, which needs a well-established adversary to distract attention away from domestic issues. It reinforced the national image that President Putin has curated, that of international respect being rightfully restored to Russia as a powerful actor in the international system.
- Cases of espionage are usually handled outside of the public eye, but as Russian TV covered the story soon after the detention, the Estonian government was prompted to respond, initially playing down the incident and suggesting that it was not politically motivated but the work of local Russian commanders involved in the smuggling trade.<sup>9</sup>
- The case highlights the importance of understanding how threats in the information environment constantly evolve with changes in strategic context, and that relatively minor incidents can be framed by an adversary to sustain a narrative beneficial to their strategic aims.



IMAGE – The bridge exchange on 27 September 2015.

## CONTEXT

■ **East-West relations at the time of the incident.** The status conflict between Russia and the West escalated in late 2013 when the EU-Ukraine agreement was stopped by President Yanukovich, pro-European demonstrations started in Kiev and there were rising tensions due to the Russian annexation of Crimea, conflict in Ukraine and downing of

MH-17.<sup>10</sup> Two days before the detention of Kohver, US President Obama visited Estonia and made public statements about support to the Baltic nations. On the day Kohver was detained, the NATO Wales summit declaration condemned Russia's intervention in Ukraine and leaders agreed to reverse the decline in national defence budgets.

## KEY ACTORS

**Federal Security Service of Russian Federation (FSB)** state security organisation and successor of the KGB. Related primarily to internal security, but also plays a role in overseas espionage efforts

**Estonian Internal Security Service (KAPO)** responsible for maintenance of national security through collection of information and implementation of preventive measures as well as investigation of offences<sup>11</sup>

**Estonian Ministry of Foreign Affairs**

**Eston Kohver** employee of the Tartu Department of Estonian Security Police

**Maxim Gruzdev** contact that Eston Kohver was expected to meet at the border. Gruzdev was a Russian resident with double citizenship (Estonian and Russian)

**Jevgeni Aksyonov** public attorney appointed by Russian Federation to defend Kohver

**Alexei Dressen** native Russian-speaking former KAPO official of Volga German origin, who was born in Riga in 1968

**Uno Puusepp** a former KGB employee, later a KAPO technical specialist for ten years

# NARRATIVES

## Russian government

- Kohver was detained in the territory of the Russian Federation.<sup>12</sup>
- Kohver planned to hire an FSB employee called 'Ivanov' to work against Russia and for Estonia and the West.
- This investigation was carried out in strict compliance with Russian law and under the rules of criminal procedure, international law and the rights of an Estonian citizen.<sup>13</sup>

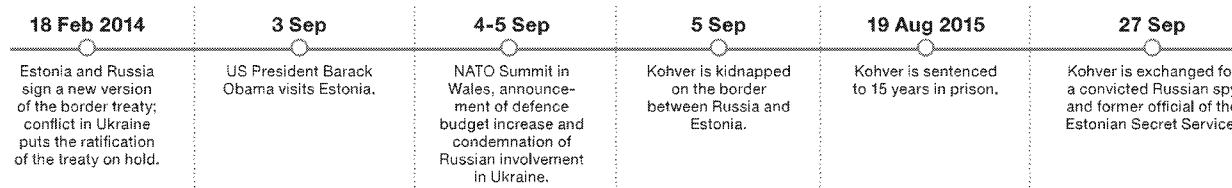
## Estonian government

- Eston Kohver, an Estonian official, was kidnapped in the territory of Estonia and forcefully taken to the Russian Federation.<sup>14</sup>
- The borderline was unguarded during the incident and tracking units were switched off presumably due to the ongoing anti-smuggling operation Kohver was involved in.
- There was a backup security team to support Kohver, but the team was unable to interfere during the kidnapping.<sup>15</sup> The Estonian Border Guard arrived at the scene within minutes and identified traces of a struggle and evidence that someone had come from the Russian Federation and went back there.<sup>16</sup>

## European Union

- Russia's actions were a clear violation of international law and it should act to fulfil international obligations.<sup>17</sup>

# KEY EVENTS



# STRATEGIC LOGIC

It is unclear if the actions undertaken by the Russian Federation were intended to be limited in scope and simply got out of hand, or were deliberately calculated to create strategic tension. Despite attempts by Estonia to downplay the event, the incident was exploited by the Russian media, with domestic coverage promoting a 'Cold War' narrative and Estonia used to represent NATO as an organisation inherently hostile to Russia. It is difficult to identify if the Kremlin wanted to elicit any specific response from Estonia because the Russian Ministry of Foreign Affairs was mostly unresponsive as events unfolded. The periods of significant media attention from

Russian media (press releases on detention, the demonstration of belongings related to Kohver, the swap operation and documentary on Puusepp) were mostly aimed at Russian domestic audiences. The main aim appears to have been to present the West as hostile to Russia and signal to NATO nations that cooperative security can be a messy business. It is also possible that Russia wanted to gain a bargaining chip to be exchanged for an FSB spy, or that it was simply testing a Western / Estonian response to a border incursion.

# MEASURES

**DIPLOMATIC.** Russia kept a low diplomatic profile during the period of detention. The few comments made by the Russian Foreign Ministry and commentary tended to refer to the case as a criminal matter not worthy of such international attention, suggesting an attempt to allow room for de-escalation of the whole affair.<sup>18</sup> The Embassy of the Russian Federation in Estonia drew parallels between the detention of Kohver and the detention of Yaroshenko and Seleznev in the United States, which reinforced the narrative of status conflict with the West.<sup>19</sup>

**INFORMATION.** Russian media coverage was relatively low profile apart from three phases: Immediately following the detention (including the demonstration of Kohver's belongings on TV), when former employee of KGB and later KAPO Uno Puusepp appeared in a documentary of him shown on the Russian channel NTV, and during the swap operation at the Piusa River. The detailed media reports on the bridge exchange of Kohver

and Dressen had echoes of an exchange in 1962, when Soviet spy Rudolf Abel (Vilyam Fisher) was traded for Gary Powers from US Air Force on the Glienicke Bridge of Havel River. In contrast to Kohver and his family, which did not appear in the media or made any public statements, Alexei Dressen gave several interviews and comments to the Russian media after his release. Russian media presented events to domestic audiences as a way of confirming the narrative that Western secret services conduct Cold War-style operations against them, with Estonia serving the role of ardent supporter of the West (US and NATO), who actively participate in anti-Russian provocation.

**INTELLIGENCE / LEGAL.** The operation during which Kohver was detained was pre-planned and carried out by professionals and they were aware of Kohver's location.<sup>20</sup> The FSB admitted responsibility for the act but did not acknowledge it occurred on Estonian territory.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- The 2010 Estonian National Security Concept defines internal security as aiming to guarantee a safe living environment and a society which is resilient to respond to threats.<sup>21</sup>
- Protection of constitutional order.
- Guarding the external border.
- Combating international organised crime.
- Development, preservation and protection of common values associated with social cohesion and a sense of security.

## VULNERABILITIES

- Inadequate border security and criminal activities such as unlawful border crossing, human trafficking and smuggling.
- Unclear legal status of the Estonian-Russian border (which is also the de facto NATO and EU border).

## THREATS

- Risk of diplomatic row escalating to include other measures.
- Lack of unified response to incident from NATO allies could affect cohesion and unity of the alliance.
- Russian press release on Kohver's detention that prompted the Estonian government to respond, unusual in intelligence cases.

## EFFECTS

- Estonia invested significantly in modernising its border security despite this being an issue of low political importance with limited economic benefit.<sup>22</sup>
- Fuelling of a Cold War-style East vs West narrative.
- Increased perception of risk of similar incidents occurring in other nations sharing borders with Russia and fear of escalation.
- Reinforced public support for Estonian Security Services.

# FINNISH AIRSPACE VIOLATIONS

## SUMMARY

From March 2014 there was a marked increase in close military encounters between Russia and NATO nations and partner nations, occurring on a regular basis and over a wide geographic area. These included airspace violations, near-miss mid-air collisions and maritime encounters.<sup>1</sup> In the same year NATO scrambled in response to more than 100 aeroplanes in European airspace, more than three times than it did in the previous year.<sup>2,3</sup> Some incidents could be considered routine or low risk, but high risk incidents have a high probability of casualties or a direct military confrontation.

Finland experienced two phases of such violations with two occurring in May and three in August 2014. In addition to the increased risk of collision with civilian aeroplanes, incidents were evaluated as threatening by Finnish officials concerning the stability of the relationship between Finland and Russia. Furthermore, they were referenced in the Finnish debate on potential NATO membership, in particular during

the run-up to Finland and Sweden signing Host Nation Support Agreements with NATO in September 2014.

During and after the incursions, Finland kept its communication and information channels with Russian representatives open, which decreased the risk of escalation and spontaneous reactions of actors. As public debate and statements of Finnish officials focused strongly on technical and safety issues of incursions, the possibility for cooperation and progress with Russia regarding agreements increased. Even though the Finnish response managed the impact of the incidents with regard to escalations of Finland-Russia relations, they put pressure on the Finnish government to address military and border safety issues and increased the focus of public debate on possible Russian threats if Finland were to join NATO. Significantly in the later part of 2014, Russia's unpredictability and actions in Ukraine increased public debate around NATO membership in Finland, more so than violations.

## KEY POINTS

- The airspace violations that occurred in Finland were part of an increase in close military encounters between Russia and the West in 2014, ranging from routine to high risk. High risk incidents have a high probability of casualties or a direct military confrontation and have a severe risk of escalation.<sup>4</sup>

- Airspace violations are an example of how force posture, through the use of airpower, can be used to achieve strategic effects. The framing of such incidents affects the way in which they are interpreted by audiences. National authorities need to be responsive, specific and consistent when communicating about such events, in order to mitigate the risk of unintended escalation.

- The violations of Finnish airspace in 2014 were barely covered in Russian media but covered extensively in Finland. Russia's silence indirectly created confusion within Finland as the public looked to the politicians for answers which were not provided by media or political commentary.

- According to both linguistic analysis and public polling, at no point did Finnish public opinion stray from the status quo of non-membership of NATO. Seeded in Finnish media is a public expectation to maintain balance and a wariness towards Russia's potential reactions (verbally linked to Russia's unpredictability). This is seen to limit the NATO debate from straying too far from the status quo of non-membership.



IMAGE – Finnish Karelia Air Command F-18 / SHUTTERSTOCK

## CONTEXT

- **Airspace violations.** An airspace violation occurs when a pilot enters controlled airspace without appropriate clearance. The term 'violation' does not necessarily imply a deliberate act. Such violations are usually committed by 'non-cooperative' military aircraft which have no flight plan in the ATM (Air Traffic Management) system, no communication with civil ATC (Air Traffic Control), no active transponder or no coordination with civil ATC.

- **Flight transponders.** Transponders transmit the plane's identifying letters and/or numbers, call sign, the transponder's serial number, altitude, air speed, and heading, as well as GPS coordinates. The presence of transponders makes the data public and available not only to pilots and air traffic controllers, but to everyone with an internet connection. Not all Russian military aircraft have a 'transponder' on board. Russian military planes are equipped with transmitters that automatically transmit encoded data to Russian military radars.

## KEY ACTORS

**Russian Embassy Helsinki**  
**Russian Ministry of Defence**  
**Karelia Air Command**  
**Finnish Border Guard (Division under Interior Ministry)**  
**Finnish Foreign Ministry**  
**Finnish Defence Ministry**

**Carl Haglund** *Finnish Defence Minister (2012 – 2015)*  
**Sauli Niinistö** *Finnish President (2012 – present)*  
**Erkki Tuomioja** *Finnish Foreign Minister (2000 – 2007 and 2011 – 2015)*  
**Alexander Stubb** *Finnish Prime Minister (2014 – 2015)*

# NARRATIVES

## Russian government

- Rejection of any account of incidents which blame the Russian military for risky or unprofessional behaviour.

- Not only Russian aircraft, but also aircraft of all NATO countries fly over the Baltic Sea without switching on their identification devices. The number of such flights by NATO over the Baltic Sea is twice that of Russian planes.<sup>5</sup>

- Amplifying reliance of Finland on bilateral economic ties in messaging, particularly following EU economic sanctions against Russia in July 2014.

## Finnish government

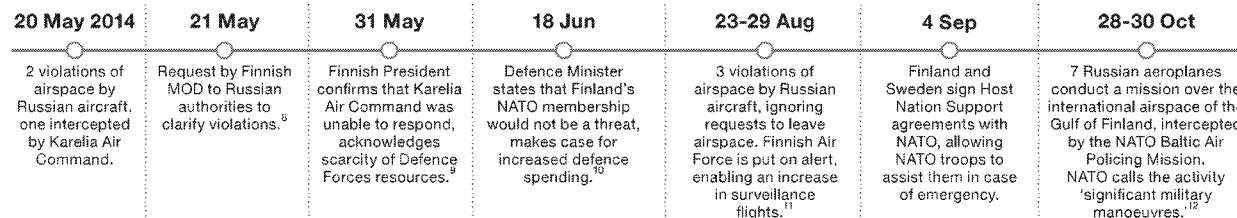
- These violations are serious and further steps will be taken, including stepping up air surveillance.

- Formal request for the Russian authorities to provide clarification of violations.<sup>6</sup>

- We wish to seek agreement to ensure that no flight will be made without transponder.<sup>7</sup>

- Rhetoric is centred around 'unpredictability' of Russia.

# KEY EVENTS



# STRATEGIC LOGIC

Ambiguity is a significant factor in this case study. The airspace violations may have been a deliberately hostile act intended as a demonstration of both Russia's military capability and their will to act in the air domain outside of the accepted rules of international aviation. The Russian Federation may not have intended to violate Finnish airspace and may have been merely negligent within an assessed margin of risk, but there is no evidence to indicate that they acted to prevent violations or regretted such

incidents when they occurred. When taken in context with an overall increase in military activity at that time, it is assessed that the Russian Air Force was authorised to act more aggressively towards NATO nations and partner nations such as Sweden and Finland. It is also likely that the Russian Federation was assessing patterns of response by testing the preparedness of specific military capabilities and the capacity for international cooperation.<sup>13</sup>

# MEASURES

**DIPLOMATIC.** Statements from Russian government/military officials, denying allegations of airspace violation. Violations can be interpreted as being political messages, especially when they occur close to important diplomatic events (e.g. Obama visit, NATO Summit Wales). Incidents can be interpreted as a way of putting Finland under pressure to sign a bilateral agreement which would risk undermining NATO and EU unity.

**INFORMATION.** By denying any wrong-doing and not commenting on the timing of the incidents, Russia created doubt about what had happened, why it had happened and what the next move might be.

**MILITARY.** Russian military aircrafts entering Finnish airspace, often with their on-board transponders turned off (allowed since military aircrafts are not bound by the International Civil Aviation Organisation's rules of the international airspace) and without filing flight plans.<sup>14</sup>

**ECONOMIC.** Following the July 2014 EU sanctions against Russia, Russian narratives re-focus on Finland's bilateral economic reliance on Russia.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Constructive dialogue with Russian Federation.
- The option of NATO membership is continuously evaluated based on national security and defence policy interests. Any defence development should not create any practical impediment to a future military alignment.
- Intensification of Nordic defence cooperation, especially with Sweden.
- Maintaining the functioning of Finnish society based on transparency, extensive liberties and rights, whilst ensuring sufficient government control and emergency management capacity.

## VULNERABILITIES

- With specific reference to incident management, scarcity of the resources of the Defence Forces of Finland slows tracking and response time to violations, in some cases making the Finnish Air Force unable to respond if a violation occurs.<sup>15</sup>
- Lack of bilateral agreements on air safety.
- Lack of public information on 'due regard' – the behaviour required of pilots while near civilian aircraft.

## THREATS

- Airspace violations pose a direct threat to civilians in cases where they do not issue a flight plan or maintain contact with civilian air traffic control, which has caused several near-collisions. These incidents carry a risk of escalation, the consequences of which could be a serious deterioration of relations and escalation of measures on both sides.
- Demonstration of Russian capability to use force has propaganda-related aim of intimidation and coercion. Political messaging: further integration/NATO membership of target can/will cause further actions by Russia.

## EFFECTS

- Increased Finnish attention to the possible effects of NATO membership for Finnish and regional security, including a 2016 assessment report of the Finnish Ministry for Foreign Affairs.<sup>16</sup>
- Increased support for Finnish Defence Forces (although difficult to isolate from other factors such as Crimea).
- Increased military spending/availability of forces to the NATO Baltic Air Policing mission, consequently increased ability of the Alliance to maintain a high tempo of operations in reaction to Russia's actions.<sup>17</sup>

# SOUTH STREAM PIPELINE

## SUMMARY

South Stream was an offshore gas pipeline project designed to deliver natural gas from the Russian Federation through the Black Sea to Bulgaria, Serbia, Hungary, Slovenia, Austria, Italy, Croatia, Macedonia, Greece, and Turkey. It was a controversial project, posing a direct threat to the viability of the EU-backed Nabucco pipeline, planned to connect the EU to gas reserves in the Caspian Sea. In November 2007, Gazprom signed an agreement with the Italian energy company Eni to establish a joint project company. Bulgaria signed a preliminary agreement with Russia in January 2008, with energy companies from other nations involved following soon after.

Gazprom already supplied a third of EU gas, and the Nabucco pipeline was intended to decrease this dependency. In 2009, Ukraine, Hungary, Romania, Poland and Bulgaria also reported gas shortages, prompting concerns around Russian economic leverage and energy blockades on Eastern and Central European nations.<sup>1</sup>

Apart from the controversial methods used to advance the project, its overall ownership structure directly violated the EU's Third Energy Package passed in 2009.<sup>2</sup> Instead of amending the project to comply with EU law, Gazprom and the Russian government lobbied

participating EU member states to ignore EU legislation and exclude South Stream from applicable EU regulations, suggesting that the project was never intended to be constructed or operated according to EU rules.

A new Bulgarian government with historic and financial ties with the Kremlin took office in April 2012 and accelerated work on the South Stream project despite the obvious contradiction with EU regulation and opposition from Brussels. In April 2014, the Bulgarian legislature amended the country's energy law in a way which challenged EU regulations and gave legal authority to the South Stream ownership structure, creating friction between the EU Commission and the Bulgarian government. As Gazprom was already exporting to Bulgaria via Ukraine, the situation raised questions as to whether Gazprom was more interested in creating internal differences in the EU than opening new markets. Following pressure from opposition parties and the EU Commission, Bulgaria's government finally backed down, and in December 2014, President Putin announced the cancellation of the project.

## KEY POINTS

- South Stream was not financially viable, which indicates its motivations were more geopolitical: to provide political and economic leverage over CEE states; consolidate European dependence on Russian energy exports; exert control over Ukraine without threatening other customers and to undermine the Nabucco pipeline as an alternative supply option.<sup>3</sup>

- 'Pipeline diplomacy' is a powerful Russian foreign policy tool to leverage strategic influence and weaken the EU through non-military means. South Stream demonstrated Russia's intent to use economic leverage to undermine the enforcement of the EU's legislation and energy policies. Despite the explicit energy policy and legislation

prohibiting a project such as South Stream, several EU countries still supported it for domestic reasons in defiance of EU law.

- There is a significant risk of 'state capture' in large energy infrastructure projects. State capture is a type of political corruption where external actors influence a state's decision-making to their own advantage and the detriment of the national interest.<sup>4</sup> This highlights the importance of understanding the impact of business interests on state functions at local, regional and national levels, particularly through corporate lobbying. Transparency and accountability are crucial in ensuring that such large projects are subject to enough public scrutiny.

## CONTEXT

- **Russian influence in Bulgaria.** Several political parties in Bulgaria have long fostered financial, political, geopolitical and strategic relations with Russian politicians. Russia-linked corruption is still prevalent in Bulgaria, as with many former Soviet-aligned states. Gazprom is the sole provider of natural gas for Bulgaria while the Russian companies *Rosatom* and *Lukoil* dominate the nuclear energy sector and oil industry, respectively.<sup>5</sup> The annexation of Crimea in 2014 put Russia under closer observation especially after rumours that Gazprom sent a draft to the Bulgarian Ministry of Energy of the legal amendments proposed in Parliament two weeks later.

- **European energy security.** In 2014, 38 European countries carried out energy security stress tests to simulate disruption in Russian gas imports. The results concluded there was a possibility of a substantial impact, mostly in eastern member states and the Energy Community countries of Albania, Bosnia and Herzegovina, Georgia, the former Yugoslav Republic of Macedonia, Kosovo, Moldova, Montenegro, Serbia and Ukraine.<sup>6,7</sup>

## KEY ACTORS

**Gazprom** *Russia's largest natural gas company*

**Ministry of Energy of the Russian Federation**

**Bulgargaz** *Bulgaria's largest natural gas distribution company. The majority of the gas is purchased and imported from Russia through Gazprom contracts.<sup>8</sup>*

**European Commission**

**Eni** *Italian multinational oil and gas company*

**Alexander Novak** *Minister of Energy of Russia (2012 – present)*

**Sergei Shmatko** *Minister of Energy of Russia (2008 – 2012)*

**Alexei Miller** *CEO of Gazprom*

**Boyko Borisov** *Prime Minister of Bulgaria (2009 – 2013; 2014 – 2017;*

*2017 – present). Founder of political party GERB*

**Plamen Oresharski** *Prime Minister of Bulgaria (2013 – 2014). Member of the Bulgarian Socialist Party*



# NARRATIVES

## Russian government

- South Stream is a significant contribution to providing Europe with energy security and will allow Gazprom to create alternative and secure natural gas supply routes to consumers.<sup>9</sup>
- With the abandonment of this project, the EU will not benefit from Russian gas.
- Bulgaria is 'deprived of the possibility of behaving like a sovereign state'.<sup>10</sup>

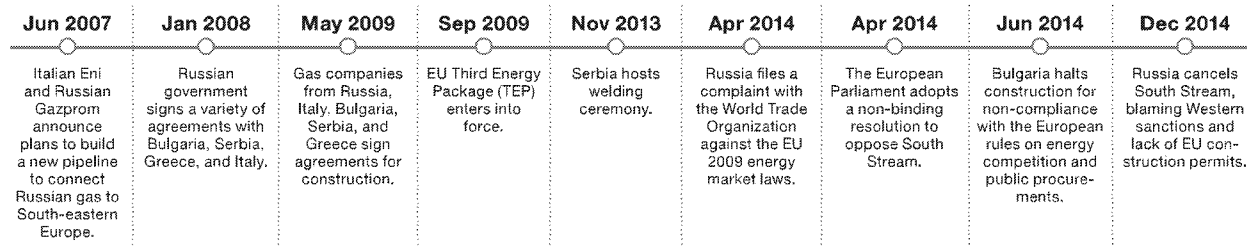
## Bulgarian government

- South Stream will provide a direct connection to gas sources and is beneficial to Bulgaria. Bulgaria will be a 'regional hub'.
- It will eliminate transit risks, and secure uninterrupted Russian gas supplies to millions of European consumers.
- South Stream will improve the European energy map and be an integral part of the EU's energy security system.

## European Commission

- South Stream is part of Russia's long-term strategy to leverage influence in the EU and is in conflict with EU law; therefore it should be opposed.<sup>11</sup>
- We will not accept any blackmailing on energy matters. Bulgaria is not a small country, it has the whole of Europe behind it.<sup>12</sup>

# KEY EVENTS



# STRATEGIC LOGIC

South Stream would provide the Russian Federation with political and economic leverage in South-eastern and Central Europe, increase European dependence on Russian energy exports, diversify transit capacity by bypassing Ukraine and undermine the Nabucco gas pipeline project. It is likely that the Russian side planned to force a compromise with the EU

using the demand for gas as a bargaining chip and to present the project as a fait accompli because construction had started. This approach ultimately failed following a collapse in negotiations between the EU and the Russian government because of Russia's aggression in Ukraine.<sup>13</sup>

# MEASURES

**DIPLOMATIC.** Statements of exaggerated profits and unsubstantiated costs propagated by Russian and Bulgarian officials, even from the Presidents of the two countries.<sup>14</sup>

**INFORMATION.** The repetition of unsubstantiated figures to cause confusion, outward fabrication of facts such as the stage of contract signing and secret meetings between the Bulgarian government and Gazprom officials.<sup>15,16</sup> The constant repetition of the ideograph 'regional hub' by various actors in and about Bulgaria was used to gather more public support with the promise of political and economic advantages.

**ECONOMIC.** As the leading gas supplier and recipient of a third of Bulgarian exports, Russia had the upper hand in negotiations over the project.<sup>17</sup> Russia controls a third of Bulgarian economic output.<sup>18</sup> Russia supplies a quarter of the EU's gas needs, but 80 per cent of that of Hungary.<sup>19</sup>

**FINANCIAL.** Promises to include companies close to the government, and alleged bribery of energy experts on rotation.<sup>20</sup>

**LEGAL.** Indirect access to both the executive and legislative branches of Bulgaria through corruption schemes propelled by kleptocratic and nepotistic characteristics of the government.<sup>21</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- The Black Sea region's importance in economy, trade and security. Given Bulgaria's active role in maintaining peace in the region and its commitments as a guard of the external borders of NATO and the EU, the stability of the Black Sea region plays a vital role in Bulgarian national security.
- Government control of key aspects of the economy.
- Secure and reliable delivery of energy.

## VULNERABILITIES

- Substantial dependency on Russian energy imports leaves EU countries vulnerable to economic leverage. Lack of energy import diversification can create a dangerous dependency.
- Media monopolies run by MPs from the Bulgarian Socialist Party and the Movement for Rights and Freedoms; conflict of interest as media moguls are both connected to Members of Parliament and own construction firms involved in the project.
- Corruption, high-level corruption in particular.

## THREATS

- Russian influence over political decisions by controlling future energy supplies, through Russian-owned energy infrastructure in the EU.
- Russian economic leverage by holding the majority of energy exports to certain EU member-states.
- Corruption threatens the existence of and compliance with social, legal and moral rules, reinforces organised crime, undermines the credibility of authorities, weakens their functioning and discredits reform.

## EFFECTS

- EU countries acted in conflict with EU legislation, creating divisions between member states.
- Undermining of Bulgarian obligations towards the EU.
- Making Bulgarian government more amicable to concessions: the new centre-right government in 2010 was sending signals of halting three major Russian-sponsored energy projects (Belene Nuclear Power Plant, South Stream, Bourgas-Aledanroupolis oil pipeline) but after that slowly commenced administrative work on the projects.<sup>22</sup>

# RUSSIAN LANGUAGE REFERENDUM IN LATVIA

## SUMMARY

In February 2012, a referendum was held in Latvia to determine whether or not to amend the constitution and denote Russian as a second state language. Although the majority of participants voted against this proposed change, the episode exposed and temporarily aggravated fractures in Latvian society, where language is a sensitive topic – Russian was obligatory during the years the nation was occupied and part of the USSR. In 2011, 37.2 per cent of the population had Russian as their first language.<sup>1</sup>

In January 2010 and eight months before parliamentary elections, the right-wing party 'National Alliance' proposed a referendum to amend the constitution and mandate the exclusive use of Latvian in publicly funded schools. However, they only gathered 120,433 of the 153,232 signatures required to force a referendum. In response to the National Alliance initiative, the youth movement 'United Latvia' started a campaign for a referendum to amend the constitution and make Russian a second state language. Together with the newly created organisation 'Native Tongue' they collected 187,378 signatures for their petition.

Nils Ušakovs, the Mayor of Riga and leader of the political alliance 'Harmony Centre', was likely a key figure in swaying more moderate Russian speakers to participate, particularly in the collection of signatures for the petition. Harmony Centre had the largest vote share in elections but was absent from government, having failed to establish a ruling

coalition with another party. Ušakovs initially denounced the referendum as unnecessary but then signed the petition after National Alliance cabinet members voted against funding the referendum.<sup>2</sup> He took the position that it was not simply a language issue, but about a "lack of respect towards a considerable segment of the population."<sup>3</sup> When the country went to the polls, around three-quarters of voters said they were against the amendment, with only the eastern region of Latgale, with its high concentration of Russian-speakers, having majority support for the change.<sup>4</sup>

Evidence which supports any assessment that the Russian Federation was attempting to influence the outcome of the vote relates to key actors in the 'Yes' campaign, statements by Russian officials and support from Kremlin-backed media. The Latvian Security Police assessed that some funding did come from Russia, but could not provide details for security reasons. The initiators of the referendum, Vladimir Lindermans and Jevgēnijs Osipovs, have well-documented links to the Russian Federation, although they deny receiving any direct support.<sup>5,6</sup> The Security Police highlighted Aleksandr Gaponenko, who admitted receiving funding from Russia through various NGOs, as a key figure behind Native Tongue.<sup>7</sup> Moreover, two TV channels were found in breach of their licence for commercials which supported the 'Yes' vote, and it was suspected that the funds came from Russia.<sup>8</sup>

## KEY POINTS

- The National Alliance was criticised for the politicisation of language policy at a time when Latvia was successfully moving towards an integrated society and mutual understanding of issues relating to language and ethnicity had significantly improved.<sup>9</sup>
- Issues such as ethnicity, citizenship and political rights have the potential to create social divisions which can be exploited by hostile actors. This case highlights the importance of independent research to pinpoint areas of potential conflict between different identity groups and identify vulnerabilities.

- Societal resilience can be enhanced by reducing potential areas of conflict between identity groups and promoting a national identity based on shared values and a joint vision of the future rather than ethnicity or language. A strong civil society is crucial for creating the room in public discourse for the expression of divergent views. Such 'depoliticised spaces' can help build better social cohesion and political consensus by enabling more democratic policy-making.

## CONTEXT

- **Language and citizenship.** The language issue in Latvia is closely related to the sensitive issue of citizenship. Inhabitants who immigrated to Latvia during the Soviet occupation (mostly Russians, Belarusians and Ukrainians) did not automatically receive Latvian citizenship after independence in 1991. They have the status of 'non-citizens', and can apply for citizenship through a naturalisation process but otherwise do not have the right to vote.<sup>10</sup> In 2012, there were a total of 304,806 non-citizens (by 2018 this figure had declined to around 228,000).<sup>11</sup> Despite initial criticism in the 1990s, Latvia's integration policies were widely seen as working before the referendum.<sup>12,13</sup>

- **Russia's compatriot policy.** Compatriot policy loosely defines the Russian diaspora by a mix of ethnicity and self-identification. A key aspect of this policy is the preservation of the Russian language through the funding of local NGOs. However, these aim "not to build cultural ties and public diplomacy in its best sense, but rather to serve as a conduit for Russian foreign policy through the local Russian community as well as being instruments of political influence."<sup>14</sup> Russian Minister of Foreign Affairs, Sergei Lavrov, said that "diasporas are our powerful resource, and should be used at full capacity."<sup>15</sup> The policy came under increased scrutiny in the 'near abroad' – nations that were once part of the Soviet Union – after Putin used the protection of Russian-aligned ethnic groups in Ukraine as justification for the annexation of Crimea in 2014.

## KEY ACTORS

**United Latvia** youth movement, started campaign for language referendum  
**Native Tongue** NGO established explicitly for the referendum  
**Harmony Centre** social-democratic political alliance, including the largely pro-Russian "Harmony" party which won the most seats in the 2011 parliamentary elections but was excluded from the governing coalition  
**National Alliance "All for Latvia"** right-wing Latvian political party which proposed initial referendum to exclude Russian from schools

### 'Yes' vote supporters:

**Vladimirs Lindermans** former leader of the Latvian branch of the National Bolshevik Party and a leader of 'Native Tongue'  
**Eduards Svatkovs** leader of 'United Latvia'  
**Jevgēnijs Osipovs** leader of the radical-left 'Osipovs' party  
**Nils Ušakovs** Mayor of Riga (since 2009), leader of "Harmony Centre"  
**Aleksandrs Gaponenko** a non-citizen and Director of the Institute of European Studies in Riga<sup>16</sup>

### 'No' vote supporters (all elected parties supported the 'Against' vote apart from Harmony Centre):

**Andris Bērziņš** President of Latvia (2011 – 2015)  
**Valdis Dombrovskis** Prime Minister of Latvia (2009 – 2014)  
**Raivis Dzintars** leader of National Alliance "All for Latvia!"

# NARRATIVES

## Yes-vote supporters

- Russian residents in Latvia have been treated as second-class citizens, and their human rights have been violated over the years.<sup>17,18</sup>
- The Russian language referendum is a response to the attempt by Latvian nationalists to exclude Russian from state-schools; this would be detrimental for academic results.<sup>19</sup>
- Latvia is pursuing a policy of narrow-minded nationalism which does not allow for other ethnicities.
- If Harmony Centre had been invited into government, the Russian-speaking minority would be better represented and there would be less support for the referendum.<sup>20</sup>

## No-vote supporters

- This referendum is an attempt to weaken Latvia's sovereignty, independence and identity.<sup>21,22</sup>
- The country has much greater priorities than language, such as economic recession.<sup>23</sup>
- A referendum will not solve the country's problems, which go much deeper than language, but will cause further divisions.<sup>24</sup>
- Accusations of the referendum being financed by Russia (e.g. by MP Raivis Dzintars from the National Alliance).<sup>25</sup>

# KEY EVENTS



# STRATEGIC LOGIC

The Russian Federation considers the neighbouring Baltic nations to be part of its traditional sphere of interests. Russian involvement in the Latvian referendum should be seen in the context of its 'compatriot policy', which includes support to Russian language speakers abroad.<sup>28</sup> This policy attempts to establish a master narrative of a unified identity group – regardless of any

underlying complexity – and mobilise them in support of foreign policy goals, while undermining the ruling authority of the target nation. In this case, established networks were used in an attempt to destabilise Latvia from within, using a range of measures to exploit a fault line in society which had been exposed by the unnecessary domestic politicisation of a social issue.

# MEASURES

**DIPLOMATIC.** Russian political representatives (President, Foreign Minister, MPs) pressured the Latvian government to change its citizenship policy. The Russian Ambassador to Latvia blamed the Latvian government's policies for causing the referendum, accusing it of not addressing interethnic issues.<sup>29</sup> Russian Foreign Minister Sergei Lavrov portrayed the referendum as a legitimate desire for justice, commenting that "people want to be heard. They want to achieve that their rights to speak, think and raise children in a native language are respected."<sup>30</sup>

**INFORMATION.** The Baltic branches of Russian TV channels under direct or indirect control of the Russian government (e.g. the popular First

Baltic Channel) supported the referendum.<sup>31</sup> *NTV* and *REN TV Baltic*, both registered in the UK and subject to Ofcom codes of practice, were found in breach for misleading advertisements urging people to sign the petition.<sup>32</sup> Flyers appeared in Daugavpils with the slogan "Let's not be servants to nationalists."<sup>33</sup>

**FINANCIAL.** In May 2012, Latvia's Interior Minister Rihards Kozlovskis said that some of the funding for the referendum had come from Russia, but did not provide any more details, citing protection laws and the fact that this information was classified.<sup>34</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Safeguarding national sovereignty, territorial integrity, and democratic constitutional order.
- Provision of fundamental values established in the Constitution of the Republic of Latvia.
- Maintaining a strong civil society that has a unified understanding about its value orientation.
- Maintaining the identity of the Republic of Latvia in regard to the Western world that wants to see Latvia as an independent, democratic, and legitimate country.<sup>35</sup>

## VULNERABILITIES

- Diverse ethnic composition of society with a relatively large Russian-speaking minority. Existing tensions between different identity groups, such as complaints by ethnic Russians of being discriminated against, can be exploited by outside actors.
- Issue of non-citizens who cannot participate in elections, cannot hold governmental employment but have to pay taxes.
- Inclination of Russian-speaking groups to be mobilised along the lines of ethnicity and language.

## THREATS

- Targeted division which increases tension between different groups in society. In defending the Latvian language, the Latvian government risked being seen as marginalising the Russian minority, thus further entrenching their opposition to the government.
- Efforts to create distrust between society and government by portraying the government as violating human rights of non-citizens.

- Attempts to internationally discredit the Republic of Latvia and aggravate the domestic policy in the Republic of Latvia.
- Russia's compatriot policy could be perceived as disruptive since it encourages compatriots to advocate for change of domestic policy in other countries. It thus directly undermines the ethnic integration policy of Latvia which is largely based on language.<sup>36</sup>

## EFFECTS

- The referendum re-emphasised the issue of citizenship and limitation of non-citizens' rights, and enabled criticism of the Latvian government by Russia's official leadership.
- The Latvian Ministry of Foreign Affairs acknowledged that the referendum revealed sensitive issues about Latvian society. The government further recognised the need for more integration and naturalisation measures in Latvia, with an emphasis on non-citizens given assistance to learn Latvian.<sup>37</sup>
- Exacerbation, even if just temporary, of the ethnic/language clash within the society. 'Yes'-campaigners vowed that the referendum was not the end and that Russian-speaking citizens would continue to fight for equal rights.<sup>38</sup>
- Entrenching of radical views on both sides of the debate.

# INSTITUTE OF DEMOCRACY AND COOPERATION

## SUMMARY

The Institute of Democracy and Cooperation (IDC) was founded in 2008 and describes itself as a 'think tank' which focuses on "the role of history in contemporary politics, the relationship between sovereignty of states and human rights, east-west relations, and the role of NGOs and civil society in democracies."<sup>1</sup> While the IDC has no formal connection to the Russian government, its board members and directors are close allies of the Kremlin and the positions they take closely align with the Kremlin's agenda, overtly supporting and justifying Russian Federation policy and ideology.<sup>2</sup>

The Paris branch is led by former Russian Duma member Natalya Narochnitskaya and British historian John Laughland, while the New York branch (closed in 2015) was led by Andranik Migranyan, former advisor to Boris Yeltsin. The IDC's perspective is based on Europe-Russia cultural ties, Russian nationalism, and Russian exceptionalism built on Orthodox Christianity and it presents research through this perspective across a range of issues including the Syrian War, EU politics, human rights, historical revisionism, and religion. Its efforts appear to be primarily focused on conferences, university talks and UN side-events, as well as media appearances on a range of pro-Kremlin outlets.

## KEY POINTS

- Certain Russian and Russia-funded GONGOs, NGOs and think tanks exist to promote the political agenda of the Kremlin in order to achieve Russian foreign policy goals. It is likely that the IDC is one such example, although there is insufficient publicly available evidence to conclude definitively that this is the case.<sup>3,4</sup>
- The IDC promotes themes ranging from problems with the liberal world order, double standards in international community behaviour towards territorial sovereignty, the American subjugation of Christian values, the need for a multi-polar world and Russia as an important actor in the international order.
- Organisations such as the IDC seek to legitimise their agenda by portraying themselves to be intellectually robust, honest and equivalent to other reputable NGOs and think tanks. Such organisations are made distinct by their opaque financing, informal links to hostile state actors and a lack of empirically-driven research. Like other entities aligned with the Kremlin they generally seek to point out the weaknesses of other states rather than promote Russia's own strengths.<sup>5</sup>
- Addressing the potential threat from such organisations requires an approach which respects freedom of expression and association. Governments should: collaborate with other nations to investigate networks, raise awareness of organisations which have unclear links to adversaries to prevent tacit endorsement and increase the level of accountability and financial transparency.

## CONTEXT

■ **Russian 'soft power' tools.** The IDC was founded during a period when Russia was evolving its approach to 'soft power' in the early to mid-2000s. During this period, the Russian government invested significant resources in such tools as *Russia Today* (later *RT*) and the *Russkiy Mir Foundation*. Some of these institutions were inspired by Western models, while others were Russian innovations.<sup>6,7</sup> Russian soft power today is characterised by a tendency to exploit vulnerabilities in other societies rather than promote the strengths of its own society.<sup>8</sup> Russian soft power should be understood as different to Western conceptions of soft power. While Western soft power is usually defined as a mixture of a government's actions and the result of civil society activity which is independent of their government, the Russian version is based more heavily on governmental and quasi-governmental institutions that promote a government-directed image of Russia.<sup>9</sup> Putin defined it as "a matrix of tools and methods to reach foreign policy goals without the use of arms but by exerting information and other levers of influence."<sup>10,11</sup>



IMAGE – The IDC's John Laughland commenting on NATO's mission on RT in 2014.

## KEY ACTORS

**Natalya Narochnitskaya** *Head of the Paris branch. Has connections with the Kremlin as a former member of the State Duma and vice-chairman of the Duma's Foreign Affairs Committee.<sup>12</sup> Holds high-level or advisory positions in the Russkiy Mir Foundation, the Historical Perspective Foundation, and the Foundation for Supporting and Protecting the Rights of Compatriots Living Abroad.<sup>13</sup>*

**John Laughland** *Director of studies, A British citizen who holds a doctorate in philosophy from the University of Oxford. Known primarily for his Eurosceptic views.*

**Anatoly Kucherena** *Founder of IDC. A Russian academic and lawyer known for representing exiled former Ukrainian leader Viktor Yanukovich and NSA whistleblower Edward Snowden. He serves on the Public Chamber – a civil society advisory board for the Kremlin – and sits on the board which oversees the Federal Security Service (FSB).<sup>14</sup>*

**Andranik Migranyan** *Director of IDC's New York branch from 2008-2015. Held posts on the Council on Foreign and Defense Policy of the Russian Federation, the Public Chamber of the Russian Federation, the Presidential Council of the Russian Federation and the Valdai Discussion Club.<sup>15</sup>*

## NARRATIVES

### IDC

- The liberal world order is flawed.
- Russia is a major actor in the international order.
- There is a need for a new multi-polar world order which mitigates the ability of NATO and the US to do harm.

- The international community shows double standards and hypocrisy in world politics (especially in regards to inconsistent recognition of secessionist movements).
- American Christianity is being subjugated by liberal values.

# KEY EVENTS

2007 – 2008	May 2008	4 Jul 2013	23 Nov 2013	Dec 2013	25 Nov 2014	28 Jun 2015	2015
The IDC forms; offices in New York and Paris open.	The IDC releases its first publication "Orange Webs" which argues that the Orange Revolution (2004-2005) was a Western plot. <sup>16</sup> Excerpts from the publication are hosted on RT before its official release.	The IDC organises a Paris symposium on the defence of family values, which is attended by the French Christian Democratic party leader Christine Boutin.	The IDC holds conference on 'the family' in Leipzig. Speeches by Olga Batalina and Elena Mizulina, Chairman and Vice-Chairman of the Family Affairs Committee of the Russian Duma.	Laughland denounces pro-Europe protests in Kiev and the ultranationalist Svoboda party, accuses Western media of propaganda.	Laughland speaks at a conference organised by the State Duma in Moscow on "Overcoming the crisis of confidence in Europe." <sup>17</sup>	The IDC New York office closes. Mi-granyan explains that the IDC's "mission is over," because "the situation with human rights in the US has improved." <sup>18,19</sup>	The IDC is granted special consultative status by the United Nations Economic and Social Council (ECOSOC).

## STRATEGIC LOGIC

There is no conclusive evidence available in the public domain to support the assessment that the IDC has direct financial links with the Kremlin, or that the Kremlin directs or enables its activities. However, it promotes narratives that are very closely aligned with those of the Kremlin; John Laughland is a regular contributor to Russian state television and the leadership's multiple roles with other Russian entities discredit the IDC as an independent institution. It could therefore be considered a component of the

Kremlin's soft power measures in support of foreign policy objectives.<sup>20,21,22</sup> Consistent with other Russian soft power measures, the IDC seeks to point out the flaws of other societies over and above the promotion of the strengths of Russia.<sup>23</sup> It is assessed that the primary target audience of the IDC lies in political circles and policy-makers.

## MEASURES

**DIPLOMATIC.** The IDC has sought to achieve legitimacy and influence through diplomatic entities and events.<sup>24</sup>

**INFORMATION.** The IDC deals with international topics such as Syria and Ukraine that are of interest to the Kremlin, primarily reflecting a pro-Kremlin perspective of history. Narochnitskaya and Laughland leverage the perceived legitimacy of a European think tank to bolster their status as authorities on relevant issues.

Events in which guest speakers from sympathetic organisations attend add an external, but echoing, voice. These events seem to receive minimal media coverage in France but are occasionally covered by pro-Kremlin-media sources.

The IDC has also occasionally appeared in a range of English and French language media outlets which had varying reach. The most significant of these media outputs are Laughland's regular articles for *RT France* which tend to focus on divisions, problems and hypocrisies in EU politics and the US as well as topics of interest to the Kremlin such as Ukraine, Catalanian secessionist movements and Syria.<sup>25</sup>

**FINANCIAL.** The IDC is funded by unidentified 'private donors'. Laughland claims funding comes from the Foundation for Historical Outlook in Moscow, which is financed by unspecified private Russian companies.<sup>26</sup>

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

France's national security functions relevant to institutions like the IDC include:

- National cohesion.<sup>27</sup>
- Informed public debate.
- Trust in government institutions.
- A healthy civil society in which a diverse range of voices (citizens, organisations and businesses) can participate in the contestation and construction of progress in society.<sup>28</sup>

### VULNERABILITIES

- Anti-American sentiments in France. The "US versus Russia" dichotomy presents an avenue through which pro-Russian propaganda may resonate disguised as anti-Americanism.
- Conservative-secular cleavages in French society. The IDC focuses on controversial issues such as the legalisation of same-sex marriage, presenting arguments which align with more conservative viewpoints in society.<sup>29</sup>

### THREATS

- Creation of ambiguity by adversaries in an unstable and uncertain strategic environment, which in turn threatens to increase existing tensions in society.<sup>30</sup>
- Strengthening the interest of far-right movements and polarisation in France through disruptive discourse.
- Undermining of public discourse, if arguments based on heavy bias and selective use of facts are perceived as scientific facts.<sup>31</sup>

### EFFECTS

- The IDC is assessed to have limited resonance at the mass public level, due to its narrow communication output, minimal resources and limited reach. It has low levels of engagement on social media channels and relatively low presence in mainstream media.<sup>32</sup>
- The IDC is perhaps marginally more effective at the political decision-making level through its events which feature high-level Russian figures, as well as through its engagement with figures from fringe or nationalist parties.
- The effect of IDC appearances at decision-maker level discussions and events may sensitise these audiences to Kremlin-aligned perspectives.
- Surveys of French public opinion suggest anti-Russian sentiment is still high (70 per cent of respondents displaying anti-Russian opinions and 85 per cent distrusting Putin).<sup>33</sup>

# ZAMBIAN ELECTIONS 2006

## SUMMARY

Zambia is one of the most important destinations for Chinese investments in Africa.<sup>1</sup> The southern African state is one of the world's largest copper producers, and China, the world's largest copper consumer, has been eager to secure continued access to raw materials.<sup>2</sup> Chinese investment in the Zambian mining and construction sectors, by both state-owned and private companies, has been actively encouraged by the Chinese government, which also provides development aid relating to agriculture, telecommunications and infrastructure. This investment has been accompanied by an influx of Chinese workers, as many companies prefer to import skilled labour rather than train and contract locally.<sup>3</sup>

Although the Zambian government generally welcomed Chinese investment, anti-Chinese sentiment amongst the Zambian population had steadily increased and became a pivotal issue in the 2006 presidential election.<sup>4</sup> Many Zambians were angry about the displacement of small local business by the Chinese, poor working conditions and delayed payment of wages, and the use of Chinese workers instead of hiring local people. The death of 52 workers during an explosion at a Chinese-owned mine in 2005, Zambia's worst industrial accident in 30 years, led to public outrage over the circumvention of safety standards and labour laws by many Chinese-owned companies.

Opposition presidential candidate Michael Sata tapped into fears over Chinese influence, campaigning with a manifesto which was overtly anti-Chinese. Sata criticised China's 'exploitation' of Africa, calling Chinese companies 'infestors', and pledging to expel Chinese businesses from Zambia. He also courted Taiwanese businesses and described Taiwan as a 'sovereign state', at which point China intervened. Their ambassador in Lusaka convened a press conference, accusing Sata's party of signing an agreement with the Taiwan authorities and stating that if Sata was elected president and recognised Taiwan, China would cut diplomatic ties, and investments would be stalled until bilateral relations returned to normal. The announcement was widely reported as an open threat.

Sata lost the election, but gained 29 per cent of the vote, with his party taking every seat in the capital Lusaka and the Copperbelt region, where Chinese presence was particularly high. After the results were announced, riots broke out in Sata's strongholds, predominantly targeting Chinese-owned shops.<sup>5</sup> Responding to the backlash, China focused on softening its image by providing more incentives, such as building hospitals and sports venues.<sup>6</sup> The financial crisis of 2008 and subsequent global recession also led to Zambians taking a more favourable view of China, as Chinese companies were able to mitigate the worst impact of the economic downturn in Zambia.<sup>7</sup>

## KEY POINTS

- Chinese investment was welcomed by the Zambian government but seen as threatening by a significant part of the population. The two opposing views of Chinese presence – as being either beneficial or harmful – underline the political nature of any assessment of hostility. Framing economic dependency as malign is particularly resonant when successfully linked to concerns held by the local population regarding foreign influence. The 2006 Zambian elections essentially became a referendum on Chinese influence.<sup>8</sup>

- Economic leverage can translate into domestic political influence. The Chinese ambassador announced that China would cut relations with Zambia and development aid and investment would be put on hold if Michael Sata was elected president and took steps to recognise

Taiwan. It is not clear if the Chinese intervention had a decisive effect on the election outcome, and it may even have been counterproductive, by reinforcing public opinion that Chinese investment was linked to illegitimate influence in the Zambian government<sup>9</sup> and reigniting colonial-era memories of the struggle for independence.<sup>10</sup>

- The absence of credible data on issues such as migration can lead to threat inflation, as the vacuum created by a lack of factual information allows alarmist speculation to fill the gaps. Authoritative figures on Chinese presence in Zambia were incomplete, contradictory or inaccessible, which enabled Michael Sata to cite scare numbers of 80,000 Chinese people living in the country – more realistic estimates range from 13,000 to 22,000 people.<sup>11</sup>

## CONTEXT

- **Chinese engagement in Africa.** China has been investing in the African continent for decades, undertaking large infrastructure projects including railways, ports, dams and bridges and telecommunications, as well as investing in areas such as mining, agriculture and manufacturing. There are currently over 10,000 state-owned and private Chinese firms operating in Africa.<sup>12</sup> Reports regularly surface of predatory loan practices and Chinese corporations circumventing labour laws or environmental standards. Some Western observers maintain that China's interest in the continent is part of a 'new scramble for Africa' and focused on exploiting its abundant natural resources. However, much of China's economic activities and 'soft power' efforts have underlying political objectives (e.g. building support for its 'One China' policy), and China consistently evokes the narrative of solidarity and 'win-win' situations.

- **Background on Zambia.** Zambia gained independence from Britain in 1964. Compared to other sub-Saharan African states, Zambia has since enjoyed relative political stability, despite enormous internal

ethnic and lingual heterogeneity.<sup>13</sup> The country also has relatively strong trade unions and civil society organisations. The country's population has grown from 12.4 million (2006) to 17.8 million (2018). Formerly a one-party state, Zambia's recent multiparty elections have been recognised as largely free and fair.<sup>14</sup>

- **History of Sino-Zambian relations.** Zambia established relations with China directly after independence. The relationship, described by former Zambian President Kenneth Kaunda as an 'all-weather friendship', was driven by ideological and geopolitical considerations from the 1960s-1980s: this included development aid and grand infrastructure projects, such as the TANZAM railway between Zambia and Tanzania, as well as support for Zambia's anti-apartheid campaign and collaboration during the Cold War period.<sup>15</sup> More recently, China has been focusing on trade, and on investments in the Zambian construction and mining sector.

## KEY ACTORS

**Chinese Embassy in Lusaka** most important contact for Chinese investors in Zambia, functions as extended arm of the Chinese political leadership and is directly involved in investment negotiations<sup>16</sup>

**Movement for Multi-Party Democracy (MMD)** centre-left party that was in power in Zambia from 1991-2011

**Patriotic Front (PF)** social democratic party, initially founded in 2001 as personal vehicle of Michael Sata

**Li Baodong** Chinese Ambassador to Zambia (2005 – 2007)

**Hu Jintao** President of China (2003 – 2013)

**Levy Mwanawasa** President of Zambia (2002 – 2008), MMD, died in office

**Michael Sata** Leader of Patriotic Front (PF), presidential candidate in 2006 and 2008, President of Zambia (2011-2014), died in office

# NARRATIVES

## Chinese government

- Growing bilateral trade is beneficial to both countries.
- Chinese aid and investment in areas such as mining, infrastructure or agriculture has improved life for Zambians; it contributes to the country's gross domestic product and creates job opportunities.<sup>17</sup>
- If Sata is elected president, recognises Taiwan and expels Chinese investors, then China might sever ties with Zambia.
- Chinese investors are 'scared' to come to Zambia because of Sata's 'unfortunate' remarks; further investments have been put on hold until the uncertainty surrounding bilateral relations is resolved.<sup>18</sup>

## Zambian government

- Sino-Zambian relations consist of mutually beneficial cooperation.<sup>19</sup>
- China has long been a reliable ally of Zambia, both in terms of development and international relations.<sup>20</sup>
- Zambia supports the 'One China' policy.<sup>21</sup>
- Written apology to Beijing by Zambian President Mwanawasa over Sata's comments.<sup>22</sup>

## Michael Sata

- Chinese economic engagement in Zambia amounts to exploitation and plundering of natural resources.<sup>23</sup>
- Campaign slogan 'Zambia for Zambians'; Zambia has "become a province of China."<sup>24</sup>
- Chinese companies are too often importing their own people for work that could be done by locals.
- Chinese managers are ill-treating Zambian workers, only employing them on short-term contracts with no benefits, and are not respecting safety regulations or environmental standards.<sup>25</sup>
- Accusations of large-scale repatriation of profits and tax exemptions.<sup>26</sup>

# KEY EVENTS

1960s – 80s	1990s – 2000s	Apr 2005	Jul 2006	Jan – Sep 2006	4 Sep 2006	28 Sep 2006	3 – 6 Feb 2007	20 Sep 2011
China provides development aid to Zambia, mainly driven by ideological and geopolitical considerations.	Privatisation of Zambian mining sector. Access to resources (esp. copper) becomes most important driver of Sino-Zambian relationship. <sup>27</sup>	52 workers killed in explosion at Chinese-owned mine, sparking anger at lack of safety standards.	6 workers are shot during riots over delayed wages at a Chinese-owned mine.	Populist election campaign of Michael Sata (PF) capitalises on growing anti-Chinese sentiment.	Chinese ambassador to Zambia Li Baodong tells press that China "shall have nothing to do with Zambia if Sata wins the elections and goes ahead to recognise Taiwan." <sup>28</sup>	Zambian Presidential Election: Sata performs strongly, but ultimately loses to incumbent president. Riots break out in Sata's strongholds, targeting Chinese-owned shops. <sup>20</sup>	Chinese President Hu Jintao pays unusually long visit to Zambia, announces first Special Economic Zone.	Sata wins presidency in his third attempt, although he has toned down anti-Chinese rhetoric.

# STRATEGIC LOGIC

Chinese engagement in Africa is motivated by a mix of profit and strategic interests. State-driven investment in Zambia's mining and construction sector is primarily aimed at gaining access to the country's natural resources. The aid and investment from China also has political aims, including building a long-term relationship and generating support for its 'One China' policy. The ambassador's statement that China would break off relations with Zambia if Michael Sata was elected was interpreted by the Zambian

opposition and many Western commentators as an overt and direct intervention in the election. China was accused of attempting to leverage Zambia's economic dependence on China to change voting behaviour. Nevertheless, the position articulated by the ambassador was also consistent with Beijing's 'One China' principle, which is a fundamental element of China's foreign policy and a key prerequisite for its relations with other countries.

# MEASURES

**DIPLOMATIC.** The Chinese state backs Chinese investments in Zambia at the highest political level. Negotiations on Chinese development assistance and investments take place through the FOCAC (Forum on China-Africa Cooperation), as well as during official state visits.<sup>30</sup> Not all Chinese investments in Zambia are aimed at making profit: for instance, Chinese investments in agriculture (e.g. irrigation systems) or support to Zambia's broadcasting services (e.g. providing FM transmitters) are of a charitable nature aimed at development and poverty reduction,<sup>31</sup> although they are likely also designed in pursuit of political objectives, such as gaining support for the 'One China' policy.<sup>32</sup> The elections of 2006 were the first time that China openly got involved in the political process of Zambia through public statements.

**ECONOMIC/FINANCIAL.** In 2006, China was the biggest investor in Zambia (USD 209 million),<sup>33</sup> and 200 Chinese companies were recorded in the country.<sup>34</sup> Chinese FDI is dominated by large state-led, policy-driven, publicly owned companies, although private companies are gaining more importance.<sup>35</sup> The majority of Chinese FDI to Zambia targets mining or mining-related activities, although FDI also flows into the construction, agricultural or manufacturing sector.<sup>36</sup> The state-owned Bank of China established a branch in Zambia for the political and non-commercial purpose of facilitating the day-to-day activities of Chinese companies in Zambia.<sup>37</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Free, fair and independent elections.
- Low unemployment, reduction of poverty.
- Enforcement of legal standards regarding safety and environment throughout the country.
- Encouragement of Foreign Direct Investment and development aid from allied countries.

## VULNERABILITIES

- Zambia's economy is highly dependent on the copper sector, and by extension on the fluctuation of international market prices.<sup>38</sup>
- Zambia is one of the poorest countries in the world; around two-thirds of the population live below the poverty line.<sup>39</sup>
- Corruption, especially among labour law enforcement officials that are willing to overlook lack of safety regulations.<sup>40</sup>
- Unemployment is close to 50 per cent in Zambia (2006).<sup>41</sup>
- Increasing economic dependence on Chinese investment, particularly in the mining sector.

## THREATS

- The increasing use of Chinese labour by Chinese companies in Zambia leads to increased informal employment or even unemployment among Zambians.<sup>42</sup>
- Foreign interference in elections to influence the voting behaviour of the population.
- Health and safety of Zambian workers is threatened through managers' non-observance of labour law.
- For the incumbent MMD government, popular discontent with Chinese economic engagement threatens the future flow of FDI and aid from China.

## EFFECTS

- Statements by the Chinese ambassador had no negative effect on official Sino-Zambian relations.<sup>43</sup>
- Perceived interference by ambassador reinforced the narrative of hostile Chinese influence.
- Anti-Chinese sentiment decreased during the global recession 2008–2011: despite falling copper prices, Chinese companies were able to maintain workplaces and mitigate the impact of the economic downturn, as the Chinese financial sector was relatively insulated from the crisis. In his future election campaigns, Michael Sata used 'anti-exploitation' rather than 'anti-Chinese' rhetoric.<sup>44</sup>

# SERBIAN ORTHODOX CHURCH

## SUMMARY

The Serbian Orthodox Church (*Srpska Pravoslavna Crkva* or SPC) is a self-governing church within the Eastern Orthodox Church, a family of 13 self-governing bodies defined by the nation in which they are located. Although the Serbian constitution guarantees the secular nature of the state, the SPC plays a highly important role in the construction of Serbian national identity and holds a privileged position in comparison to other religions in Serbia.<sup>1,2</sup> In 2011, 84.6 per cent of the Serbian population described themselves as orthodox.<sup>3</sup>

The SPC has strong connections to the Russian Orthodox Church (ROC, Moscow Patriarchate) and their cooperation has increased over the last ten years. The ROC is closely connected to Russian language, history and faith, Russian political life and the Russian Federation's intelligence apparatus. It uses an Eastern Orthodox Christian tradition to promote a pro-Russia stance as the only viable path for Eastern European states, speaks out against NATO and the EU and condemns the 'moral degradation' of the West.<sup>4</sup> The Kremlin likes to portray itself as a champion of traditional conservative and nationalist values rooted in Eastern Orthodox Christianity, in opposition to Western liberalism.<sup>5,6,7</sup>

Although the ROC and the SPC have close ties and share many interests, they should not be seen as a single entity with unified policies. The SPC is generally not as conservative as the ROC, although some of the more hard-line SPC clergy hold similar attitudes to the ROC's opposition to Western values. SPC opposition to the West is primarily linked to the Kosovo recognition issue: the SPC insists that Kosovo is part of Serbia, and must not be traded for EU membership (which is only possible for countries without open border disputes).

The Russian government has attempted to increase its influence in Serbia through and within the SPC through financial and diplomatic means. In 2016, Russian energy company Gazprom invested EUR 4 million in the creation of mosaics for Saint Sava in Belgrade, the largest Serbian Orthodox church.<sup>8</sup> Russian politicians and diplomats frequently present themselves as orthodox, refer to or use the language of the SPC in public statements, and publicly interact with the church to improve their public image and address the predominantly orthodox audience in Serbia. Similar strategies are used by extreme right groups in Serbia who are supported by hard-line SPC clergy, such as their protest against the LGBT movement in the country.

## KEY POINTS

- The SPC is an independent body and should not be seen as a 'Russian agent', but rather as a useful ally for the Kremlin to achieve foreign policy objectives, as well as a suitable channel to reach relevant Serbian audiences. The ROC and the SPC share many interests and goals. The SPC tries to influence political events in ways that are in line with the Russian agenda (especially relations with Serbia's neighbours, Serbia's bid for EU membership, and the Kosovo issue).

- The SPC actively pushes a pro-Russian outlook such as the promotion of both real and fictitious historical and religious links between

Serbs and Russians and organising protests against the independence of Kosovo or 'Western liberal values' such as LGBT events. By promoting anti-Western sentiment and perpetuating ethnic tensions, the SPC's actions broadly align with Russia's interests in the region.

- As orthodox churches often focus on one specific ethnic group and often have extensive influence at every level of society, they are a particularly effective means to exploit the (ethnic) divisions over nation states in the former Yugoslavia region.

## CONTEXT

- **Russia and the Western Balkans.** The Western Balkans is a territory of ongoing competition between Russia and other actors, such as the US and EU, and a key region regarding the control over energy supply routes to Europe.<sup>9</sup> Putin has stated that Russia will not accept Kosovo's independence and has been blocking its accession to the UN with its veto in the Security Council.<sup>10</sup>

- **Serbia's bid for EU membership.** Serbia is moving towards EU integration, including membership by 2025, but a lack of momentum has led to doubts over EU commitments to the region, which in turn has created vulnerabilities for Moscow to exploit. Between 2009 and 2015 polling indicated a decline in public support for Serbian EU membership, and

in 2015 the majority of people saw Serbia's interests best served by maintaining strong ties with Russia, with the idea of Russia being 'orthodox brothers' as the most commonly cited reason.<sup>11</sup>

- **The SPC and Kosovo.** The SPC perceives Kosovo as the cradle of its medieval civilisation; many of the SPC's most important churches and monasteries are located in Kosovo, and the Patriarchal Monastery of Peć in Kosovo is the historical seat of Serbian Patriarchs.<sup>12</sup> Since the Kosovo War, many SPC churches and monasteries have been damaged or destroyed by Kosovo Albanians, and several priests were killed. The Serbian government has accused Pristina of not looking after SPC sites properly, or even colluding in their destruction.<sup>13</sup>

## KEY ACTORS

**Serbian Orthodox Church (SPC)**  
**Russian Orthodox Church (ROC)**  
**Obraz** Serbian far-right orthodox ultranationalist group, banned since 2012

**Patriarch Irenej** head of Serbian Orthodox Church (since 2010)

**Patriarch Pavle** head of Serbian Orthodox Church (1990 – 2009)

**Patriarch Kirill** head of Russian Orthodox Church (since 2009)

**Patriarch Aleksy II** head of Russian Orthodox Church (1990 – 2008)

**Bishop Teodosije Šibalić** spiritual leader of Orthodox Serbs in Kosovo

**Sava Janjic** prominent SPC Abbot in Kosovo, opposes Brussels agreement

**Bishop Amfilohije Radović** head of the SPC in Montenegro; strong anti-NATO views, called for referendum on Montenegro's NATO membership

**Mladjan Djordjevic** key financier and supporter of opposition figure Dragan Dilas; close ties to Russia; protects 'oppressed' Serbs in MNE, Croatia, Bosnia and MKD via SPC

**Aleksandar Vučić** President of Serbia (since 2017), Prime Minister (2014 – 2017)

**Ivica Dačić** Prime Minister of Serbia (2012 – 2014; 2017)

**Ana Brnabić** Prime Minister of Serbia (since 2017), first woman and first openly gay person to hold that office



# NARRATIVES

## Serbian Orthodox Church

■ Hard-line SPC clergy openly supported Milosevic during the 1990s, publicly blessing Serb nationalist paramilitaries who committed war crimes in Croatia, Bosnia and Kosovo.<sup>14</sup> Moderate SPC clergy participated in pro-democratic protests, and asked Milosevic to step down after the Kosovo war.<sup>15,16</sup>

■ Opposition to LGBT events such as pride parades; promotion of traditional Christian values.

■ Opposition to independence of Kosovo; mixed positions on Serbian accession to the EU.<sup>17</sup> Use of religious nationalism to promote a pro-Russia path as the only viable alternative for Eastern European states.

## Russian government

■ Steps taken towards EU integration are a 'forced democratisation of the region' that is not supported by the people. The EU wants to pull Serbia away from the 'traditional Slavic-Orthodox brotherhood' or concept of 'pan-Orthodoxy' based on the historical ties between the people of Russia and the people of Serbia.<sup>18</sup>

■ Support for Serbia over the Kosovo recognition issue.

# KEY EVENTS

2001	2004	2008	2010	Jan 2013	Jul 2013	Nov 2014	Jan 2016
A group of people led by priests disperse the first attempted Pride Parade in Belgrade, beating up many participants. <sup>19</sup>	SPC holy sites in Kosovo are vandalised and destroyed on a mass scale during protests of Kosovar Albanians. <sup>20</sup>	Kosovo declares independence; not recognised by Serbia.	Clashes and vandalism surrounding the Pride Parade, involving far-right activists and some church representatives, resulting in 150 people wounded; <sup>21</sup> government prohibits Pride Parades for 3 years. <sup>22</sup>	Over 100 Serbian Orthodox grave-stones are destroyed in Kosovo; several churches are looted. <sup>23</sup>	Patriarch Irinej visits Patriarch Kirill in Moscow, calling on Russian support to preserve Kosovo and Metohija. <sup>24</sup>	ROC and SPC primates meet Serbian PM Vučić <sup>25</sup> and President Nikolić; <sup>26</sup> aiming to sustain ties with Russia despite EU membership bid; Patriarch Kirill accuses Europe of 'abandoning Christian values'. <sup>27</sup>	SPC pushes for referendum on NATO membership in Montenegro. <sup>28</sup>

# STRATEGIC LOGIC

The ROC and, by association, the SPC, are used to promote a spiritual dimension of Russian foreign policy by promoting a particular set of values. Russia's apparent aim is to use the SPC, along with a range of other 'soft power' measures to destabilise the region, delegitimise the EU and

integration process, reduce the likelihood of cooperation with NATO, and slow the progress of both transitional justice and the normalisation of relations with Serbia and Kosovo.<sup>29</sup>

# MEASURES

**DIPLOMATIC.** Russian politicians and diplomats put themselves forward as being Orthodox and speaking the language of the church to exploit its strong position and high levels of trust to advance their political interests and policy priorities.<sup>30</sup>

**INFORMATION.** Orthodox links between Russians and Serbians are a key source of public trust in Russia and its willingness to operate in the interest of Serbia.<sup>31</sup> High level of public trust in Russia and post-Soviet Union

of Orthodox Serbs and large number of followers make sure that messages from the Church or affiliated to it reach a broad, receptive audience.<sup>32</sup>

**FINANCIAL.** Funding from the Russian Orthodox Church and private sources to the Serbian Orthodox Church, for example contributing to (UN-ESCO-supported) church restoration projects (mainly in Serbia, Kosovo and Metohija in particular).<sup>33</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

■ Successful democratic transition of the countries in the region.

■ Favourable conditions for joining the EU, sustaining democratic processes and a foreign policy orientation towards Europe. The majority of Serbs wants to join the European Union, although many believe that Serbia will never become an EU member.<sup>34</sup>

## VULNERABILITIES

■ Economic and social problems, including the social status of displaced and internally displaced persons in former Yugoslavia. "Inadequate integration of certain minority communities and groups in the wider social environment" of Serbia.<sup>35</sup>

■ Unresolved political status of Kosovo, lack of progress in implementing the 2013 Brussels Agreement.

■ Lack of momentum in EU integration, partly justified by a lack of progress on critical issues such as corruption and political reform.

■ Weak state institutions.

## THREATS

■ "Distinct national, religious and political extremism and the destruction of cultural heritage [...]. Ethnically motivated acts of violence that contribute to the creation of insecurity and fear among members of the Serbian people and minority ethnic communities."<sup>36</sup>

■ Competing security threats between NATO/EU and Serbia regarding Kosovo and Metohija.

■ Risk of increased support among Serbian Orthodox audience for closer relations with Russia and away from EU accession, by directly discrediting the EU and promoting anti-Western and pro-Russian sentiments.

## EFFECTS

■ Disruption of the normalisation of relations with Kosovo by SPC interference (with the backing of ROC), which is necessary for EU accession.

■ Discrediting of pro-European politicians in the eyes of the Orthodox Serb audience (e.g. statements defying Ana Brnabić, the first openly gay minister serving in a Balkan country).<sup>37</sup>

■ Serbia's far right (connections with Orthodox Church, aligned themselves with SPC ideology and position) has employed the threat and use of violence to push the state to outlaw (certain) constitutional rights of the LGBT community (prohibition of Pride Parades after violence in Belgrade).<sup>38</sup>

# COMMUNIST PARTY OF BOHEMIA AND MORAVIA

## SUMMARY

The Communist Party of Bohemia and Moravia (KSČM) was once the unquestioned political pariah of Czech politics. However, this changed shortly after the October 2017 parliamentary elections. The KSČM's return from the political wilderness has taken place primarily through the strategic sponsorship of Czech President Miloš Zeman, who was narrowly elected to a second term in January 2018. The president's steadfast support for controversial Prime Minister Andrej Babiš also required resurrecting the communists in order for the PM's cabinet to secure a majority vote of confidence, which finally took place on 12 July 2018 after an eight-month period of political uncertainty. As a result, Moscow-friendly President Zeman is in a position to exert extraordinary influence over the current Czech government.

The KSČM's rise to a position of effective influence through its 'Patent of Toleration' with the dominant governing party ANO (Action of Dissatisfied Citizens) presents several potential security threats to the Czech Republic, NATO and the EU. The party, for example, opposes the Czech Republic's active commitment to NATO, and wants to lift all sanctions against Russia, a stance consistent with its backing of Kremlin policy in Eastern Ukraine and Crimea. In late May 2018, the KSČM,

in cooperation with strategic allies, defended Kremlin interests by colluding to block a parliamentary discussion of the use of the nerve agent novichok in the UK in March 2018, which Moscow has linked to the Czech Republic on numerous occasions. The KSČM, in concert with the radical right (e.g. SPD party), have also aided the ongoing Kremlin influence campaign in the Czech Republic through their promotion of illiberal rhetoric which undermines democratic institutions. This includes support for anti-integration, anti-immigrant, anti-Muslim, anti-NATO, and anti-Brussels policies, a trend which is likely to continue.

As their position on the novichok incident demonstrates, the KSČM are unlikely to support policies which would pro-actively defend the Czech Republic and NATO against threats from Russia. The party is instead likely to maintain a posture toward the Kremlin which leaves the Czech Republic increasingly vulnerable to hostile measures. The party's aging electorate and difficulty in recruiting new voters, however, augur a continuing electoral decline. This will likely terminate their influence after the current government leaves office and President Zeman's political sponsorship project ends.

## KEY POINTS

- No credible evidence of policy coordination with the Kremlin or funding from Russian sources exists. The KSČM instead consistently aligns itself with Kremlin policy positions in order to oppose its traditional nemesis NATO, and to support the Kremlin's vigorous reassertion of Russian power in the old Soviet mould, which brings Czech Communists back to their old geopolitical roots and alliance commitments. The party is more divided on opposition to the EU.

- The relationship of mutual convenience among the president, prime minister, and KSČM has created an informal Czech domestic political alliance which is unlikely to take a tough line against the Kremlin on diplomatic and security issues, as the decision to prevent a parliamentary investigation into the novichok incident clearly suggests. This extends

to possibly facilitating Russian penetration of the Czech nuclear energy sector through a no-bid contract for Kremlin-controlled Rosatom to rebuild two nuclear power plants.<sup>2</sup>

- Conversely, debunking false narratives about critical security-related issues, notably immigration, should also be included in regularised, expertise-based parliamentary discussions of threats. The existence in the Czech Republic of 'Islamophobia without Muslims'<sup>3</sup> serves as an example of what can happen when propaganda-based narratives on consequential issues spread unopposed and political extremists exploit them in order to divide society, attract support, and enshrine lies as truth.

## CONTEXT

**Communist groups in the Czech Republic.** The KSČM is the legacy party of the Communist Party of Czechoslovakia (KSC), which gave up effective sovereignty for more than 40 years in exchange for the Kremlin's political support and Soviet control over Czechoslovakia's political, economic, social and cultural development. The KSČM have never apologised for crimes committed during the communist era. Czech Communists have been consistently hostile toward NATO since 1990, even when

they did not align themselves with the Kremlin during the Yeltsin era when Russia was weak and preoccupied with domestic turmoil, and engaged in launching a "Partnership For Peace" with the transatlantic security alliance. Since Vladimir Putin's reassertion of Russian power projection in the international system, notably via his campaigns in Ukraine and Syria, the KSČM has openly aligned itself with the Kremlin on crucial security issues.

## KEY ACTORS

**KSČM** (*Komunistická strana Čech a Moravy – Communist Party of Bohemia and Moravia*)

**ANO** (*Akce nespokojených občanů – Action of Dissatisfied Citizens*) currently the dominant party in Czech politics and the personal political vehicle of PM Andrej Babiš

**ČSSD** (*Česká strana sociálně demokratická – Czech Social Democratic Party*), junior partner in current minority coalition government

**SPD** (*Svoboda a přímá demokracie – Freedom and Direct Democracy*) far-right anti-immigration, Eurosceptic party

**Halo Noviny** ('Hello Newspaper') longstanding print and electronic news outlet of the KSČM

**Miloš Zeman** Czech President (since 2013, re-elected 2018)

**Andrej Babiš** Czech Prime Minister (since July 2018), Chairman of the ANO political party (since 2012), billionaire businessman and owner of two major newspapers

**Vojtěch Filip** KSČM Chairman (since 2005), Member of the Lower House (since 1996)

**Jiří Dolejš** reformist Vice-Chairman of the KSČM, MP (since 2002)

**Zdeněk Ondráček** pro-Kremlin MP (since 2013)

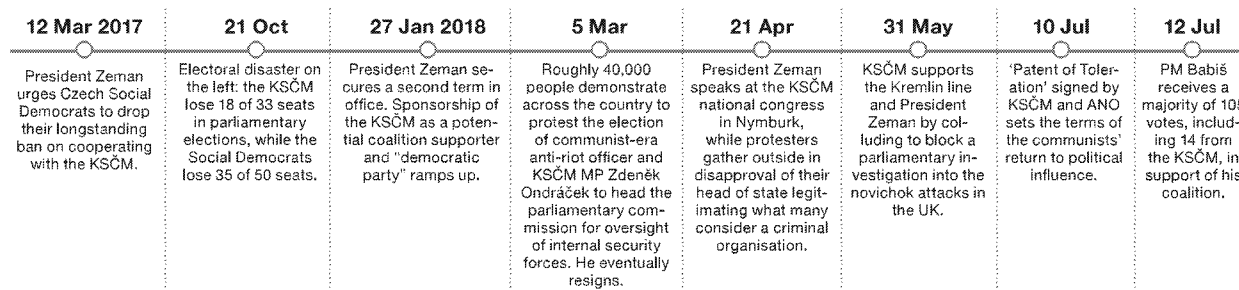
# NARRATIVES

## KSČM

- The UN, not NATO, should be the foremost guarantor of the security of the Czech Republic and the rest of Europe.<sup>4</sup>
- Russia, China and Iran should function as balancers of US and transatlantic power in the international system.
- Opposition to the Czech Republic's active commitment to NATO, including its participation in military exercises in the Baltic region.<sup>5</sup>
- Ideological links with Russia are no longer rooted in communism but have shifted toward a more open embrace of pan-Slavism.

- The KSČM will remain strongly pro-Moscow as long as the Kremlin acts as a balancer of US, NATO and EU influence in Eastern and East Central Europe.
- The Russian annexation of Crimea is legitimate and the Russian-supported uprising in Eastern Ukraine is a civil war. EU and US sanctions against Russia over Ukraine should be lifted.

# KEY EVENTS



# STRATEGIC LOGIC

Kremlin policy requires pre-empting popular demands for political change at home by making democracy appear weak, chaotic, failed, and inferior to the oligarchic system it must perpetuate in order to maintain the position of the current Russian elite. A large part of the Russian effort is aimed at opportunistically exploiting polarised debates in the Czech Republic, as well as supporting like-minded individuals, groups and political parties such as the KSČM. The KSČM does not appear to receive foreign funding, and

there exists no credible evidence of policy coordination with the Kremlin. Instead, the KSČM consistently aligns itself with Kremlin policy positions in order to oppose NATO, and to support the Kremlin's vigorous reassertion of Russian power in the region. The KSČM's alignment with Kremlin policies on key national security issues makes effective defence against hybrid threats less likely.

# MEASURES

**DIPLOMATIC.** Czech communists no longer have close diplomatic ties to the Kremlin. They instead act as a willing proxy on key policy and security issues. The main locus of official Russian diplomatic and political influence has shifted to President Zeman and his team of largely Kremlin-friendly advisors.

**INFORMATION.** KSČM hostility toward NATO and the EU have made them a reliable ally in the information war and establishing disinformation-based narratives in the Czech mainstream and alternative mass media. Two KSČM MPs aided the Kremlin cause by spreading pro-Kremlin disinformation in the Donbas region via local TV during an illegal visit in early 2016.<sup>6</sup>

**FINANCIAL.** Although past ties are well known, it is difficult to find credible evidence of financial links between Russia and the KSČM.

**INTELLIGENCE.** Moscow's priorities include covert infiltration of the Czech media<sup>7</sup> to spread Kremlin propaganda concerning Ukraine, NATO and the EU; exacerbating social and political tensions in the region; and relativising truth to encourage the idea that 'everyone is lying' and 'nothing can be believed.'

**LEGAL.** Persistent corruption weakens Czech law enforcement and justice. The current PM being under criminal investigation for EU subsidy fraud, and his reliance on support from the KSČM, considered by many to be an organisation with a criminal past, highlight this.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Public confidence in the state and rule of law, a crucial pillar of which is the fight against corruption in high politics.
- Public confidence in the mainstream media.
- Commitment to liberal democratic values, maintaining strong links to the western and transatlantic alliance.

## VULNERABILITIES

- Low political will of the informal Zeman-KSČM-ANO alliance to tackle threats to national security from the Russian Federation.
- Less than one-third of Czechs strongly support EU membership and roughly 40 per cent would prefer neutrality to NATO membership.<sup>8</sup> The potential for manipulating public opinion and political decision-making remains high.

## THREATS

- Increasing political radicalisation due to largely disinformation-based anti-immigration messaging.
- Measures targeting media and information sectors disrupting democracy.
- Continued Kremlin exploitation of Czech politicians (including President, PM, KSČM) to justify further hostile acts including Eastern Ukraine, Crimea, novichok attacks.<sup>9</sup>

## EFFECTS

- Lingering corruption charges against PM hurt Czech reputation in EU and elsewhere abroad.
- Approval of mainstream politicians is low.
- KSČM's opportunistic cabinet support weakens Czech democracy and trust in government.
- Russia ramping up exploitation of informal, Kremlin-friendly Zeman-KSČM-ANO-SPD alliance to threaten NATO cohesion (e.g., plausible deniability in novichok attacks exploited at home in Kremlin-controlled media and abroad after Zeman's statement echoing Kremlin narrative).<sup>10</sup>

# BRONZE NIGHT RIOTS

## SUMMARY

The 'Bronze Soldier' is the informal name of a controversial Soviet-era war memorial, which was located in the centre of Tallinn, Estonia's capital city, until April 2007. To many Russian-speaking groups in Estonia, the monument symbolised the victory of the Soviet Union over fascist Germany. To ethnic Estonians, it was a permanent reminder of Soviet occupation and the atrocities committed by the regime against the Estonian people. Starting in the mid-1990s, the statue became increasingly popular as a location for the Russian-speaking community to gather every year to celebrate 'Russian Victory Day'. After the statue became the site of a number of activist stunts, incidents of vandalism, protests and clashes, the situation became untenable.<sup>1</sup> A bill to demolish the memorial was rejected in 2007, but a plan was ordered by the Estonian President to remove the statue and its surrounding graves from the city centre.

Russian-speakers and pro-Russian NGOs mobilised to protest the removal of the monument. After the monument was covered up on 26 April, a crowd of over 1,000 people, mostly ethnic Russians, gathered at the site. Later that night, cars were set on fire and shops were looted in the city centre, during which a Russian citizen was stabbed to death. Around 1,000 people were detained and 150 people, including police officers, were injured, with protests also spreading to other cities in Estonia.<sup>2</sup>

The civil disturbances were not isolated incidents related to the statue's removal. A series of cyber attacks were launched against the websites

of the Estonian government, media and financial institutions, consisting largely of denial of service attacks and website defacements. In the days following the relocation, protesters surrounded the Estonian Embassy in Moscow, threw stones at the building and mobbed embassy workers, calling for an apology by the Estonian government and a reversal of the statue removal.<sup>3</sup> Russian government officials encouraged Russians to boycott Estonian goods, rail links between Estonia and Russia were severed due to 'unscheduled repairs', and border checks between the two countries were lengthened. By 30 April, the statue had been moved to the Cemetery of the Estonian Defence Forces in Tallinn.

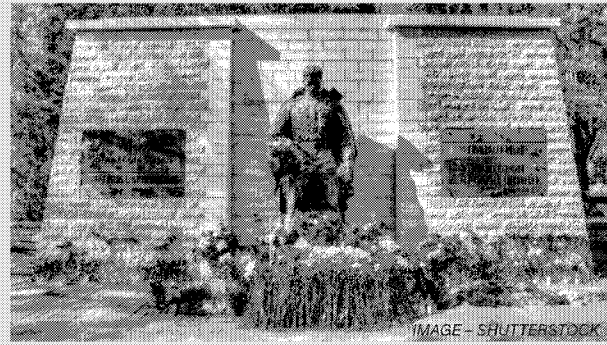


IMAGE - SHUTTERSTOCK

## KEY POINTS

- The events of Bronze Night featured a range of different measures employed by the Russian Federation (diplomatic, financial, cyber, NGOs and economic) that were integrated and synchronised in support of broader strategic objectives.

- The Russian modus operandi is to create pressure and intensify social divides, then take advantage of crises once they emerge. It is likely the Russian Federation was not directly responsible for orchestrating the civil disorder, but that it increased tension, making a crisis more likely to occur, actively supported the protests and did not discourage the conflict from escalating.<sup>4</sup>

- Inflammatory political rhetoric can exacerbate divisions between different identity groups, creating vulnerabilities which are exploitable by malign actors. Building resilience to such threats requires audience-focused research to understand fracture lines between groups, enabling effective policy-making which needs to be driven by strong political leadership.

- A strong civil society and independent media sector can reduce societal tensions by enabling inclusive public discourse and supporting the development of a national identity based on shared values, rather than ethnicity, language or identity.<sup>5</sup>

## CONTEXT

- **History of the 'Bronze Soldier' Memorial.** The monument had been erected by the Soviet authorities in 1947 and was originally named the 'Monument to the Liberators of Tallinn'. After independence in 1991, this was changed to 'For those Fallen in World War II'.<sup>6</sup> Every 9 May, ethnic Russians gathered at the memorial to commemorate Russian 'Victory Day' with the event becoming more popular in the mid-1990, increasingly with the presence of Soviet symbols (such as Soviet Army uniforms). Like other Soviet monuments in Estonia, the memorial had long been controversial and became a focal point for activists – it was vandalised and covered in paint several times. In May 2006, confrontations between Estonians and Russian-speakers in front of the statue prompted the Minister of Interior to prohibit demonstrations the next day. The same year, an Estonian nationalist threatened to destroy the statue if it was not removed, and the police started to guard the memorial round-the-clock.<sup>7</sup>

- **Compatriot policy.** The concept of 'compatriots abroad' is defined under Russian foreign policy as "individuals who live outside the borders of the Russian Federation itself yet feel that they have a historical, cultural, and linguistic linkage with Russia."<sup>8</sup> Since 1994, this concept has developed into a number of laws, state programmes and policies to strengthen ties with the Russian diaspora in the 'near abroad' of former members of the Soviet bloc, and leverage such groups to influence policies and decision-making in the country of their residence. The issue of compatriots came under greater scrutiny after the annexation of Crimea in 2014 was justified by the need to protect Russian minority groups in Ukraine.

## KEY ACTORS

### Estonian Internal Security Service (KaPo)

**Ministry of Defense** Relocation of the monument was led by the MoD.

**Ministry of Interior** Main task of guaranteeing public order.

**Reform Party (Reformierakond)** Estonian political party. Proposed moving the statue in 2006 which may have increased support for them. Became largest party (28 per cent) in March 2007 elections.

**Night Watch group (Nochnoy Dozor)** Youth group formed in mid-2006 to protect the monument.

**Naši organisation** Officially endorsed Pro-Kremlin youth group based in Russia.

**Andrus Ansip** Prime Minister of Estonia (2005–2014), leader of Reform Party.

**Dmitri Linter, Maksim Reva, Dimitri Klenski** leaders of Night Watch group.

**Mark Sirök** leader of Naši organisation.

**Jüri Bõhm** Estonian nationalist whose protest at the 9 May celebration in 2006 received a lot of media attention.

# NARRATIVES

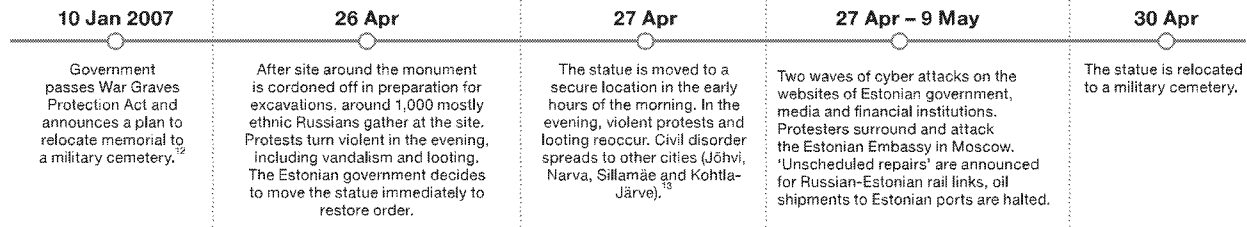
## Russian government

- The Bronze Soldier commemorates the Soviet victory in the Great Patriotic War.
- We condemn people who desecrate memorials to war heroes.<sup>9</sup>
- Estonia is indulging neofascists and inciting extremism.<sup>10</sup>
- Soviets were liberators, not occupiers, and their activities were justified measures against fascism.
- Russian-speakers should stand up against authorities and defend the statue.

## Estonian government

- The busy centre of Tallinn is the wrong location for such a memorial.
- Such memorials are symbols of occupation. Relocation of the statue will de-escalate the situation and prevent confrontation.
- This is an internal matter for Estonia and does not require discussion with the Russian Federation.
- These events constitute a well-coordinated and flagrant intervention into the internal affairs of Estonia.<sup>11</sup>

# KEY EVENTS



# STRATEGIC LOGIC

Based on the available evidence, it is unlikely that the Russian Federation was directly responsible for creating the Bronze Night crisis, but it shaped the information environment to set favourable conditions for it to occur, actively supported the protests and effectively encouraged the disorder to escalate.<sup>14</sup> The integration of measures and the ability to escalate them

should be seen as part of Russia's long-term strategy of attempting to destabilise Estonia and retain influence in what it considers a traditional sphere of interest.

# MEASURES

**DIPLOMATIC.** The Russian government used openly hostile rhetoric, encouraging pro-Russian protesters and organisations in Russia and Estonia. Foreign Minister Lavrov talked of "blasphemy" which would have "serious consequences for our relations with Estonia,"<sup>15</sup> and the State Duma's lower house unanimously passed a resolution which accused the Estonian parliament of "glorifying fascism" and called for economic sanctions.<sup>16</sup>

**INFORMATION.** The Russian government has also been accused of organising or at least condoning, the protests in front of the Estonian embassy in Moscow, which were organised mainly by the youth organisation Naši.<sup>17</sup> The Russian embassy in Estonia was believed to communicate with and support the Night Watch group, which was instrumental in rallying the protests, although an Estonian court later acquitted the Night Watch of charges of riot instigation.<sup>18</sup> Many Estonian politicians and media outlets

accused the Kremlin of organising the cyber attacks, then denying responsibility and attributing them to 'patriotic' individuals and criminal groups. The Russian Embassy in Tallinn provided Russian media organisations reporting from Estonia specific, Kremlin-friendly local contacts in an attempt to slant coverage.<sup>19</sup>

**ECONOMIC.** After calls from Russian government officials, many Russian companies effectively sanctioned Estonia by boycotting Estonian goods and services.<sup>20</sup> Moreover, transportation across the Russian-Estonian border via the Narva River bridge was severely limited, and rail links were severed for several weeks due to 'unscheduled repairs',<sup>21</sup> which interrupted oil and coal exports to Estonia. The overall estimated cost of the Bronze Night was 1.85 per cent of Estonia's GDP.<sup>22</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Political stability and societal unity.
- Integration of Estonia's significant Russian-speaking community (about a quarter of the population).<sup>23</sup>

## VULNERABILITIES

- Russian-speakers in Estonia are more likely to be exposed to media outlets such as PBK and RTR Planeta, which promote a pro-Kremlin point of view as part of Russia's foreign policy.
- Conflicting interpretations of history (World War II and Soviet rule) between Estonian and Russophone identity which are often very sensitive and emotionally-charged.
- The Estonian economy is mostly oriented to EU markets, but Estonia receives all of its natural gas from Russia, and a significant volume of Russian goods are transported through Estonian railways, making them vulnerable to disruption.<sup>24</sup>

## THREATS

- Historical narratives are often used by the Russian government to exacerbate social tensions in the Baltics and as pretext for hostile measures.
- The Bronze Night events challenged Estonian integration policies and threatened to undermine social cohesion, with the real possibility of violent conflict between groups.

■ Rhetoric on discrimination of minorities, and lack of respect for WWII-soldiers who died fighting fascism, threatened Estonia's international reputation as a peaceful and democratic country.<sup>25</sup>

## EFFECTS

- 91 people were convicted, 6 sent to prison, 67 received suspended or part-suspended sentences. 48 were banned from entering Estonia again.<sup>26</sup>
- On 24 May, the EU adopted a resolution expressing support for and solidarity with Estonia. Nevertheless, some national representatives also suggested that the relocation of the memorial was provocative.<sup>27</sup>
- Polls showed that confidence in the government increased after the riots (from 53 per cent in 2006 to 66 per cent in 2007).<sup>28</sup>

# RUSSKIY MIR FOUNDATION IN THE BALTICS

## SUMMARY

During the early 2000s, President Vladimir Putin attempted to develop relations with the West by trying to re-introduce post-Soviet Russia as an equal and respected member of the Western political system. This was supported by the establishment of an array of institutions designed to explain Russian politics to experts and decision-makers, promote Russia's cultural heritage and provide information on the 'true' Russia. Towards the end of the first decade of the 20th century, Russia's approach gradually became more confrontational with the West, and this ecosystem transformed into a set of instruments to reflect this shift in foreign policy.

The Russkiy Mir Foundation (RMF) was established in June 2007 as part of this ecosystem. The RMF is a joint project of the Russian Ministry of Foreign Affairs and the Ministry of Education and Science, and its director and board are directly appointed by the Russian president.<sup>1</sup> The RMF runs over a hundred so-called 'Russian centres' worldwide, most actively in Europe, which promote Russian language, heritage and culture. Its activities also include the organisation of events and debates, and the provision of grants to non-profit organisations for projects on Russian language and culture.<sup>2</sup>

The RMF takes its name from the concept of the 'Russian world' (Russkiy mir or Русский мир), a supra-national cultural identity consisting of Russia, diaspora living abroad and other so-called 'Russian-speaking' communities, and incorporating language, culture, historical memory and the orthodox church.<sup>3</sup> Such communities outside of Russia fall under its 'compatriot policy', a loosely-defined concept used as means to leverage influence particularly in those nations Russia considers part of its traditional sphere of influence, such as the Baltic states of Estonia, Latvia and Lithuania. The RMF is therefore about influencing foreign audiences and interacting with compatriot communities, evolving from an educational institution established to promote the Russian language abroad into a more calculated expression of Russian influence overseas.<sup>4</sup> It is difficult to assess the direct impact of the RMF, but despite its ambitious remit and negative publicity, public awareness of RMF in the Baltics is assessed to be low and their impact minimal, with activities mostly promoted to ensure the continued provision of resources from Moscow.<sup>5,6</sup>

## KEY POINTS

- The RMF should be seen as a tool of Russian foreign policy, with a mandate including: the defence of human rights; protection of the interests of compatriots living abroad; consular matters and partnerships in the cultural and scientific sectors.<sup>7</sup> While the RMF is modelled on cultural institutions such as the British Council, the Goethe-Institut and the Institut Français, what differentiates the RMF are its activities, which can threaten the social cohesion of the host nation, for example by promoting controversial interpretations of history.

- Not all soft power measures are malicious. Traditional public diplomacy (such as cultural and educational exchange programmes) has an essential part to play in maintaining cordial relations between nations. Identifying such activities as hostile should be done on a case-by-case basis, and care should be taken not to overinflate the threat. Over-estimating the ability of such organisations to hurt the host nation can escalate the perception of confrontation, exacerbating social fractures and increasing polarisation between social groups.<sup>8</sup>

## CONTEXT

- **Russia's 'soft power'**. In the early 2000s, the Russian leadership started to adjust their political system to foster the dialogue with the West and to streamline the country's re-engagement with the rest of Europe. Putin's regime developed a soft power projection system described as "a matrix of tools and methods to reach foreign policy goals without the use of arms but by exerting information and other levers of influence."<sup>9</sup> Over time, the Russian leadership started to believe that the West had no intention to accept Russia as an equal partner, and progressively construed the situation as that of increased political pressure on Russia and its ruling elite.

- **Compatriot policy**. 'Compatriots' can be broadly defined as: persons demonstrating commonality of language, history, cultural heritage, traditions and customs with the Russian state; persons living beyond the borders of the Russian Federation having spiritual, cultural, and legal

connections with Russia, and persons whose direct relatives lived on the territory of the Russian Federation or the Soviet Union.<sup>10</sup> By this definition, 30 per cent of Estonia's population are Russian compatriots, in Latvia approximately 34 per cent and in Lithuania only around 8 per cent. However, language, citizenship and ethnicity do not provide clear boundaries for identification. Simply because individuals fall under the official definition does not mean that they identify as being part of, or subscribe to, the values of the 'Russian World'.

- **Strategic framing of 'Russian speakers'**. The importance of Russia's 'compatriot' populations in the 2008 invasion of Georgia, the 2014 annexation of Crimea and in references by Russian policymakers to the benefits of agitating local communities have increased concern about the work of organisations such as RMF.

## KEY ACTORS

**Rosstrudnichestvo** *Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation*

**Puškini Instituut in Tallinn** *with branches in Tartu and Narva*

**Russian Centre at Daugavpils University** *often used as an example of the most successful Russkiy Mir project in the Baltic region*

**Russian Language and Cultural Studies Centre at Lithuanian University of Educational Sciences in Vilnius** *key partner for RMF in Lithuania*

**Russian centre in Šiauliai University, Lithuania** *the only centre outside the Lithuanian capital supported by RMF*

**Vladimir Kochin** *RMF Executive Director*

**Vyacheslav Nikonov** *The RMF Management Board's Chairman (since 2012), Chairman of the Committee on Education of the State Duma (since 2013)*

**Ludmila Verbitskaya** *Board of Trustees' Chairperson*

**Georg Bovt** *Editor-in-Chief of RusskiyMir.ru magazine*

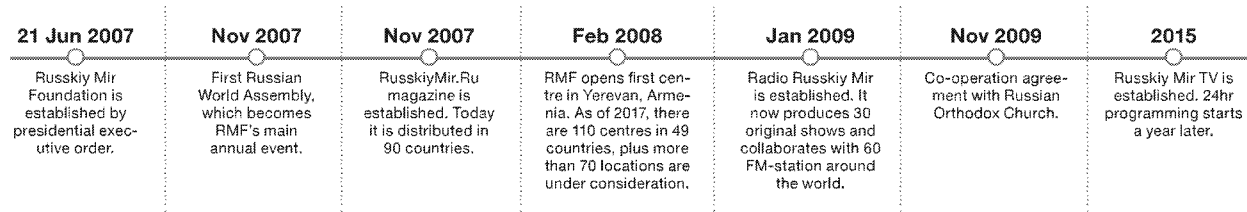
# NARRATIVES

## Russkiy Mir Foundation

- The Baltic States are in the traditional sphere of Russian cultural influence: Russian literature, theatre, cinema, media and art should be easily accessible.
- Russian language education should be available to Russian-speakers in the Baltics.
- Russia is a peaceful country and would never attack the Baltics. It was their mistake to join NATO, and NATO troops should not be near the Russian border.

- The Soviet army did not occupy the Baltic States in 1940; this was a voluntary process. Many Estonians, Latvians, and, to a lesser extent, Lithuanians were Nazi collaborators. Today's regimes in the Baltics glorify their Nazi collaborators, which is unacceptable and should be punished by the EU.
- Russian Empire and Soviet Union periods were good for the economies of Estonia and Latvia. When they left the USSR in 1991, they had strong and diverse industries which were lost by the time of EU accession.

# KEY EVENTS



# STRATEGIC LOGIC

The Russkiy Mir Foundation should be seen as part of an array of institutions developed to exert 'soft power' in line with Russian strategic thinking in the mid-2000s and underscored by the concept of the 'Russian world'. The RMF is one element of an effort to build a network of individuals and

organisations to directly influence the political decision-making of the nations where they are located and to sustain the perception of an identity group which enables confrontation.

# MEASURES

**DIPLOMATIC.** RMF activities are supported by embassies and support their missions' public and government relations.<sup>11</sup> There is no evidence of systematic synchronisation of plans and activities between Russia's Ministry of Foreign Affairs and the RMF.

**FINANCIAL.** RMF's grant activities are important to preserve and support cultural, educational, social, and, to a lesser extent, political activities of ethnic Russian and Russian-speaking communities. RMF funding is not disclosed in official sources, but the RMF director confirmed that the state provided RUB 475 million (approx. USD 7,462,250)<sup>12</sup> in 2016, RUB 446 million (approx. USD 7,006,660) in 2017, and that they expected to receive a further 6-8 per cent decrease in 2018. It was reported that RMF spent 170,000 EUR in Latvia in the period 2007 – 2012.

**INFORMATION.** RMF supports or promotes activities that can be perceived as politically biased such as the *Immortal Regiment Campaign* across Europe, a movement which marks the end of the "Great Patriotic War."<sup>13</sup> RMF works with a wide range of educational and cultural organisations across the region, both directly and indirectly related to the ethnic Russian and Russian-speaking population. Moreover, it works with organisations providing venues for Russian-related activities or having some of them in much broader programmes of other activities related to other ethnic groups, cultures, or languages. While limited, this network of contacts includes many actual or potential opinion-leaders and newsmakers within ethnic Russian and Russian-speaking communities.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS<sup>14</sup>

- Democracy, constitutional order, independence and sovereignty.
- Social cohesion between different groups in society; strong national identity; societal resilience towards misinformation and divisive influence.
- Trust in government and public institutions (for example the education system).

## VULNERABILITIES

- Cleavages between majorities and Russian-speaking minorities. For example in Latvia and Estonia, where the titular-speaking majority comprises 62 per cent<sup>15</sup> and 68.8 per cent<sup>16</sup> respectively, the rest of the population are predominantly Russian-speakers. These cleavages manifest themselves in divergent historical memory, as well as different and often opposing views on issues related to Russia, the West at large and the United States and NATO in particular.
- Penetration of the Russian state and private media in the information space. E.g. in Latvia, TV broadcasts made in Russia are watched by 63 per cent of inhabitants of Latvia; 80 per cent of Russian-speakers use Russian-language sources to acquire information.<sup>17,18</sup>

## THREATS

- By spreading divisive narratives on political, cultural and historical issues, institutions like the RMF can increase inter-ethnic divides in Latvia and Estonia, and undermine national unity.
- Uneven regional development, social inequality, poverty, poorly adapted segments of society or manifestations of intolerance can create social instability. The polarisation of society due to adversarial opinions and understandings increases uncertainty and decreases society's resilience to hostile external influence.

## EFFECTS

- RMF works across over 100 countries, so it is difficult to isolate and measure the impact of its activities. However, observations suggest that RMF has been more influential in countries which are more exposed to the influence of Russia and Russian language and culture, for instance due to geographical proximity.
- RMF encourages ethnic Russians and Russian-speaking people in the Baltic states to preserve their culture and identity. It promotes a common identity based on Russian language and culture, which can slow the integration of Russian-speaking people in Estonia, Latvia, and Lithuania.<sup>19</sup>

# CRIMINAL NETWORKS IN THE DONBAS

## SUMMARY

Corruption continues to be a significant issue in Ukraine, due to its Soviet past, weak national institutions and poor governance during the early 1990s and present-day links to the Russian 'mafia state'. The government has long been troubled by kleptocrats and an extensive bribery and embezzlement culture. Widespread criminal activity and illicit circles primarily seeking economic gain have existed in Ukraine since the collapse of the Soviet Union, particularly in the Donbas (eastern Ukrainian region commonly used to describe the oblasts of Luhansk and Donetsk). The Russian Federation is known to use such crime groups in Europe, often functioning behind 'indigenous European gangs' such as the pre-existing criminal networks in Ukraine, used as instruments of intelligence and political influence.<sup>1</sup>

When civil unrest began in 2014, the Russian Federation capitalised on its long-term exploitation of these vulnerabilities to quickly produce a fully realised threat. Using existing criminal networks, they provided lethal aid (small arms, heavy weapons, vehicles and artillery pieces), training and leadership to separatists in eastern Ukraine. In addition to taking an active part in the fighting, networks disrupted supply lines,

disrupted military forces and contributed to disinformation, effectively preventing a coherent Ukrainian response to Russia's conventional forces. By creating favourable conditions for Russian operations in the region, Russia-linked criminal networks enabled the Russian Federation, through separatist rebels, to conduct a swift and deep military conflict in the Donetsk and Luhansk Oblasts in eastern Ukraine.

As the crisis deepened and became increasingly violent, criminal networks in the Donbas region flourished. Low-level petty criminals, politically influential Russian and Ukrainian kleptocrats, and oligarchs (corrupt heads of private industry, politicians and high-level officials), were responsible for trafficking food, alcohol, cigarettes, coal, fuel, and weapons. Expansive criminal networks and sweeping corruption in both Ukraine and the Donbas still impact the conflict directly, with the Security Service of Ukraine reporting incidents or weapons smuggling and military supply contracts going to unqualified manufacturers. This poses a direct threat to crucial political reforms for Euro-Atlantic integration and the administration of financial aid in support of stabilisation.

## KEY POINTS

- Criminal networks were pervasive across public and private sectors, along with high levels of corruption and kleptocracy, which led to political and security vulnerabilities. Both internal and external actors exploited these vulnerabilities to the detriment of national security interests.

- While corruption in Ukraine maintains many classic post-Soviet features, it differs from Russian corruption in how it is organised and sustained. Corruption in Russia is considerably more reliant upon personalities and strong allegiances, particularly when it comes to large-scale corruption. In Ukraine, the overall availability of resources is markedly smaller, and few can hold onto any particular rent-seeking sector, or profitable scheme, for long without needing to form alliances with an ever-changing list of state actors, intra-regional rivals, and criminal groups. This is a topic worthy of analysis as it speaks to the unique

security risks that Ukrainian corruption and criminal networks pose to Ukraine and Ukraine's partners.

- Eliminating the systemic tendency of corruption and building trust in state institutions are vital to enable the reintegration of non-government-controlled areas. This means developing a robust legal framework and enhancing public confidence in the judiciary through the professional development of judicial personnel, transparency for financial arrangements and improved pay for judges. Governments should also reduce and deter corruption through high-level punitive action, amnesty programmes for lower-level corrupt business people, the promotion of more transparency across government and private sectors and focus on areas such as border guards or law enforcement which enable criminal networks to operate.

## CONTEXT

- **Corruption in Ukraine.** Grand corruption describes how "the abuse of high-level power benefits the few at the expense of many causing serious and widespread harm to individuals and society."<sup>2</sup> Ukraine is amongst the most corrupt countries in the world: in 2014, it was ranked 142 out of 175 in the Corruption Perceptions Index.<sup>3</sup> Some of the most high-profile embezzlement cases include former President Yanukovich, the Interior Minister's Son Oleksandr Avakov, as well as the Deputy Defence Minister.<sup>4,5,6</sup> The Ukrainian government's systemic problems stall attempts at improvement and holding corrupt persons accountable for their actions.<sup>7</sup>

- **Criminal activity in the Donbas.** In Soviet times, the largest numbers of criminal prosecutions in the Ukrainian Soviet Socialist Republic were in Donetsk and Luhansk Oblasts, collectively accounting for one-third of criminal trials in the republic.<sup>8</sup> Following the collapse of the Soviet Union and the accompanying power vacuum, there was a surge in crime, as well as the integration of criminal activity in business, politics, and legal affairs/<sup>9</sup>

law enforcement.<sup>9</sup> In Ukraine, as the state formed and stabilised, high-ranking criminals became functionally legitimate businessmen and politicians. Criminal activity ranges from local smuggling rings to large-scale heavy industries – the Donbas holds the epicentre of Ukraine's heavy industry, metallurgical facilities, and most of the country's essential coal mines.<sup>10</sup>

- **The conflict in eastern Ukraine.** As a result of the ousting of President Yanukovich during the 2014 Ukrainian revolution, as well as the annexation of Crimea by the Russian Federation, a pro-Russian armed insurgency began in the Donbas. Donetsk and Luhansk declared "independence" after holding unrecognised referendums. Press, civilians, humanitarian organisations, and non-government organisations separately reported the presence of Russian soldiers in eastern Ukraine, as well as report sightings of lethal aid crossing the Russian-Ukrainian border. Since the outbreak of the conflict, bribery and corruption have become prevalent on both sides of the contact line.<sup>11</sup>

## KEY ACTORS

**Party of Regions** *Ukrainian pro-Russian political party; electoral and financial base primarily in east and southeast*

**'Donetsk People's Republic' (DPR) and 'Luhansk People's Republic' (LPR)** *Unrecognised non-government-controlled areas in Donetsk and Luhansk Oblasts, Ukraine*

**Security Service of Ukraine (SBU or SSU)**<sup>12</sup>

**National Anti-Corruption Bureau of Ukraine (NABU)**<sup>13</sup>

**Specialised Anti-corruption Prosecutor's Office (SAPO)**<sup>14</sup>

**Viktor Yanukovich** *former President of Ukraine (2010-2014), removed from power as a result of the Euromaidan Revolution*

**Petro Poroshenko** *President of Ukraine (2014-present)*

**Vladislav Surkov** *aide to the President of Russia (2013-present), heavily involved in Russian activity in eastern Ukraine*<sup>15,16</sup>

**Igor Plotnitsky** *head of the "LPR" (2014-2017); held monopoly over supply of goods including pharmaceuticals and contraband fuel*

**Aleksandr Zakharchenko** *head of the "DPR" (2014-2018); involved in counterfeit cigarettes and amphetamines; close ties to the Kremlin*

**Rinat Akhmetov** *Ukrainian businessman and oligarch from Donetsk; richest man in Ukraine*<sup>17</sup>



# NARRATIVES

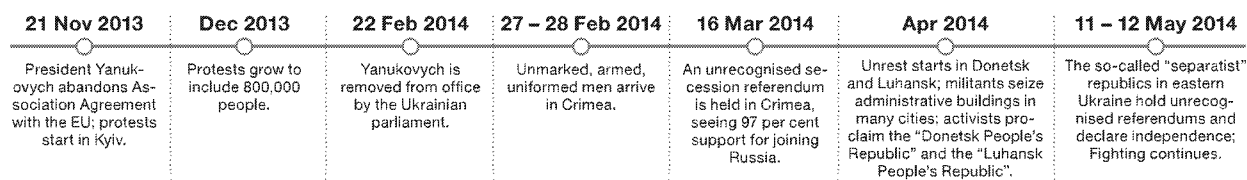
## Ukrainian government

- Russia is the aggressor in eastern Ukraine and Crimea; it is violating Ukrainian territorial integrity and state sovereignty.
- The Russian Federation uses covert forces to undermine state stability and progress towards the West.
- There are new government institutions and civil society organisations focusing on anti-corruption efforts. These efforts include fighting criminal networks and Russian influence in Ukraine.

## Russian government

- The Russian Federation is only acting in the interest of ethnic Russians and Russian citizens in Ukraine.
- Ukraine is a corrupt, failed state; its instability has domestic origins.

# KEY EVENTS



# STRATEGIC LOGIC

Russia's strategy in Ukraine involved the use of non-military means to undermine the authority of the government and destabilise the situation. Despite operating primarily for financial self-interest, criminal elements were connected to Russia through regional business interests and supported by

or including Russian or pro-Russian kleptocrats.<sup>18</sup> Russia used these connections to encourage existing anti-government elements to challenge the government, initially through protest and then via direct action, becoming a separatist insurgency.<sup>19</sup>

# MEASURES

**DIPLOMATIC.** The same corrupt government officials involved in or enabling criminal networks lead to conflicting difficult diplomatic relations with both Russia and the West. Oligarchs with lucrative business ties to Russia are said to have used their extensive political influence to undermine Ukraine's approach towards the West.<sup>20</sup>

**INFORMATION.** Many news and media outlets were/are owned by oligarchs (including President Poroshenko, Rinat Akhmetov, Ihor Kolomoisky, Dmytro Firtash and others), and known to be utilised for political goals.<sup>21</sup>

**MILITARY.** The conflict in eastern Ukraine created an ideal environment for the pre-existing illicit global arms trade network and market by creating a legal vacuum and a new market for materiel. Illegal arms trade occurs on both sides of the contact line, as a lack of legislation and regulation enables a bustling criminal network. Moreover, officials in state defence enterprise UkrOboronProm owned shell companies that were used for fraud and embezzlement schemes to use substandard parts, including used and outdated engines, to pocket the profits.<sup>22</sup> NABU investigations allege that millions of dollars have been syphoned off of military equipment contracts, both domestic and international.<sup>23</sup> These criminal activities benefitted the Russian-led separatists who fought a military with sub-part armaments. Inability to address these issues will prevent Ukraine from reaching its goal to meet NATO standards by 2020.

**ECONOMIC / FINANCIAL.** Large-scale criminal networks are often disguised through shell operations and layers of persons at various levels in different sectors.<sup>24</sup> Kleptocrats control parts of all sectors, including government, heavy industry, finance, military, and information. Prevalent corruption in Ukraine enables billions of dollars to be misappropriated from government contracts, development funding, and international aid. Decision-making is often closely interlinked with corruption: it was, and in some cases still is, typical to bribe border guards, law enforcement, and government officials to achieve a particular outcome.

**INTELLIGENCE.** High level of infiltration of the Ukrainian intelligence services by Russian spies, and evidence of substantial cooperation between the Ukrainian Security Service (SBU) and the Russian Federal Security Service (FSB), significantly degraded Ukrainian intelligence capability, including through the defection of entire units to the rebel side.<sup>25,26,27</sup>

**LEGAL.** The broken judicial system enabled corrupt officials to operate, making the country unable to enforce reforms completely. Since 2014 Ukraine has made substantial progress in legal reform and law enforcement. However, many past issues remain due to the dynamic between political corruption and a weak institutional framework.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Political independence, effective state institutions, transparent decision-making, public trust in government processes.
- Sovereignty, territorial integrity and full control over all regions.
- Reliable security guarantees.<sup>28</sup>
- Economic independence.
- Domestic reforms as part of the path towards possible EU membership and further integration with the West.
- Fully functional modern military that meets NATO defence and security standards by 2020.

## VULNERABILITIES

- Widespread corruption and subordination of public authorities to corporate and personal interests, embezzlement of public funds, disorganised public bodies, political appointments based on loyalty rather than merit. Weakened and inefficient public institutions (particularly military- and security-related) which were unable to address critical political issues.
- Security and defence issues were not a high priority for Kyiv, and western political engagement was stagnant ("Ukraine fatigue").<sup>29</sup>
- Weapons and equipment were outdated or obsolete, there was an insufficient logistical support system, and lack of intelligence/ counterintelligence force. Criminal networks and corruption in the Ukrainian government continue to lead to misappropriation of funds or rigged contracts leading to an ill-equipped Ukrainian Armed Forces.<sup>30</sup>
- Enormous amounts of international aid led to embezzlement and misappropriation of funds.

- Political and business links with formal or informal ties to Russian governmental or commercial entities were integrated into parts of criminal networks.

## THREATS

- Territorial violation of the highest degree in the form of separatism actively supported by the Russian Federation. Russian military presence in eastern Ukraine. Destabilisation of the Ukrainian state.
- Exploitation of existing vulnerabilities by the Russian Federation, which used criminal networks to influence politics, ran disinformation campaigns, and destabilised the Ukrainian state.

## EFFECTS

- Political functions inhibited; difficult to implement reforms; prevention of progress.
- Unemployment, poverty, social injustice, overall public distrust in the government after decades under oligarchical systems.
- Ongoing economic crisis with a weakened national currency and ongoing developmental reforms. Many corrupt oligarchs and elites have been removed, but not all of them.
- Ukrainian government established three anti-corruption bodies in recent years (NABU, NAPC, SAPO). Ukraine has yet to create an independent anti-corruption court per its mandate. One survey found that 80 per cent of Ukrainians in government-controlled areas consider the fight against corruption as unsuccessful.<sup>31</sup>

# CIVIL DISORDER IN BAHRAIN 2011

## SUMMARY

In 2011, the Kingdom of Bahrain was affected by the 'Arab Spring', a wave of popular protests that spread across the Middle East and North Africa. The first, mostly peaceful protests took place on 14 February and involved around 6,000 people nationwide of mixed religious and social backgrounds. Social media played a crucial role both in the organisation of protests and as a source of information. Bahrain had experienced low-level political unrest for a few years and in the six months since the previous parliamentary elections, which were viewed as flawed. Protesters, predominantly Shia, were angered by the slow pace of political reform, the apparent favouritism to foreign workers over Bahraini citizens and discrimination against them by the ruling Sunni minority. At the start of protests, their demands included political and constitutional reforms, an end to inequality and systematic discrimination towards Shia Muslims, and to the alleged practice of political naturalisation of Sunni Muslims to change the country's demographics.

Fuelled by anger at the government's insufficient response to the demands and the use of lethal force by the security forces, the protests escalated quickly. The nature of the protests soon changed, with demands emerging for the end of the ruling regime. In March, the protests became increasingly violent and led to sectarian clashes. Bahrain requested support from its Gulf allies, who sent 1,500 Gulf Cooperation Council (GCC) troops into Bahrain to help restore stability.

It is likely that deliberate agitation by Iran, by way of overt public statements and agents of influence, contributed to the escalation. The Iranian regime, most prominently Ayatollah Khamenei, expressed criticism of the Bahraini government and voiced support for the disadvantaged Shia population. These statements framed the protests as a sectarian issue and encouraged the Shia opposition. Moreover, Iranian Arabic-language TV channels encouraged Shia protesters in Bahrain.<sup>1</sup> It is reasonable to assume that the Iranian government was interested in the destabilisation of the Bahraini regime, given Iran's historical record of interfering with Bahrain's interior affairs, combined with its territorial claims over the country. The Bahraini government repeatedly

denounced the existence of external interference behind the uprising, and explicitly referred to Iran.<sup>2</sup> As a result, the protests were framed as being the result of interference from an external actor, rather than acknowledging those grievances that underpinned the mobilisation of certain communities to protest. The main opposition party, Al-Wefaq, complained that state-controlled media portrayed the protesters as sectarian and pro-Iranian from the outset. Alleged Iranian interference was systematically used by the government to justify repression in the years following the 2011 uprising.



IMAGE – Bahraini protest on 22 February 2011.  
WIKIMEDIA / Lewa'a Alnasr

## KEY POINTS

- The grievances of the Bahraini Shia population were a critical vulnerability which gave Iran the opportunity to exert influence. Tensions between sectarian groups should be minimised by political dialogue and the fostering of national unity and identity based on shared values which sets itself apart from both Iran and Saudi Arabia.
- The Bahrain Independent Commission of Inquiry was unable to find any material evidence of Iranian interference, partly because of the commission's lack of access to confidential government reports.<sup>3</sup> Despite this, after the report was published the King gave a speech in which he repeated the claim that "Iran is supporting anti-government protests", an apparent contradiction with the official report which

highlights the difficulty in publicly attributing responsibility for hostile acts.<sup>4</sup>

- The media in Bahrain was biased towards the government of Bahrain. Six out of Bahrain's seven daily newspapers were pro-government, and all radio and television broadcasts in Bahrain state-controlled. During the protests, government censorship was particularly harsh, and state media gave inaccurate or one-sided versions of events, in particular by presenting the demonstrations as purely sectarian and linked to Iran. The media did not represent the views of the vast majority of Bahrainis, many of whom felt marginalised as a result.<sup>5</sup>

## CONTEXT

■ **Bahrain.** The Kingdom of Bahrain became independent in 1971 and is ruled by the Al Khalifa family, who are Sunni Muslims.<sup>6</sup> 70.3 per cent of the population is Muslim, the majority of which are Shiites (no official figures available). One of Bahrain's main allies is the Kingdom of Saudi Arabia (Sunni). It has had strained relations with Iran, where Shia Islam is the state religion.

■ **Iran's claims on Bahrain.** Over the past 100 years, Iran has periodically voiced territorial claims over the Bahrain Islands, which were historically part of the Persian Empire, although direct rule only lasted for some thirty years in the 17th century. In 2007, an influential newspaper with close links to the Iranian regime published an editorial calling Bahrain "a province of Iran," which sparked considerable tension in the region.<sup>7</sup>

■ **Historical influence activities of Iran.** After the Iranian Revolution in 1971, Iran's government attempted to spread the Islamic revolution throughout the Muslim world. In 1981, Bahraini Shia fundamentalists orchestrated a coup attempt which – if successful – would have brought an Iran-based Shia cleric to power as the leader of an Islamic government.<sup>8</sup> The militant group behind the coup, the Islamic Front for the Liberation of Bahrain, was backed by Iran. The Bahraini government also blamed Iran for unrest in the mid-1990s. Iran has supported Shia militant groups in Bahrain, several of which were labelled terrorist groups by the US State Department.<sup>9</sup>

## KEY ACTORS

### Cabinet of Bahrain

**Al Wefaq** main opposition party of Bahrain

**Public Security Forces of Bahrain** reporting to Ministry of Interior

**Al Wasat** regarded as the only independent newspaper in Bahrain

**Gulf Cooperation Council** (Saudi Arabia, Kuwait, Qatar, UAE, Qatar, Oman)

**Hamad bin Isa Al Khalifa** King of Bahrain (since 2002), Emir of Bahrain (1999-2002)

**Khalifa bin Salman Al Khalifa** Prime Minister of Bahrain (since 1970)

**Sheikh Isa Ahmad Qassem** Bahrain's leading Shia cleric, seen as spiritual leader of Al Wefaq party with close ties to Iran

**Ayatollah Khamenei** Supreme Leader of Iran (since 1989)

## NARRATIVES

### Iranian government

■ It is Iran's duty to protect their fellow Shia in Bahrain from oppression and abuse that they suffer at the hands of the regime.

■ The GCC's interference in Bahrain's internal affairs is unacceptable and will further complicate matters.

### Bahraini government

■ The uprising is the result of a "fomented subversive plot against security and stability."<sup>10</sup>

■ The uprising has been provoked by external interference (i.e. Iran), and not by legitimate grievances of the population.

■ The demonstrators are Shia that have been agitated by Iran to overthrow the regime.

### Saudi Arabia / GCC

■ Iran is an expansionist power that is trying to extend its influence in the region.

■ The Kingdom will stand by the side of their Bahraini neighbours and protect them from Iranian interference.

## KEY EVENTS

14 Feb 2011	15 Feb	17 Feb	23 Feb	25 Feb	Mar	14 Mar	Apr	Jun
First day of protests in Bahrain (6,000 people); a man is killed by security forces.	A second person is killed; King gives speech reaffirming freedom of expression in Bahrain.	"Bloody Thursday," 4 deaths; protests grow larger.	Opposition leaders released from jail by royal pardon; first calls for the removal of the regime are heard.	Limited reshuffle of government cabinet.	Sectarian clashes occur, continue over next weeks; government imposes martial law; Iranian leaders express support for the protesters.	GCC troops arrive in Bahrain after invitation from government.	Government moves to ban two main Shia political parties.	King establishes the Bahrain Independent Commission of Inquiry.

## STRATEGIC LOGIC

It is reasonable to assume that the Iranian government was interested in the destabilisation of the Bahraini regime, given Iran's historical record of interfering with Bahrain's interior affairs (including backing militant Shia groups, and allegedly supporting a coup attempt in 1981). During the 2011 protests, Iranian officials and media criticised the Bahraini government's treatment of the Shia majority and voiced support for the protesters. In doing so, Iran

likely contributed towards the escalation of the peaceful demonstrations into violent sectarian clashes, and the framing of protests as a Sunni-Shia issue rather than a popular movement calling for political reform. This strategy appeals to subnational identities in detriment of the Bahraini national identity, which threatens societal cohesion.

## MEASURES

**DIPLOMATIC.** Public criticism of the Bahraini government's treatment of its Shia population, most prominently by Ayatollah Khamenei. 191 Iranian members of parliament issued a statement condemning the Bahraini government's crackdown on anti-regime protesters.<sup>11</sup> Iran recalled its ambassador to Bahrain due to the crackdown on the mostly Shia demonstrators,<sup>12</sup> and later expelled one Bahraini diplomat.

**MILITARY.** Threats to use force; e.g. a parliamentarian said that "Tehran will use all the power and potentials at its disposal to halt the oppression of the people of Bahrain."<sup>13</sup> In April 2011, the Iranian Foreign Minister sent

a letter to UN Secretary-General, asking for "serious and immediate action by the Security Council over suppressing people's demands in Bahrain using military force."<sup>14</sup>

**INFORMATION.** Use of Iranian Arabic-language satellite channels (especially Al-Alam, which is watched by 90 per cent of Bahraini Shia<sup>15</sup>) to spread their narrative. Al-Alam has been described as an Iranian tool of influence to stir up opinion in the Arab world.<sup>16</sup> Possibly use of social media to agitate protesters and escalate the uprising against the regime.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

■ In oil monarchies like Bahrain, national security is equivalent to regime security. Critical aspects include political stability, societal cohesion and national self-determination.

■ Bahrain's National Action Charter (2001) defines national security as "the fence and fortress for protection of the country and maintenance of its lands and economic, social, and political gains and support the process of comprehensive development."<sup>17</sup>

### VULNERABILITIES

■ A majority Shia population is ruled by a Sunni minority and discriminated against – for example, Shias are largely prevented from accessing jobs in the security services, they cannot serve in the armed forces, and their political influence is limited (e.g. gerrymandering of Shia constituencies by the government).<sup>18</sup> The resulting discontent is fertile ground for agitation and foreign influence.

■ Bahrain's economy is heavily oil-dependent.

### THREATS

■ Escalation of socio-political protests into sectarian violence, not least due to stirring up of discontent by Iran.

■ Risk of Bahrain becoming an arena for a proxy conflict between Saudi Arabia and Iran, who are both invested in the country.<sup>19</sup>

■ Growing threat of religious/ideological extremism, not least due to what Bahrain's Interior Minister called "anti-Bahrain propaganda by Iran-backed media."<sup>20</sup>

### EFFECTS

■ Increased divisions of society along sectarian lines, escalation of violence.

■ Reinforcement of opposition movements.

■ Weakened support for the government due to the perception of the Bahrain regime as oppressive.

■ Increased reliance of Bahrain on its GCC neighbours for regime survival.

# PAKISTANI INVOLVEMENT IN YEMEN

## SUMMARY

In March 2015, the Kingdom of Saudi Arabia (KSA) initiated Decisive Storm, a multilateral operation to influence the civil war in Yemen. The KSA's initial claim that Pakistan, a key ally, had already "expressed desire" to participate in the operation, caused some embarrassment for Islamabad.<sup>1</sup> A formal request by the KSA for Pakistani fighter jets, ground troops and naval warships to join its campaign in Yemen led to a lengthy debate in the Pakistani parliament. The majority of the public opposed direct involvement in the conflict and was wary of Pakistani support being taken for granted by the KSA. Many commentators saw the intervention as a potentially disastrous and costly war. Ultimately, the Pakistani parliament voted unanimously to remain neutral in the conflict, which made it difficult for the government to provide anything more than symbolic support.

Pakistan's decision-making process was subject to intense lobbying from the KSA, Iran and also China. The KSA and Pakistan have long had a close reciprocal relationship, with the KSA generously providing aid to Pakistan in return for military assistance. Despite intense pressure by the KSA to participate in the intervention, Pakistan was wary of antagonising its powerful neighbour Iran by meddling in its sphere of interest – Iran is believed to back the Houthi rebels in Yemen. Moreover, in 2015 Pakistan had high hopes that Western sanctions on Iran would soon be lifted as a result of a US nuclear deal, making Iran's vast hydrocarbon reserves available to energy-starved Pakistan.<sup>2</sup> Some analysts also suggested that China, which has a great interest in peace and stability in the region due to its large-scale infrastructure projects, might also have had some major influence on Pakistan's decision: China's President Xi visited Pakistan during the period of decision-making to lobby for neutrality and a diplomatic resolution of the conflict, and to promise enormous investments in infrastructure and energy amounting to USD 46 billion over several years as part of the One Belt One Road initiative.<sup>3</sup>

Pakistan also had many domestic factors to consider: participation in what many believed to be a proxy war between the KSA and Iran would likely aggravate the Sunni/Shia divide both in the region and at home (20 per cent of Pakistan's population are Shia Muslims). A crucial consideration was the risk of overstressing the Pakistani military, which

was engaged in a large-scale counter-insurgency operation along the Afghan border and additionally committed at the border with India.

Nevertheless, there has since been some evidence of creeping military involvement by Pakistan in spite of the parliamentary no-vote: in early 2017, there were reports of a brigade being sent to the KSA to protect against Houthi incursions into KSA territory. In a significant shift, the Pakistani army announced in February 2018 that it was sending 1,000 troops to the KSA in advisory and training roles. Although this still amounts to only indirect involvement in Yemen, the lack of detail in public announcements and the bypassing of the Pakistani parliament led to some domestic backlash.<sup>4</sup>



IMAGE – Shutterstock

## KEY POINTS

- Pakistan tried to walk a diplomatic tightrope by choosing the absolute minimum level of involvement by eventually sending troops for 'border operations.' It thus hoped to please the KSA by being somewhat involved, but at the same time not to antagonise Iran by contributing more directly. Words and actions were intended to convey the presumed role for Pakistan as a regional mediator, rather than an active participant of the regional geopolitical conflict between Iran and the KSA.

- Actions to assist the KSA often occurred without accompanying public announcements, indicating a two-track policy: Pakistan's political policy is compatible with the parliamentary resolution and aims to appease Iran, China and its own population; the other track is a more pragmatic approach, which caters to the demands of realpolitik.<sup>5</sup>

- Some information fratricide resulted owing to the highly contradictory nature of the diametrically opposing demands that were placed on Pakistan. Instead of soothing the KSA and Iran, Pakistan's words and actions seem to have angered both to some extent.

## CONTEXT

- **Pakistani-KSA relations.** Pakistan and the KSA have a long-standing relationship, with Pakistan in some regards the junior partner due to its relative economic weakness and vulnerability. Pakistan is a major recipient of KSA aid and cheap oil. Pakistan possesses a far superior standing army with extensive operational experience and has developed a reputation for being the provider of military muscle to the KSA (e.g. in Gulf War 1991).

- **Pakistani-China relations.** China is the most important supporter of Pakistan's economy, with Chinese aid now exceeding US aid. China is significantly expanding its investments in Pakistani infrastructure

(including financing an Iran-Pakistan pipeline), with Pakistan representing a critical geographical point in China's 'One Belt One Road Initiative', an ambitious infrastructure project to create a new 'Silk Road'. Regional stability, including Yemen, is vital for the realisation of this project: the Yemen conflict threatens the Bab al-Mandeb Strait, a body of water controlled by Yemen and a chokepoint for the transportation of oil. President Xi visited Pakistan in April 2015 to discuss, amongst other topics, the possible role of Pakistan in the Yemen conflict and promised to stand behind Pakistan if it decided to rebuff the KSA's request. The personal intervention of the Chinese President signalled the importance of the issue to China.

## KEY ACTORS

**Parliament of Pakistan**  
**Ministry of Defence of Pakistan**

**Nawaz Sharif** *Prime Minister of Pakistan (1990 – 1993, 1997 – 1999, 2013 – 2017)*

**Khwaja Asif** *Defence Minister of Pakistan (2013 – 2017)*

**Khurram Dastgir Khan** *Defence Minister of Pakistan (2017 – 2018)*

**Xi Jinping** *President of China (since 2013)*

**Mohammad Javad Zarif** *Minister of Foreign Affairs of Iran (since 2013)*

**Prince Muhammad bin Salman** *Crown Prince of Saudi Arabia; Defence Minister (since 2015)*

## NARRATIVES

### KSA government

- This multilateral intervention will restore the legitimate government in Yemen and terminate the threat posed by Houthi rebels.
- Iran is inflaming the conflict by backing the Shia Houthi rebels.

### Iranian government

- Iran does not back the Houthi rebels.
- The KSA is committing genocide in Yemen.<sup>5</sup>
- Pakistan should assist in finding a diplomatic solution to the crisis.

### Chinese government

- Stability in the region is of great importance; military intervention in Yemen will destabilise the region.

### Pakistani government and media

- The parliament "desires that Pakistan should maintain neutrality in the Yemen conflict so as to be able to play a proactive diplomatic role to end the crisis."<sup>7</sup>
- Press/public (majority): this is not Pakistan's war, and Pakistan is not the KSA's puppet.<sup>8</sup>
- Government: Pakistan is prepared to protect the territorial integrity of the KSA.

## KEY EVENTS

25 Mar 2015	31 Mar	6 Apr	8 – 9 Apr	10 Apr	20 – 21 Apr	Dec 2016	15 Feb 2018
KSA-led military operations begin in Yemen.	Pakistan's Defence Minister visits KSA, promises to protect Saudi territory but states necessity to "give peace a chance". <sup>9</sup>	KSA Defence Minister announces KSA has formally asked Pakistan to join the coalition.	Iranian Foreign Minister visits Pakistan, asking the country to remain neutral and work towards a cease-fire.	Pakistan's parliament passes a resolution declaring neutrality on Yemen.	China's President Xi visits Pakistan, announces USD 46 billion investment.	Pakistani Chief of Army Staff visits KSA; following the visit, there are reports of a brigade of soldiers being sent to the KSA for 'guard' duty against possible incursions of Houthis into KSA.	Press release from Pakistani military announcing decision to send 1,000 troops to KSA in advisory and training roles.

## STRATEGIC LOGIC

While Iran's and China's wish for Pakistani non-intervention coincided with the preferences of the Pakistani public and most of its politicians, the KSA tried to influence Pakistan into joining an intervention that was, arguably, not in Pakistan's national interest. The intervention seemed likely to become a costly and drawn-out conflict in a region that Pakistan had

little connection to, and was likely to cause Pakistan problems at home (including increased sectarianism, public discontent, overstretching of the military). The KSA framed its offer as part of the long-existing mutually beneficial relationship and combined intense diplomatic pressure with the implicit threat of discontinuing their generous aid and assistance.

## MEASURES

**DIPLOMATIC.** Riyadh initially named Pakistan as a participant in the coalition before Pakistan had made any public statement on the matter.<sup>10</sup> The KSA's diplomatic pressure on Pakistan was intense, including shuttle diplomacy and high-level meetings.

**INFORMATION/FINANCIAL.** The KSA has gradually been building its influence at the level of the general Pakistani populace, most noticeably by funding hundreds of madrasas which provide children with housing, clothing and religious education.<sup>11</sup> However, the KSA's religious influence has also been blamed for raising sectarian tensions by spreading puritanical Wahhabi beliefs. Some pro-Saudi groups held rallies in Pakistan in support of the Yemen intervention.<sup>12</sup>

**ECONOMIC.** The KSA has long been a generous provider of aid and investment to Pakistan. In 2014 alone, the KSA gave Pakistan an "unconditional grant" of USD 1.5 billion to service its debts. In 2016, in return for Pakistan's participation in the KSA's multilateral exercise North Thunder – an attempt to stabilise bilateral relations – the KSA pledged USD 122 million, including a USD 67 million grant and the rest in loans for various development projects in Pakistan.<sup>13</sup> The KSA also provides jobs to 2.2 million Pakistani citizens, who send back some USD 4 – 5 billion in remittances back home every year.<sup>14,15</sup>

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Pakistan's sovereignty concerning its ability to freely choose its foreign policy path without external pressure.
- Harmonious coexistence between different ethnic and religious groups within Pakistan.
- Cordial relations with all the major regional powers.
- Energy security and functioning infrastructure for Pakistan's rapidly growing population.

### VULNERABILITIES

- Energy shortage: Pakistan's population is fast approaching 200 million, and its economy is losing up to six per cent of GDP due to infrastructure bottlenecks and a chronic shortage of electricity.<sup>16</sup>
- Oil dependence: The KSA is the primary source of oil for Pakistan.
- Weak economy: Huge debt and weak currency. Outside offers of aid and investment, likely tied to political demands, become more appealing.

### THREATS

- Worsening of inter-ethnic and inter-religious discord: the Yemen intervention can be explained as part of the broader Sunni/Shia conflict

embodied through KSA-Iranian rivalry; Pakistani involvement in Yemen would likely increase sectarian disputes at home, where 20 per cent of the population is Shia.

- Public discontent: Disconnect with the Pakistani government as a result of public opinion being ignored if geopolitical interests of external actors take precedence.

- Overstretching of the military: Pakistan is already heavily involved in counterinsurgency campaigns (esp. against Pakistani Taliban) and needs to keep enough troops at the Indian border. Involvement in Yemen would spread the military dangerously thin.

### EFFECTS

- Brief cooling of KSA-Pakistani relations after the initial decision to remain neutral, although relations have improved since Pakistan participated in a joint military exercise and deployed some troops to the KSA.

- Continued sectarian tensions, including ongoing attacks by Sunni supremacists on the Shia minority.

- Continued susceptibility to external influence, as no sustainable solution has been found to Pakistan's economic and energy-related vulnerabilities.

# OPERATION PARAKRAM

## SUMMARY

The India-Pakistan standoff from 2001 – 2002 was the biggest conflict between India and Pakistan since 1971. Operation Parakram (Sanskrit: 'Valour') was India's response to the terrorist threat it attributed to Pakistan and was an act of 'coercive diplomacy' – the use of military mobilisation as part of a diplomatic strategy. The operation was launched by New Delhi with the stated intent of compelling Pakistan to cease its support to violent extremists following two terrorist attacks in 2001, first on the legislative assembly in October and then the Indian parliament two months later. The Indian government attributed the attacks to two Pakistan-based terrorist organisations, Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM), and alleged these organisations were actively supported by Pakistan's Intelligence Service. New Delhi demanded that Pakistan tackle cross-border infiltration, close training camps and make a categorical and unambiguous renunciation of terrorism.

Under the Sundarji Doctrine, India mobilised its main strike forces from central India to complement the holding corps already in place on the border, but because of the distances involved and the size of the strike force, this took three weeks. As a result, Pakistan had enough time to counter-mobilise its own forces and allow for intermediary diplomacy, predominantly from the US and UK. By the time Indian troops had

arrived in the border region, the momentum was lost, and it was difficult for India to politically justify further military action, especially due to pressure from the US. Musharraf had made a live television address denouncing terrorism and promising to deal with militant groups in Pakistan.<sup>2,3</sup>

New Delhi's strategy meant influencing two key target audiences. First, demonstrating to Islamabad the capability of India's armed forces and the political will to act should Pakistan not comply with its demands. Second, by overtly threatening an escalation into conventional warfare, trying to influence the international community, particularly the US, to pressurise Pakistan to dissociate itself from Islamic terrorism in accordance with the global war on terror.

When measured against stated objectives, the operation was of mixed success. There was a reduction in cross-border infiltration in early 2002, Islamabad pledged to deny Kashmir to terrorist organisations and also temporarily cracked down on terrorist groups in Pakistan.<sup>4,5</sup> However, Pakistan did not comply with India's request to extradite twenty criminals, and the actions taken by Islamabad to crack down on militants and their cross-border activity were very short-lived.<sup>6</sup>

## KEY POINTS

- Coercive diplomacy is a type of strategic coercion, an approach which forces the target to take a particular action or to stop or undo an action already taken.<sup>7</sup> To compel an adversary to behave in a certain way, a government needs to coordinate actions and words into a credible, coherent message. This is complicated, however, by the requirement to speak simultaneously to different audiences: the adversary, the international community and domestic publics.

- The lack of political direction in defining strategic objectives was likely a significant factor in the operation's failures. Without clear aims, there was no way a military objective could be realised, and the military leadership were unable to organise and maintain military means.<sup>8,9</sup> A lack of information sharing and cooperation between civilian and military authorities compounded this.

- Because no end date was specified for Pakistan to comply with demands, the Indian government needed to coordinate military and diplomatic instruments over a protracted length of time, while concurrently signalling restraint to the US and sustaining domestic support for the operation.<sup>10</sup>

- The decisiveness of India's message was undercut by the inability of the Indian Armed Forces to present a credible and timely threat. After the order for mobilisation was given, the Indian Armed Forces took almost three weeks to move to the border area. During these three weeks, the Armed Forces of Pakistan were able to respond by counter-mobilising and using diplomacy to engage with allies.<sup>11</sup>

## CONTEXT

- **Indo-Pakistani rivalry.** India and Pakistan, sharing a 2,900 km long border, have been rivals since 1947 when both nations became independent states. The two countries have a long history of difficult relations and have fought in several conflicts and wars over the disputed territory of Kashmir and in 1971 over East Pakistan (now Bangladesh).<sup>12</sup> From 1947 on, both governments have claimed the region of Kashmir as sovereign territory, leading to several disputes and major military conflicts between 1947 and 1971. From the early 1970s up until 1998, India and Pakistan enjoyed a period of relative stability.<sup>13</sup> The situation was complicated again by Pakistan and India both testing nuclear weapons in 1998.<sup>14</sup>

- **Terror attacks.** In October 2001, a massive car bomb was detonated outside the Kashmir Legislative Assembly in Srinagar, killing 29 people. The Indian government blamed Islamabad.<sup>15</sup> Two months later five Islamic

terrorists attacked the Indian Parliament targeting political leaders; this failed, but several innocent people were killed.<sup>16</sup> This second attack was seen as a strike at the heart of India's democracy. New Delhi implicated Pakistani-based terrorist groups LeT and JeM in both attacks.<sup>17,18</sup>

- **The Sundarji Doctrine.** Indian's approach to defence policy towards Pakistan which it employed 1981 – 2004 was described as "a nonaggressive, non-provocative defence policy based on the philosophy of defensive defence."<sup>19</sup> According to the Sundarji Doctrine, India held seven defensive holding corps near the border region with Pakistan with limited offensive capability. Offensive combat power was provided by three strike corps based in central India, a significant distance from the border region.

## KEY ACTORS

**Lashkar-e-Taiba (LeT)** ("Army of the Pure") a violent Islamist Sunni organisation operating in Pakistan and Kashmir

**Jaish-e-Mohammed (JeM)** ("Army of Muhammad") a violent Islamist Sunni organisation operating in Pakistan and Kashmir

**Pervez Musharraf** President of Pakistan (2001-2008)

**Abdul Sattar** Foreign Minister of Pakistan (1999-2002)

**Lal Krishna Advani** Indian Minister of Home Affairs (1998-2004)

**Atal Bihari Vajpayee** Prime Minister of India (1998-2004)

**George Fernandes** Indian Defence Minister (2001-2004)

# NARRATIVES

## Indian government

- Pakistan and terrorist organisations are behind the terrorist attacks.<sup>20</sup>
- Pakistan is a revisionist and aggressive country.
- India has significant military capability which it is willing to use.
- India does not want war, but war is being thrust upon us.<sup>21</sup> The fight this time must be the final war against terrorism.<sup>22,23</sup>

## Pakistani government

- Pakistan is not a terrorist country; it is fighting against Islamist terrorism (e.g. Taliban, Al-Qaeda) and banned terrorist organisations in its own country (e.g. LeT).
- India is a nationalist and expansionist country, which tries to subdue Pakistan. Pakistan is fully prepared and capable of defeating all challenges.<sup>24</sup>
- Pakistan does not want war, local or general, conventional or nuclear; the decision lies with India.<sup>25</sup>

# KEY EVENTS

1 Oct 2001	13 Dec 2001	14 Dec 2001	Late Dec 2001	12 Jan 2002	14 May 2002	24 May 2002	10 Jun 2002	Oct 2003	Nov 2003
Car bomb attack against Kashmir Legislative Assembly by Islamist terrorist groups.	5 terrorists attack the Indian Parliament, 14 people (including attackers) are killed.	New Delhi demands Islamabad stop terrorist activities; Pakistan orders Armed Forces to standing high alert; Operation Parakram starts.	Indian and Pakistani ballistic missiles moved to LoC; mortar and artillery fire are placed in Kashmir.	Musharraf makes nationwide address denouncing terrorism and promising action on militant groups.	Three gunmen kill 34 people in an army camp near Jammu, escalating tensions.	Pakistan launches series of missile tests.	Air restrictions over India end; both countries withdraw warships.	India and Pakistan start to demobilise; Operation Parakram ends.	Ceasefire between India and Pakistan signed.

# STRATEGIC LOGIC

India launched Operation Parakram in response to a series of terrorist attacks and as a strategy of coercive diplomacy to influence political decision making in Islamabad. India wanted to demonstrate military capability and

political will, and compel Pakistan to comply with their demand to take 'credible, firm, substantive and visible actions' against violent militants operating from territory under its control.<sup>26</sup>

# MEASURES

**DIPLOMATIC.** New Delhi cut India's diplomatic representation in Pakistan by half and recalled its High Commissioner to Pakistan. India demanded that Islamabad should stop supporting terrorist and radical groups in Pakistan and in Pakistan Occupied Kashmir (POK). The government worked with the US to persuade Pakistan to prevent cross-border terrorism.<sup>27</sup> The US and UK, who relied on bases located in Pakistan for their military operations against the Taliban and Al-Qaeda in Afghanistan, advised New Delhi to exercise restraint. Operation Parakram was problematic because Islamabad redeployed force elements from Afghanistan's border in the west to India's border in the east.<sup>28</sup>

**ECONOMIC.** India stopped all border transit between Pakistan and India and denied airspace to Pakistan International Airlines.

**MILITARY.** By January 2002, India had mobilised approximately 500,000 troops and three armoured divisions in Kashmir along the Pakistani border. In response, Islamabad deployed over 300,000 troops along the Line of Control (LoC). By May 2002, the number of Indian military and paramilitary forces deployed along the Indo-Pakistani border had grown to around 700,000 troops.<sup>29</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

■ Territorial unity, stability of the border region with India. Support for the right of self-determination of the people of Kashmir.

■ Aim of achieving parity with India through military and diplomatic means, and limiting what Islamabad perceives as New Delhi's expansionist policy in the South Asia region.

■ Continued partnership with and assistance from key international partners (especially US).

## VULNERABILITIES

■ Fear of separatism; lack of national unity among several provinces (Sindh, Punjab, Baluchistan, and Northwest Frontier);<sup>30</sup> territorial disputes with Afghanistan.<sup>31</sup>

■ Elements of Pakistan society, in particular, those from poor socio-economic backgrounds, are vulnerable to violent extremist ideology.<sup>32</sup>

■ The military dominates Pakistan's strategic thinking because of the army's continuous role in government.

■ Cross-LoC trade is highly dependent on India-Pakistan relations, which are fragile.<sup>33</sup> The two most significant issues for Indian and Pakistan economic relations are terrorism and drug trafficking.<sup>34</sup>

■ Dependence on allies and partners, especially on the US, who provides economic and military support to Islamabad.<sup>35</sup>

## THREATS

■ Huge military build-up. Possibility of escalation into a full-scale conventional or even nuclear war. Existential threat: Islamabad feared that India could cut Pakistan in two in a full-scale war.<sup>36</sup>

■ India's growing economy is much larger and stronger than that of Pakistan.<sup>37,38</sup> Strengthening of India's status as a major power in the South Asian region.

■ Asymmetric Pakistan-India power relationship.<sup>39,40</sup> India has significantly more active military personnel (as of 2017, India has 2,800,000; versus Pakistan's 637,000) and reservists, and vastly outspends Pakistan (India's defence budget is USD 51 billion, while Pakistan's is USD 7 billion).<sup>41</sup>

## EFFECTS

■ Enormous cost of Operation Parakram, without major visible results: India spent at least USD 3.2 billion, while the response cost Pakistan USD 1.4 billion.<sup>42</sup> The Indian army had suffered 798 casualties by July 2003.

■ India's aims were not achieved: Pakistan continued supporting radical Islamist movements in Kashmir in the long run, despite public assurances and short-lived crack-downs.

■ Operation Parakram revealed several vulnerabilities of Indian military strategy and Indian Armed Forces, and showed that the Sundarji Doctrine was not fit for purpose.<sup>43</sup> In response, India developed a strategy to deal with insurgent camps in POK should terrorist attacks occur, which avoids escalating to war while maintaining a no first use (NFU) nuclear posture.<sup>44</sup> A new doctrine was developed that focused on ensuring a surprise, rapid mobilisation against Pakistan and keep the conflict limited; India's traditional defensive posture became more pro-active in 2004.<sup>45</sup> New Delhi also updated its intelligence and defence networks and built up border controls on the LoC.<sup>46</sup>

# SNAP EXERCISES AND CRIMEA

## SUMMARY

On 26 February 2014, President Putin ordered a week-long readiness exercise in the Western and Central Military Districts, involving around 150,000 troops and coinciding with the deployment of covert Russian force elements before the annexation of Crimea. Although Russian officials maintained that the readiness exercise had been planned months in advance and was unconnected to events in Ukraine, its timing, scope and the accompanying rhetoric which emphasised its size, should be seen as a threatening message in the context of growing Russian-Ukrainian tensions.<sup>1</sup> Along with other measures, this exercise was part of a strategy intended to achieve effects on three target audiences: intimidating the interim government in Kiev and deterring it from entering into open conflict in Crimea, dissuading third parties from intervening in the conflict, and providing reassurance and encouragement to pro-Russian actors in Crimea (and later Eastern Ukraine). In addition to signalling deterrence and political resolve, the exercise also served as a deception to divert attention away from Crimea: a distraction force was deployed near Ukrainian borders in the Western Military District, while the Southern Military District, closest to Crimea, was not involved in the exercise.<sup>2</sup> While the majority of troops indeed conducted regular exercises, a small element of the force was being mobilised for the annexation of Crimea.<sup>3</sup>

Similar exercises also took place later during the continuing conflict in Eastern Ukraine, where Russia began a mass deployment of forces near the Ukrainian-Russian border.<sup>4</sup> A pattern of snap exercises has

been discernible in other regions, such as in close vicinity to Estonia, Latvia and Lithuania, where the timing of force posture has been used for strategic effect. The message of these exercises can be considered quite clear in the sense of Russia demonstrating its readiness for confrontation and deterring further actions against Russia's interests in an area which it considers its sphere of influence.



The military exercises involved the Western and Central military districts.

The Southern military district, closer to Ukraine's pro-Russian Crimean Peninsula, was not involved.

The Russian Navy has a major presence in the Crimean port of Sevastopol, it was not involved in the exercises.

Russia's readiness exercise from 26 February – 3 March 2014. Image – own elaboration based on Laris Karklis/The Washington Post

## KEY POINTS

■ A key advantage of the use of snap exercises is their ambiguity: if accused of hidden and hostile motives, Russia can claim that every army needs to exercise their troops regularly.<sup>5</sup> This plausible deniability during a critical time period can seriously hamper the decision-making of affected governments and of international organisations. It took time for NATO to understand the size and scale of Russian troops deploying to Crimea while the Russians continuously denied their presence.<sup>6</sup>

■ Russia's desire to achieve a political effect through military posture was clear: if the Russian government had wanted to de-escalate tension, a pre-planned exercise would likely have been cancelled to avoid any misinterpretation.<sup>7</sup>

■ Russia used a strategy of 'pressure and shield': fomenting public unrest and encouraging local militia to create an indigenous insurgency – undermining government authority from within – then shielding them by deploying significant forces close to the border, deterring the Ukrainian government from risking open confrontation.

■ The integration and synchronisation of a range of measures to create confusion and deceive an enemy is a classic example of Russian military deception, often referred to as *maskirovka*, which according to doctrine consists of concealment, simulation and imitation, disinformation and demonstrations of military capability.<sup>8</sup>

## CONTEXT

■ **Unrest in Ukraine.** Pro-EU protests began in November 2014, after President Yanukovich's decision not to sign an Association Agreement with the European Union. In the following months, protests escalated and turned violent after the government passed harsh anti-protest laws and imprisoned hundreds of protesters. From 18 – 20 February 2014, at least 88 people were killed in Kiev by security forces. In February, the Ukrainian parliament impeached President Yanukovich and installed an interim government under President Turchynov. In response, thousands of pro-Russian protesters rallied in Crimea against the new administration, the legitimacy of which was also challenged by Russian officials. 60 per cent of Crimea's population is ethnic Russian, and Russia's Black Sea Fleet has been stationed in Sevastopol for centuries.

■ **Annexation of Crimea.** On 27 and 28 February, unmarked armed men seized key government buildings in Crimea and two key airports in

Simferopol and Sevastopol. On 1 March, the Russian parliament approved Putin's request to use military force in Ukraine. On 6 March, Crimea's parliament voted unanimously in favour of joining the Russian Federation.

■ **Vienna Document.** The Vienna Document<sup>9</sup> is a Confidence and Security-Building Measure (CSBM) agreed upon with the OSCE in 1990, which requires participating states (amongst other things) to notify each other ahead of time about major military activities such as exercises. As the troops involved had not been given notice in advance of the exercises, the 42-day notification required by the Vienna Document did not apply. Russia did not invite observers as the troops involved in each exercise scenario did not exceed the number required under Chapter VI, but three inspections were carried out under Chapter IX which covers arms control. No infringements were found.<sup>10</sup>

## KEY ACTORS

Russian Armed Forces  
Ukrainian Government  
Crimean Parliament

Vladimir Putin President and Supreme Commander in Chief of the Russian Federation (2000 – 2008, since 2012)

Sergey Shoigu Russian Defence Minister (since 2012)

Sergei Lavrov Russian Foreign Minister (since 2004)

Arseniy Yatsenyuk Prime Minister of Ukraine (2014 – 2016)

Sergey Aksyonov new "separatist" Prime Minister of the Autonomous Republic of Crimea (since 2014)



# NARRATIVES

## Russian government

- Exercises of this scale are not unusual and are frequently ordered by the President.
- This readiness exercise was previously planned and is not linked to events in Ukraine.<sup>11</sup>
- The drills will include military exercises “on Russia’s borders with other countries, including Ukraine.”<sup>12</sup>
- Russia is closely following events in Ukraine and is taking (unspecified) measures to ensure the security of the Black Sea Fleet based in Crimea. Crimea has strong historical ties to Russia. Russia needs to protect the rights of ethnic Russians in Crimea from the new “fascist” government.

## Ukrainian government

- Everything is being done to avoid increasing tension in Crimea; security forces have received instructions to not at any cost provoke any conflict or confrontation with civilians.
- Ukraine will not use force and provoke bloodshed.<sup>13</sup> Russia’s statements regarding the infringement of civil rights of national minorities and religious denominations are false.
- The irregular presence of Russian troops in Crimea is a violation of the agreement regarding the Black Sea Fleet; the Russian government must immediately withdraw these troops and return them to places of permanent deployment.

# KEY EVENTS



# STRATEGIC LOGIC

The snap exercise featured in this case was presented as a readiness test of the armed forces but was, in reality, part of a strategy of classic Russian military deception with the intent of achieving several effects. First, demonstrating political and military resolve toward the new Ukrainian government and to the West. Second, encouraging pro-Russian elements in Ukraine. Finally, by holding the exercises in the Central and Western Military Districts, rather than the Southern Military District which bordered Crimea, Russia was able to create a distraction while mobilising

special forces for the invasion of Crimea.<sup>15</sup> Ambiguity and plausible deniability were crucial elements of the operation to annex Crimea, including the use of unidentified armed personnel which were in actuality Russian special forces. The use of military posture and the employment of additional non-military instruments to influence Ukrainian decision-making meant Russia only needed to employ a low level of actual force, ultimately succeeding in annexing Crimea with a minimum of effort and cost.<sup>16</sup>

# MEASURES

**DIPLOMATIC.** Russian political representatives (President, Foreign Minister, Defence Minister) played with demonstrating the readiness of large military forces while denying any intention to use it as an element of policy.

**MILITARY.** The readiness exercise demonstrated the Russian armed forces’ ability to put substantial combat forces on high alert status in a short time and showed its ability to act militarily with extremely short

warning time for other actors. Russia also used the exercise as a cover for irregular troop movements: by April 2014, Russia had built up over 40,000 troops at the Ukrainian border as part of the same readiness exercise, which also served to covertly shift selected units towards Crimea.<sup>17</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

Ukraine’s national security strategy of 2007 (updated in 2012)<sup>18</sup> lists the following among its national interests:

- “Enhancement of constitutional rights and freedoms of people and citizens;”
- “Protection of state sovereignty, territorial integrity, and inviolability of borders;”
- “Setting up competitive, social market economy and improvement of social welfare;”
- “Providing safe living conditions [...]”
- “Protection and development of spiritual and cultural values of Ukrainian society and reinforcement of its identity on the principles of ethnic and cultural diversity.”

## VULNERABILITIES

- Historically-based segmentation of society with divergent cultural identities and broad political affiliations.
- Military non-alignment. Mere partnership with NATO does not provide any guarantee of military help in case of an armed attack.
- Extensive trade and energy dependency on Russia.
- Poor governance. Underdeveloped democratic institutions, tradition of clientelism between political scene, government and business; critical lack of transparency and accountability of political leadership and state administration.

## THREATS

- The Ukrainian government understood the large-scale readiness exercise right along the Ukrainian border as an immediate threat of incursion. Risk of fully-fledged open conflict with an adversary with far superior capability and readiness.
- Threat of territorial loss and severe destabilisation of the country.
- Strengthening of assertiveness of protesters and fighters with pro-Russian and separatist sentiments due to the belief of Russian support.
- Threat of losing national and international legitimacy by seeming to over-react to ambiguous situations (such as formally identified fighters); difficulty of finding an acceptable course of action at any given time.

## EFFECTS

- Russia’s military posturing placed enormous pressure on Ukraine’s political leadership and had a most critical impact on national decision-making: it prevented the government from taking any direct military action against unidentified armed men capturing strategic points in Crimea.
- Territorial integrity of Ukraine was violated to a very high degree – change of state borders through annexation of territory.
- Grave violation of international law without a prospect of an effective remedial action by the international community in the near future.

# ELECTRONIC WARFARE DURING ZAPAD 2017

## SUMMARY

Zapad 2017 was a joint strategic exercise between the Russian and Belarusian Armed Forces. Two weeks before the exercise started, a western district of Latvia experienced a major cellular network outage that lasted for seven hours. The outage was believed to be a result of a mobile communications jammer from Kaliningrad or a warship in the Baltic Sea aimed at Sweden's Öland island, but also affecting the Latvian coastal region.<sup>1</sup> A few days later, commercial aircraft flying over Norway's Eastern Finnmark reported a complete loss of GPS signal, which lasted for a week. This GPS disruption meant that aircraft had to use alternative means to navigate. Various measurements showed that the interference was coming from the Russian border region in the east.<sup>2</sup> The day before the official start of Zapad, Latvia's '112' emergency phone service was unavailable for 16 hours. Media and government officials were quick to suggest Russian involvement, but the Interior Ministry later stated that this was actually due to a malfunction and not outside interference.<sup>3</sup> The cellular network outage in Latvia and the GPS disruption in Norway were linked to Zapad, during which the Russian Armed Forces tested the deployment and application of advanced Electronic Warfare (EW) technology. The exercise was conducted in a largely EW-hostile environment, assessed to reflect the conditions for which they needed to prepare should conflict arise with NATO.<sup>4</sup> Disruptions in Latvia's and Norway's communications systems were likely side-effects of the Russian Armed Forces jamming the systems of their own troops near the border. Officials from both Norway and Latvia commented on these occurrences, although both stressed that there was no evidence yet

and that nothing pointed towards a deliberate attack. However, Latvia's Foreign Minister called the incident "a symbolic political gesture against the Baltic States, which showed that Russia was doing everything to intimidate NATO," and hypothesised about Article V being invoked in more serious EW attacks in the future.<sup>5</sup> The NATO Secretary General also addressed the issue a few weeks later, underlining the need for transparency in military exercises.

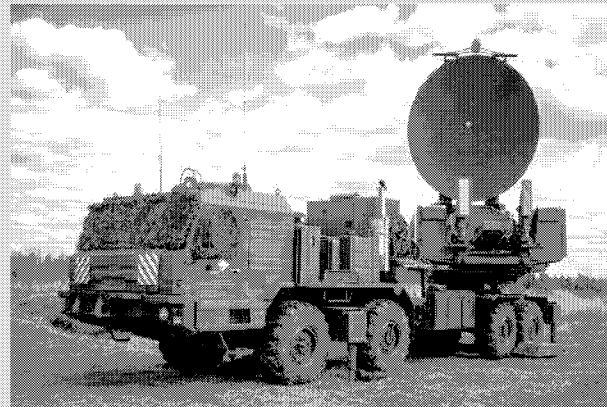


IMAGE – Russian Krasukha-2 EW system / Mil.ru

## KEY POINTS

- The ambiguous nature of the jamming and the length of time it took to determine the source of the disruption with a high degree of certainty impeded the ability to attribute responsibility and respond in a timely and decisive manner.
- Russia embarked on a programme of EW modernisation in 2009 and has deployed EW against Ukrainian government forces, in support of kinetic targeting, to jam communications and degrade morale through direct text messages.<sup>6</sup> Russia's holistic military thinking means that EW capability will continue to be exploited and effects created well beyond the realm of traditional EW thinking. This convergence of Russia's EW, cyber and information warfare approaches, will continue to challenge existing NATO concepts and practices.<sup>7</sup>
- Electronic Attack (EA) integrates with other measures to achieve psychological effects, either by the deliberate targeting of communication networks or by the footprint causing 'collateral damage'. Apart from the

physical disruption to basic social functions and services, disruption of critical infrastructure through EA can cause uncertainty and create public anxiety.

- Military observers widely expected testing of EW technology in Zapad 2017, so potential spill-over into border regions could have been anticipated. Preparation for such incidents should focus on credible, factual responses consistent across national authorities, stressing civil preparedness such as redundancy in national communications systems.
- The incorrect attribution of responsibility for the outage of the 112 emergency phoneline highlights the risk of threat inflation and the importance of national authorities maintaining a high level of situational awareness, being able to establish the facts and communicate them to the public promptly.

## CONTEXT

■ **Zapad 2017.** Zapad ('West') is a series of military manoeuvres that the Russian armed forces conduct with Belarus every four years. The Kremlin insists that the scenario is purely defensive and in the run-up to Zapad 2017, Moscow accused Western officials and commentators of vastly exaggerating the scale of the exercise. Evidence indicates that the exercise kept to the size originally announced, which allowed the Kremlin to claim that the 'Russophobic' West had overreacted.<sup>8</sup> Baltic politicians in particular described the drills as an aggressive show of force.<sup>9</sup>

■ **Electronic Warfare (EW).** EW describes the use of the electromagnetic spectrum (EMS) for defensive or offensive purposes. Russia's EW capability forms a key part of its conventional armed forces as a combat support asset. Russia sees EW as a seamless whole, ranging from kinetic combat operations to cyber and psychological operations.<sup>10</sup> Russia's view on the line between war and peace is much less clearly defined than that of Western countries, leaving a lot of grey area and possibilities for hybrid measures such as ambiguous EMS activities.<sup>11</sup> There have been many reports of Russia testing and using new EW capabilities in Crimea, Eastern Ukraine and Syria. Zapad 2017 provided a good opportunity for Russian troops to gather information about how its EW systems performed against countries with more advanced communications networks.<sup>12</sup>

## KEY ACTORS

**Latvian Ministry of the Interior**  
**National Security Committee of the Latvian Parliament**  
**Norwegian Intelligence Service**  
**Norwegian National Communications Authority**

**Russian Ministry of Defence**  
**Edgars Rinkēvičs** *Latvian Minister for Foreign Affairs (since 2011)*  
**Frank Bakke-Jensen** *Norwegian Minister of Defense (since 2017)*  
**General-Major Yuriy Lastochkin** *Chief of Russian EW Troops (since 2014)*  
**Jens Stoltenberg** *NATO Secretary General (since 2014)*

## NARRATIVES

### Latvian government

- Zapad 2017 is an aggressive demonstration of force.
- Disruptions in communications seem to be connected to the exercise, although Latvia does not seem to have been intentionally targeted.
- Electronic attacks on national communications systems are an extremely serious matter.
- Latvia should not panic about Zapad 2017, because Latvia has increased funding for defence and the presence of allied forces in the Baltics.<sup>13</sup>

### Norwegian government

- It is not surprising that Russian jamming has affected the Norwegian side of the border.
- Alternative ways to navigate will protect against GPS jamming.
- Russia should have anticipated the side effects on civil aviation.

### NATO

- Utmost transparency regarding military exercises is required to make sure there are no misunderstandings.
- Russia has developed powerful EW capabilities, which have been on display in Syria and Ukraine.

### Russian government

- The improvement of EW systems is one of the most important elements in ensuring national security.
- EW is a complex intellectual and technical component, especially in hybrid conflicts.

## KEY EVENTS

2014	2015	Jun 2017	Jul – Aug 2017	30 Aug 2017	7 Sep 2017	13 Sep 2017	14-20 Sep 2017
GPS jamming and communications degradation are frequent in Eastern Ukraine.	Russian forces test and use EW technology in Syria, including jamming of US drones.	Over 20 merchant ships are subjected to a suspected GPS spoofing attack in the Black Sea.	Russian Armed Forces conduct 5 major exercises that together assemble over 1,100 pieces of EW equipment.	Western Latvia experiences a major cellular network outage for 7 hours.	Commercial aircraft flying over Eastern Finnmark in Norway report a complete loss of GPS signal due to electronic jamming; disruptions last for about a week.	Latvia's emergency telephone hotline 112 is out for 16 hours (later turns out to be unrelated incident).	Official dates of Zapad 2017 military exercise, although senior NATO diplomats say military activity intensified weeks before the official start date.

## STRATEGIC LOGIC

The Russian Federation's build-up of EW capabilities is part of an asymmetric strategy and a cost-effective, low-risk way of disrupting a technologically superior adversary. Electronic attacks can be highly disruptive to civilian and military systems, while at the same time providing a surprising amount of plausible deniability – during Zapad 2017 the national intelligence services had difficulties identifying the source of the jamming and whether it was deliberate.<sup>14</sup> Similar to cyber attacks, EW attacks that affect civilian systems create media attention, which can have a significant psychological effect and contribute to public anxiety. It is not clear if Russia intended to disrupt civilian communications deliberately, but it is almost certain that they were responsible. The lack of control measures to prevent spill-over of signals was at the very least negligent, and the absence of any public acknowledgment of responsibility in itself should be seen as hostile.

## MEASURES

**DIPLOMATIC.** No warning or subsequent public clarification of the EW-related incidents, which contributed to uncertainty. No comment was made on the jamming allegations during Zapad 2017.

**MILITARY.** Testing of growing EW capabilities during Zapad 2017. Jamming of GPS signals in Norway's Eastern Finnmark, but also all the way to the west to Alta airport (some 250 km west of the Russian border) for a week. Attributed to unintentional side-effects of EW-related activities aimed at Russia's own troops. Jamming of phone services in Latvia's Kurzeme district for seven hours also attributed to spill-over from the Zapad exercise.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Resilience of civil communications systems (and related emergency networks).
- Safety of transportation systems, especially civilian traffic/aviation; this includes having alternative modes of navigating to GPS, which provides critical positioning capabilities to military and civilian users.
- The Latvian National Security Concept also mentions that an "element characterising the internal security [...] is the level of safety and stability the inhabitants feel in their daily life in the country."<sup>15</sup>

### VULNERABILITIES

- The US and other NATO states have neglected EW during the past few decades, allowing the Russian Armed Forces to gain both quantitative and qualitative EW superiority.<sup>16</sup> US and NATO rely heavily on powerful high-technology systems (e.g. long-range precision strike capabilities) which are vulnerable to electronic disruption.<sup>17</sup>
- While military units are generally able to deal with disruptions of the electromagnetic spectrum, civil society is much more vulnerable – for instance, for most people, cell phones are crucial in emergency situations.<sup>18</sup>

### THREATS

- Russia has the capability to severely disrupt civilian systems. Even if the jamming of civilian systems occurs as an unintentional spill-over effect, it carries many risks, including transportation accidents with potentially lethal results.<sup>19</sup> Knocking out cell phones also prevents authorities from quickly disseminating information to its citizens in crisis situations.<sup>20</sup>
- The ambiguous nature of the EW activity threatens to lead to more uncertainty and reduced confidence in sensors and networks.

### EFFECTS

- EW activity during Zapad did not cause any lasting damage in Norway or Latvia.
- The main effect was cognitive: the spill-over of a military capability into NATO countries' civilian systems played into the hyped-up attention around the Zapad exercise and drew attention to the considerable Russian EW capabilities.
- Debates on the safety of civilian communication and transportation systems.<sup>21</sup>

# RUSSIAN ESPIONAGE IN SWEDEN

## SUMMARY

In 2014, the Swedish Security Service (SÄPO) reported that the threat from Russia's intelligence activities was increasing, as part of a range of measures and as a precursor to possible military action.<sup>1</sup> The service cited ten countries as actively involved in systematic, unlawful activities against Sweden or Swedish interests abroad, predominantly through the use of undercover intelligence officers working out of embassies, trade representations and consulates. These officers worked under false pretences, posing as diplomats, journalists or people in business and recruiting agents to supply information. Russia was singled out as a particular risk, the only country with a 'full spectrum' approach, covering 'politics, economics, industry, technology, military defence and dissidents.'<sup>2</sup> SÄPO again warned in 2015 that Russia was operating spies both covertly and under diplomatic cover to collect information about Swedish defence, politics, economy, technology, and science. In 2016, it was suspected that Russia was trying to openly influence the Swedish debate on security policy through public rhetoric, and integrated such open statements with more covert activities, such as disinformation in the Swedish press, infiltration of think tank events, cyber attacks and espionage, particularly during the discussion of a Host Nation Support Agreement with NATO.<sup>3</sup>

Swedish government officials and intelligence agencies have become more outspoken about the threat from Russia, warning the population to be vigilant. The Armed Forces introduced a hotline for tips about suspicious activities during military exercises. Despite the increase in media reports of Russian spying and the flow of official statements citing suspicious events, details on specific incidents were not so

forthcoming, unsurprising given the political sensitivities surrounding accusations of espionage and the requirement for the security services to protect sources and methods. In addition, a number of media reports of incidents loosely blamed on Russia – submarine sightings, sabotage of communications towers and cyber attacks – filled the vacuum left by the lack of explicit evidence from national authorities but were never conclusively attributed to Russia, to which the Kremlin responded with accusations of 'Russophobic hysteria'.



Sputnik News making fun of the hunt for an alleged Russian submarine in the Swedish archipelago in 2014.

## KEY POINTS

- While there may be intense public interest in the counter-espionage and counter-subversion activities, security services often have to withhold certain information to prevent compromising operations. Protecting sources of information and the methods used in intelligence collection takes priority over transparency. There may also be legal restrictions in place.<sup>4</sup>
- This case highlights the challenge to national security institutions in keeping the public informed on matters of intelligence in a coherent and consistent manner. A distinction needs to be made between overall threat warnings and evidence that supports attribution on a case by case basis. Speculation beyond the known facts can create

unnecessary ambiguity, risking sensational media reporting and threat inflation, which in turn can affect government credibility. The Kremlin often fosters a domestic narrative that Sweden and the West are over-reacting to encourage popular support for the regime.

- The use of espionage to subvert a ruling authority should be seen in the context of Russia's 'new generation warfare'. Espionage is not just about gathering information, but also shaping events and influencing public opinion in the long term. Agents can pass false or misleading information to the media, and reporting on real or suspected espionage activities can undermine public trust in national authorities, building up the image of a militarily superior Russia.

## CONTEXT

■ **Espionage.** While intelligence activities – the gathering and processing of information – is not unlawful in itself, intelligence activities become unlawful when information is gathered that could harm a state's security if disclosed. SÄPO defines espionage as "seeking to obtain sensitive or classified information of vital importance to national security with the aim of passing this information to a foreign power."<sup>5</sup>

■ **Growing Russian assertiveness.** Under President Putin, Russian intelligence activities increased, and the Kremlin adapted Soviet espionage tactics and strategies against the West. This includes the practice of espionage, which is embedded as part of a comprehensive strategic toolbox employed by the Kremlin towards EU and NATO members. Espionage efforts are considered a key component of Russia's multi-domain deception and obfuscation strategy.

## KEY ACTORS

**Swedish Security Service (SÄPO)** government agency under the Ministry of Justice; responsible for counter-espionage

**Military Intelligence and Security Service (MUST)** main foreign intelligence agency, under Swedish Armed Forces Central Command

**Swedish Civil Contingencies Agency (MSB)** organised under MOD, responsible for issues concerning civil protection, public safety, emergency management, and civil defence

**Russian Federal Security Service (FSB)** primarily internal security, but also external activities

**Russian Main Intelligence Directorate (GRU)** primarily military intelligence

**Russian Foreign Intelligence Service (SVR)** mainly civilian affairs

**Stefan Lofven** Prime Minister of Sweden (since 2014)

**Peter Hultqvist** Minister of Defence, Sweden (since 2014)

**Daniel Stenling** Head of Counter-intelligence, SÄPO

**Anders Thornberg** Director-General, SÄPO (2012 – 2018)

# NARRATIVES

## Russian government

- Swedish government and media are being Russophobic, jumping to conclusions despite lack of evidence.
- Military responses to so-called submarine sightings are ridiculous; these over-reactions stem from “anti-Russian hysteria and propaganda.”
- Sweden’s mainstream media seems to have adopted a new mantra: whenever anything bad happens, blame it on Russia.

## Swedish government

- Russian intelligence activities against Sweden are nothing new; the authorities are well aware of overt and covert influence activities and are taking appropriate measures.<sup>6</sup>
- Espionage is a reality, and it is important to understand the different methods that are being used.<sup>7</sup>
- Sweden’s foreign and security policy builds on military non-alignment, cohesion in the EU and increased cooperation on a broad front.<sup>9</sup>

# KEY EVENTS

Oct 2014	May 2016	May 2016	Sep 2016	Jun 2017	Sep 2017
Suspected sighting of a submarine in Stockholm archipelago sets off a week-long submarine hunt. <sup>9</sup>	Two communications mast towers in Borås are sabotaged. Investigation inconclusive. <sup>10</sup>	Sweden expels Russian research plane because of concerns over surveillance capability. <sup>11</sup>	Several reports of suspicious activity in Northern Sweden, including contact with soldiers on social media and observation of exercises. <sup>12</sup> Not attributed.	Suspected Russian submarine sighting in Gävle port, turns out to be an imprint on the ocean bed. <sup>13</sup>	Reports of intelligence gathering during Swedish Aurora-17 military exercise. Not attributed. <sup>14</sup>

# STRATEGIC LOGIC

Russia is concerned about Swedish policies moving the country closer to NATO, fearing that this undermines Russia’s standing in the strategically important Baltic Sea region.<sup>15</sup> Russian espionage activities against Sweden have increased since 2014 and should, therefore, be seen as part of a broader Russian strategy that seeks to undermine and disrupt regional security.<sup>15</sup> Goals include: collecting information about civilian and military

installations, capabilities and tactics; collecting information on international security and defence cooperation arrangements; and obtaining information on sensitive military technology. Espionage can also send a message: extensive reporting based on speculation risks causing uncertainty and a decline of public trust in national authorities, and unnecessary over-reaction which is readily exploited by the Kremlin.

# MEASURES

**DIPLOMATIC.** Swedish intelligence estimates that a third of Russian diplomats posted at the Embassy in Stockholm are spies for Russian intelligence services operating under diplomatic immunity.<sup>17</sup> Russian officials have made public statements attempting to influence Swedish debates on security policy decisions: for instance, the Russian Embassy in Stockholm and the Russian MFA openly mocked Swedish government and military responses to reported submarine sightings in the Stockholm archipelago in October 2014.<sup>16</sup>

**INTELLIGENCE.** The most prominent (and publicly disclosed) examples of suspected espionage in Sweden include:

- Intelligence gathering on military exercises (e.g. reports of suspicious persons, vehicles<sup>19</sup> and UAS20 during the NATO-led BALTOPS exercise in July 2016,<sup>21</sup> International Bison Counter and Flygvapenövning in September 2016,<sup>22</sup> and during Aurora-17 in September 2017<sup>23</sup>);

- Placing of agents as legitimate figures in Swedish politics, academia and news media, and attempted recruitment of people already working in Swedish agencies;<sup>24</sup>

- Corporate espionage and illegal technology transfers, including infiltrating Swedish defence companies and other industries;<sup>25</sup> SÄPO has warned of the risks around outsourcing data storage to foreign private firms;<sup>26</sup>

- Cyber espionage aimed at gathering intelligence on Swedish systems and identifying vulnerabilities;<sup>27</sup>

- Mobilisation of local actors or agents to foment divisiveness and political factionalism or to carry out sabotage against critical infrastructure.

**LEGAL.** Russia uses legal instruments to weaken Swedish officials’ ability to expel Russian spies from Sweden (including tit-for-tat expulsions of diplomats).<sup>28</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Swedish defence capabilities, operational planning, and international collaborative frameworks.
- Ability of the government to share and handle classified information, and protect databases and records.
- Safeguarding critical research and development (R&D) and sensitive technology.
- Protecting public opinion and sentiments from disinformation; building societal resilience.

## VULNERABILITIES

- Partial dismantling of Sweden’s Cold War-era defence capabilities: resources for Swedish counter-intelligence work lagged behind the threat.
- Despite strong societal resilience against disinformation, pro-Russian actors can exploit arguments that resonate in a Swedish context (e.g. polarised debates on migration).

## THREATS

- Financial, physical, security-related, and reputational losses associated with enhanced espionage activities. Collection of sensitive information for hostile purposes, stealing of state and corporate secrets.
- Over-reporting on and conspiracy theories around suspected or alleged Russian espionage in Swedish media and social media can lead to uncertainty and loss of public trust in national defence systems.

## EFFECTS

- Heightened public awareness of foreign influence activities in Sweden.
- Increased resources and efforts devoted to counter-espionage (e.g. SÄPO is receiving an additional USD 80.3 million between 2016 and 2020 to enhance counter-espionage efforts).
- Increased willingness of the government to openly call out Russian espionage. The intelligence agencies MUST and SÄPO explicitly mention specific Russian intelligence activities and release relevant information and evidence.

# RELIGIOUS EXTREMISM IN THE NETHERLANDS

## SUMMARY

Salafi outreach, predominantly facilitated by Saudi Arabia through mosques, welfare and educational activities, has been taking place in the Netherlands since the 1980s. The issue of the influence of Saudi citizens, NGOs and authority figures in the promotion of anti-Western ideas came into sharp focus following the attacks of 9/11, raising questions about the flow of religious-ideological influence and financing from Saudi Arabia.<sup>1</sup> Despite public anxiety over the risk of home-grown jihadism, concern eventually subsided, as non-violent Salafism became the more dominant strand for the next decade.<sup>2</sup> In 2014, however, the Dutch Intelligence and Security Service (AIVD) warned that the extremist interpretation of Salafism was again on the rise. Instability in the Middle East and the declaration of the 'ISIS caliphate' was cited as a significant factor in this development.

In 2017, the AIVD stated it was closely monitoring the Salafi movement, concerned that its ideology was being used to "legitimise intolerance, anti-democratic activities and polarisation."<sup>3</sup> The risk to national security from Salafi currents of Islam includes violent extremism at the fringes, a lack of integration of Muslim immigrants and contention in

political and social discourse.<sup>4</sup> The Salafi movement in the Netherlands is particularly professional in its communications, so that much of the information about Islam available to the Dutch public – in particular online and through satellite television – reflects Salafi worldviews.<sup>5</sup> This helps to explain why Salafi ideas are so popular among young Dutch Muslims and converts.<sup>6</sup>

The Dutch government announced in 2018 it was "looking at ways to prevent money from foreign countries being used to buy undesirable influence over Dutch civil society organisations, including religious and ideological organisations," noting that "funding flows that abuse our liberties, originating from countries that lack freedom, must be limited as far as possible."<sup>7</sup> Ideas proposed included obliging organisations to disclose any finances, including donations.<sup>8</sup> A government list was subsequently leaked by the media with details of 30 Dutch Islamic organisations that had applied for, or received, funding from Gulf states in recent years – Kuwait and Saudi Arabia in particular – involving millions of euros.<sup>9</sup>

## KEY POINTS

- The Netherlands identifies any religious ideology as a concern when it threatens the democratic legal order. Even if no laws are broken, this can be threatened by individuals trying to achieve antidemocratic political aims by undemocratic means, such as through: violence; incitement of hatred and discrimination; systematic disruption and undermining of democratic institutions; rejection of state authority; imposition of an alternative legal system and clandestine efforts to influence democratic decision-making.<sup>10</sup>

- The Salafi movement in the Netherlands is only partially organised through Salafi mosques and charitable foundations and represented less formally through other mosques and alternative media channels. The security services assessed that "close contacts between sections of the movement here in the Netherlands and Salafist individuals and

structures in the Middle East potentially give those external players an (undesirable) level of influence over parts of the Dutch spectrum."<sup>11</sup>

- Interventions to counter the threat from aspects of Salafism must be specific and transparent: a perception that all of Islam is being framed as harmful, or that the government is moving against Muslims in general, will lead to further polarisation in society. The Dutch security services have said it is up to the Muslim community itself to temper the Salafi movement in the Netherlands. Too much external pressure only leads to a stronger movement, confirming the Salafi argument that Muslims are under attack and that they are justified in their preaching of hatred of Western civilisation.

## CONTEXT

- **Immigration and integration in the Netherlands.** The largest minority groups – from Turkey, Morocco, Indonesia and Suriname – all brought their version of Islam to the Netherlands. Roughly 5 per cent of the Dutch population (17 million people) is Muslim,<sup>12</sup> of which around 40,000 – 65,000 are Salafi.<sup>13</sup> In 2018 there were 27 Salafi mosques in the Netherlands (up from 13 in 2014).<sup>14</sup> Problems with the integration of Muslim immigrants, both Salafi and non-Salafi, led to a debate on the nature of multiculturalism and the essence of Dutch values. Much of the right-wing politics and right-wing extremism that has grown in the Netherlands over the last 20 years has been in response to the debate on immigration.<sup>15</sup>

- **Salafism as a spectrum.** Salafism is a collective term for various Orthodox Sunni currents in Islam, which attempt to practice a "purer" and more literalist version of Islam, and support the implementation of Islamic

law (sharia). Promotion of (non-violent) Salafism worldwide by various Gulf countries and Saudi Arabia, in particular, should be viewed within the larger religious-political power struggle in the Arab world for the true interpretation of Islam, most especially vis-à-vis Shia interpretations of Islam. There is no central authority over Salafism, which contains many different movements and splinter groups. Some analysts identify three different Salafi movements: apolitical, political and jihadist Salafism.<sup>16</sup> Each Salafi tradition comes with its own threats and effects on society.<sup>17</sup> Violent jihadis pose a domestic terrorist threat and send foreign fighters to warzones. Apolitical Salafis oppose integration into Dutch society, which leads to a greater polarisation between these Salafis and Dutch society. Political Salafis stand for an active Islamisation of the individual, the family and society. Even though they will use the democratic process from a pragmatic point of view, they still view democracy as a vastly inferior system.

## KEY ACTORS

**AIVD** Dutch General Intelligence and Security Service

**NCTV** Dutch National Coordinator for Security and Counterterrorism, falls within the responsibility of the Dutch Ministry of Justice and Security

**FIOD** Dutch Fiscal Intelligence and Investigation Service

**Dutch Ministry of Social Affairs and Employment** tracks undemocratic organisations in the Netherlands but does not release the information publicly

**Dutch Ministry of Foreign Affairs** receives information from Gulf States on which Dutch organisations are being funded via embassies, charities and NGOs

**WODC (Research and Documentation Centre)** tasked with mapping the extent of foreign mosque funding; under the Ministry of Justice and Security

**Council of Moroccan Mosques** has called on Dutch Islamic institutions to be open about their funding

# NARRATIVES

## Dutch government

- Salafi thought promotes undemocratic and intolerant messages; Salafi jihadism poses a threat to Dutch society.
- Debates over how to deal with the challenges of Salafism cause polarisation within Dutch society.

## Radical Dutch Salafis

- Repeatedly try to provoke a response from authorities, so that they can then claim to be the victims of a hostile Western society, and use that supposed hostility to justify their own anti-Western, anti-democratic stance.<sup>18</sup>

# KEY EVENTS

1940s – 80s	Aug 1988	Aug 2001	2 Nov 2004	2014	Jul 2016	2018	Apr 2018	Ongoing
Immigration influx from Indonesia and Suriname, guest workers arrive from Turkey and Morocco.	First two Islamic elementary schools start their school year.	32 Islamic elementary schools start their school year (6,000 students).	Theo van Gogh, a Dutch filmmaker who produced a critical film of Islam, is violently murdered by a Dutch-Moroccan Salafi; retaliatory violence includes vandalism of mosques.	Dutch authorities count 13 Salafi mosques and 50 Salafi preachers in NLD. <sup>19</sup>	After years of requests from parliament, the Dutch MFA confirms the existence of (but does not publish) a list of Islamic institutions receiving Gulf funding.	Dutch authorities count 27 Salafi mosques and 110 Salafi preachers in NLD. <sup>20</sup>	Dutch media publish confidential lists of Gulf payments to Dutch mosque organisations.	Over the last decade, groups of asylum seekers (esp. from MENA-region) come to NLD.

# STRATEGIC LOGIC

Several Gulf states, particularly Saudi Arabia and Kuwait, fund Islamic organisations and (non-jihadist) Salafism in the Netherlands, often through clerics and charitable organisations. While the nature of this 'religious soft power' is complex and has evolved over time,<sup>21</sup> the general approach is to promote a preferred version of Islam abroad while decreasing the outreach

of other interpretations of Islam. While it is highly unlikely that such religious outreach was ever intended to deliberately harm the Netherlands, it propagated ideas which were then interpreted by certain groups and individuals in a way which ran contrary to the democratic legal order of Dutch society.

# MEASURES

**FINANCIAL.** Gulf states, especially Saudi Arabia and Kuwait, have funded Islamic institutions in the Netherlands for years, including paying for the construction of mosques, publishing Korans, and financing the training of imams and Islamic meetings. Many Dutch preachers go to the Gulf for study trips and university. Secret lists emerged in 2018 giving details of Gulf funding, including Kuwaiti payments totalling nearly EUR 6 million, and one mosque in Dordrecht receiving USD 88,888 from Saudi Arabia.<sup>22</sup> A number of Salafi mosque foundations in the Netherlands are the result of missionary and funding activities carried out from Saudi Arabia. These foundations are financially and organisationally linked to Saudi NGOs (e.g. Muslim World League, and the International Organization for Relief, Welfare and Development), which in turn have close ties to the Saudi establishment. The mosque foundations are not very transparent regarding the origin and allocation of their finances, which has led to a number of AIVD investigations.<sup>23</sup>

Even though the government funds much of the Islamic educational system in the Netherlands, the AIVD found in 2002 that about 20 per cent of Islamic elementary schools received funding from, and were influenced by, Saudi foundations.<sup>24</sup>

**INFORMATION.** Media attention often focuses on controversial foreign preachers and other guest speakers at Dutch mosques. The Salafist movement uses a range of media and arranges courses and conferences with guest speakers.<sup>25</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Universal acceptance of democratic processes and values such as societal openness and tolerance; willingness to discuss all issues freely and without taboos.

- Societal unity, integration of minority groups into Dutch society.

## VULNERABILITIES

■ Due to the freedom of religion and separation of church and state (Article 6 of the Dutch constitution), actions against Salafi mosques and organisations are difficult. Faith-based organisations are immune to criminal prosecution in the Netherlands. It is only possible to prosecute imams and other individuals based on hate speech (which the government has done in the past).

■ The separation of church and state also prevents the Dutch government from creating a ban on foreign funding of religious organisations, as is the case in Austria.

## THREATS

- Spread of anti-integration sentiments among Salafi groups, growth of intolerance and anti-Western society sentiments.

■ Risk of indirect or direct involvement in radical Islamic violence,<sup>26</sup> and risk of violent jihadism and domestic terrorism stemming from returning foreign fighters (according to AIVD, around 250 jihadists have travelled to Iraq and Syria in recent years).<sup>27</sup>

■ Increased polarisation in Dutch society over immigration and integration issues, which may result in the growth of support for extreme right-wing movements.

## EFFECTS

■ The effects below are a result of the rapid spread of Salafism, to which Gulf funding contributed. A direct correlation between Gulf funding and the effects described is nearly impossible to pinpoint.

- Political polarisation over the topic of Islam/Salafism.

■ Growing polarisation also amongst different strands of Islam, occasionally even violent disputes.<sup>28</sup>

# CYBER ATTACKS ON ROK & US

## SUMMARY

Between 4–9 July 2009, a series of coordinated cyber attacks took place, affecting 27 government and commercial websites in the Republic of Korea (ROK) and the United States (US). The attacks were relatively unsophisticated and, at their worst, reduced functionality or rendered the website temporarily unavailable.<sup>1</sup> Tweaked versions of extant malware were used by the attackers to execute Distributed Denial of Service (DDoS) attacks to flood certain websites in the ROK and the US with data traffic and make them unavailable. This outcome was achieved by hijacking unsecure unpatched computers worldwide. The attack was directed at the websites of political, administrative, media and commercial organisations in the ROK and at political, entertainment and media websites in the US. The low impact and ready countering of the 2009 cyber attack meant that functionality was not compromised and the impact was more abstract: the attacks attracted a large amount of media attention and forced the ROK and US to react.

The ROK quickly attributed the attacks to the Democratic People's Republic of Korea (DPRK),<sup>2</sup> which has been developing Offensive Cyber Capabilities (OCC) since the 1990s as a way to overcome asymmetries in conventional warfare capabilities between the DPRK and its adversaries. The use of OCC is particularly advantageous for the DPRK as it is relatively cheap and easy to develop and because it

enables the DPRK to conduct low-level attacks against its highly networked adversaries with relative anonymity. Further, the DPRK's un-networked nature means it is not vulnerable to like-for-like attacks.<sup>3</sup>



IMAGE – SHUTTERSTOCK

## KEY POINTS

■ Due to the nature of the attack – the use of DDoS, the targeting of websites rather than operational systems, and the fact that the attacks were not aimed at gathering intelligence – it is assessed that the cyber attacks were aimed at causing disruption, making a statement of capability or intent, and/or testing for international reaction to cyber attacks.

■ Due to the difficulties in providing concrete evidence for effective attribution, the options available to the ROK and the US to respond to the attacks were extremely limited.<sup>4</sup>

■ The attack highlighted the importance of consistent messaging: ROK and US had differing narratives in terms of attribution and

displayed different levels of reaction. ROK officials quickly blamed the DPRK. US officials initially declined to speculate about the attackers' identity, and in 2010 claimed they had "largely ruled out" the DPRK; however, in 2011 experts concluded that clues in the coding pointed to the DPRK.<sup>5</sup>

■ Disruption, even if only minor, can have larger effects if it causes widespread confusion or panic. Communication strategies need to be included in civil contingency plans to calm the population and distribute essential information immediately to mitigate the spread of rumours and disinformation.<sup>6</sup>

## CONTEXT

**Distributed Denial of Service (DDoS).** DDoS attacks occur when multiple hacked and compromised computer systems flood the target websites or servers with access requests. The mass of incoming messages and connection requests cause the target system to slow down or even crash and shut down and therefore lead to a denial of service for any legitimate users of the targeted resource. DDoS attacks offer a

relatively low-intensity method which has a high degree of deniability and low likelihood of retaliation or escalation.<sup>7</sup> This is because at first iteration, the infected computers which form the network of bots committing the DDoS attacks, are owned by innocent and unwitting individuals with no connection to the culprits. The culprits are also able to further hide their identity by changing the language used in their code, among other tactics.

## KEY ACTORS

**DPRK Reconnaissance General Bureau** believed to lead cyber activities, complementing its responsibility for other provocative and asymmetric activities<sup>8</sup>

**DPRK General Staff Department of the Korean People's Army** leads on more traditional cyber command<sup>9</sup>

**ROK National Intelligence Service** responsible for investigating the cyber attack<sup>10</sup>

**ROK Ministry of Defence** increased funding for the security of its computer system after the attack<sup>11</sup>

**US Department of Homeland Security** the department's Computer Emergency Readiness Team worked with federal departments "to mitigate against such attacks"<sup>12</sup>

**Kim Jong-il** Supreme Leader of DPRK (1994 – 2011)

**Lee Myung-bak** President of ROK (2008 – 2013)



# NARRATIVES

## DPRK government

- No comment specifically on 2009 attacks.
- Information war is the medium through which the wars of this century will be waged.<sup>13</sup>
- The DPRK is "fully ready for any form of hi-tech war."<sup>14</sup>
- The DPRK strives for independence in politics, self-sufficiency in economics and self-reliance in defence.

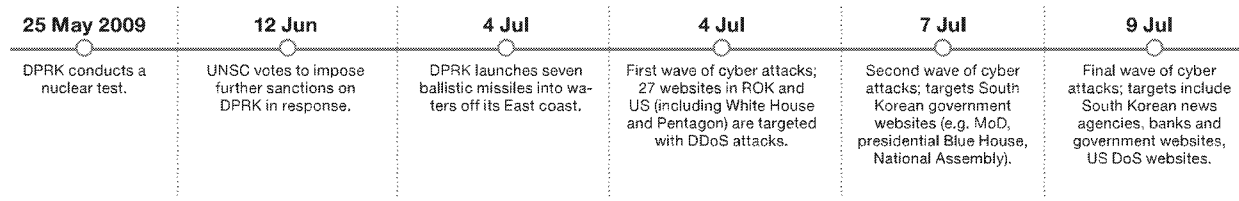
## ROK government

- The attack appears to be planned and executed by a specific organisation.<sup>15</sup>
- The attacks on the ROK seem to be connected to the attacks on the US.<sup>16</sup>
- North Korea was behind the cyber attacks.<sup>17</sup>
- The attack did not cause significant damage.

## US government

- It is not possible to confirm the source of the attacks.<sup>18</sup>
- The attacks did not cause any significant damage.<sup>19</sup>
- Protection against cyber attacks is a matter of great concern to the US.<sup>20,21</sup>
- The DPRK has been developing offensive cyber operations since at least 2009.<sup>22</sup>

# KEY EVENTS



# STRATEGIC LOGIC

The 2009 cyber attacks demonstrated the DPRK's cyber capabilities and monitored reactions to a distributed, deniable attack of predictably limited impact. Cyber attacks often tend to be covert and involve hacking into computer systems to retrieve information or take control. However,

the 2009 attack – and similar DDoS attacks – tend to make a highly visible political point.<sup>23</sup> It is likely that the attacks were designed to draw attention to the DPRK's capabilities, intimidate and increase citizens' feeling of insecurity, and instigate doubt in digital services and infrastructure.

# MEASURES

**DIPLOMATIC.** No official statements were made by DPRK in connection with this cyber attack. It is possible that the cyber attacks were an attempt to enhance the DPRK's negotiation position in public and covert diplomacy, especially regarding nuclear tests.

**INFORMATION.** Attempt to deny ROK and US citizens access to information from government, media and banking websites.

**MILITARY.** DPRK showed readiness to target the ROK and US through civilian infrastructure. No evidence of coordinated military signalling. Military assets do not seem to have been targeted.

**FINANCIAL.** OCC as very cost-effective way of gaining asymmetric strategic advantage.

**INTELLIGENCE.** Attacks were likely an act of reconnaissance to test the response and resilience of ROK and US systems.

**LEGAL.** OCC carries low risk of legal repercussions due to weak international laws and norms in this area.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- The internet and services that run over it have become part of the Critical National Infrastructure (CNI) of every nation.
- Public confidence in the ability of the government to defend against threats and maintain a functioning state.

## VULNERABILITIES

- Growing connectivity in all areas (banking, military systems, electrical power, public transport etc.), which presents significant vulnerabilities if those systems are compromised.
- Internet interruptions could generate a lack of situational awareness, command and control for the state.

## THREATS

- Rapid development of the DPRK's cyber capabilities. The 2009 attacks were not assessed to be particularly threatening, but were interpreted as a statement of intent and potential capability.
- Cyber attacks, even when not damaging, threaten to cause public insecurity and confusion, loss of confidence in the government, and (inter-)national political embarrassment.

## EFFECTS

- The 2009 attacks were not very damaging, but caused a great deal of media attention, especially in the ROK.
- The attacks highlighted the uncoordinated nature of government response, as some websites were able to fend off the simple attack while others were not.<sup>24</sup>
- Political inertia and inconsistent narratives from the two affected nations regarding attribution; the US flip-flopped on whether or not the DPRK was the perpetrator. This allowed others to frame the narrative.

# CASAS DEL ALBA IN PERU

## SUMMARY

In 2007, Peruvian officials, including President Alan García, accused the Venezuelan government of using development aid to interfere in its domestic affairs.<sup>1</sup> They claimed that Venezuela, in concert with Bolivia, was supporting around 58 'ALBA Houses' (Casas de la Alianza Bolivariana para los Pueblos de Nuestra América) in Peru, which were informally established in 2006.<sup>2</sup> These ALBA Houses provided charitable work in education and healthcare to impoverished rural Peruvian communities, particularly in the poor southern regions near the Bolivian border. The Peruvian government argued that the activities of the ALBA Houses were not motivated by purely humanitarian principles. It accused the ALBA Houses of using the direct interaction with vulnerable audiences to gather support for President Chávez' Bolivarian vision of a united Socialist South America as an alternative to the US model of liberal capitalism, and subvert Peruvian government authority.<sup>3</sup>

A key element of the ALBA Houses' work was to coordinate 'Mission Miracle', a joint Cuban-Venezuelan initiative that provided free eye surgery to impoverished Peruvians. As part of this initiative, patients were treated outside Peruvian territory in Bolivia and Venezuela, often via unregistered flights and without paperwork to track the passengers.<sup>4</sup>

The Peruvian government highlighted this as a particular concern, especially since pro-Chávez propaganda material, including videos and books, was shown on these flights.<sup>5</sup> Evidence also indicated a connection between the ALBA Houses and extremist political groups.<sup>6</sup> For instance, in February 2008, some ALBA House directors participated in violent protests against pro-privatisation legislation in the Peruvian Province of Cusco. According to eye-witnesses, Mission Miracle staff also encouraged patients to participate in these protests.<sup>7</sup> Coinciding with the launch of the ALBA Houses, President Chávez publicly supported far-left candidate Ollanta Humala, who narrowly missed power in Peru's 2006 presidential elections.<sup>8</sup> Humala himself was a public supporter of the ALBA Houses.

In 2008, the Peruvian congress set up an investigation into the activities of the ALBA Houses, and the following year, the final report recommended the closure of all ALBA Houses, concluding that they were a "political instrument of the Chávez government to achieve its expansionist project."<sup>9</sup> While the Peruvian government decided not to dissolve all ALBA Houses, many closed down on their own accord<sup>10</sup> and the Venezuelan government suspended Mission Miracle in Peru.<sup>11</sup>

## KEY POINTS

- The ALBA Houses were part of a complex set of integrated measures across the political, economic and social spectrums, rooted in the simple and unifying master narrative of a Bolivarian revolution. They were also ambiguous in nature and systematically avoided official channels and control mechanisms.<sup>12</sup> Venezuela denied any formal connections to the houses, claiming they were spontaneously set up by "private sympathisers with the Bolivarian project."<sup>13</sup>
- Development aid such as healthcare, education and infrastructure projects, can be an instrument of foreign policy as a kind of 'social diplomacy'. Social diplomacy can generate support for a political

ideology by providing services that the host government has failed to deliver, gaining political consent in strategically aligned countries but undermining the ruling authority of others.

- Formal investigations can reduce ambiguity and help contribute to a comprehensive threat assessment by identifying key vulnerabilities that could be exploited by foreign actors. A high-profile government investigation also sends a signal of unity and resolve that can deter foreign interference, irrespective of any actual legal consequences.

## CONTEXT

■ **Chávez' Bolivarianism.** Bolivarianism refers to a set of ideas that promote a united socialist South America as an alternative to US-led global capitalism and imperialism. It constitutes the core principles of Venezuelan domestic and foreign politics and provides the ideological framework for the ALBA Houses. Based on the thinking of 19<sup>th</sup> century independence leader Simón Bolívar, it calls for a Bolivarian revolution to realise '21<sup>st</sup> century Socialism' based on social and participatory democracy. When Hugo Chávez took office in 1999, Venezuela was named the 'Bolivarian Republic of Venezuela'.<sup>14</sup>

■ **Bolivarian Alliance for the Peoples of Our America (ALBA).** ALBA is essentially a loosely defined socialist economic alliance initiated by Cuba and Venezuela, based on the core principles of Bolivarian thinking. It was officially established in 2006 as a socialist alternative to the US-proposed Free Trade Area of the Americas (FTAA). ALBA

opposes liberalisation and privatisation, and supports Chávez' aspiration to a regional socialist bloc through political, economic and social integration. While Cuba, Venezuela, Bolivia and Nicaragua were member states, Peru refused to join the organisation and instead signed a bilateral free trade agreement with the US. The ALBA Houses were ideologically but not functionally connected to the ALBA alliance.<sup>15</sup>

■ **Mission Miracle.** A joint initiative by Cuba and Venezuela that provides free eye surgery to impoverished people across South America, launched in 2004. Countries include, among others, Cuba, Bolivia, Nicaragua, Ecuador, Peru and Guatemala. Mission Miracle is only one example of a wide set of Bolivarian Missions that provide development aid in a variety of areas, ranging from health care to education and infrastructure projects across South America. They are a key instrument of Venezuela's social diplomacy approach.<sup>16</sup>

## KEY ACTORS

**Venezuelan Embassy in Peru**  
**Bolivian Embassy in Peru**  
**Bolivarian Alliance for the Peoples of Our America** (*Alianza Bolivariana para los Pueblos de Nuestra América, ALBA*)  
**Congressional Investigation Commission** (2008 – 2009)

**Alan García** *President of Peru (2006 – 2011)*  
**Allan Wagner** *Minister of Defense of Peru (2006 – 2007)*  
**Walter Menchola** *Congressman (2006 – 2011), head of congressional investigation*  
**Hernan Fuentes** *Governor of Puno Province (2006 – 2010), supporter of ALBA Houses*  
**Ollanta Humala** *Leader of the Peruvian Nationalist Party, presidential candidate in the 2006 elections, President of Peru (2011 – 2016), supporter of ALBA Houses*  
**Virly Torres** *First Secretary of the Venezuelan Embassy (2005 – 2009)*  
**Marcial Maydana** *Director of Peru's ALBA Houses in southern Puno Province*  
**Hugo Chávez** *President of Venezuela (1999 – 2013)*

# NARRATIVES

## Peruvian government

- ALBA Houses are not just charity institutions, but promote Venezuelan Bolivarianism, support left-wing extremism and incite protests.<sup>17</sup>
- ALBA Houses pose a threat to Peruvian sovereignty; they are an instrument of foreign interference in Peru's domestic affairs aimed at subverting the Peruvian government and replacing it with a pro-Chávez leadership.<sup>18</sup>
- ALBA Houses form part of a broader strategy by Hugo Chávez to establish a Bolivarian South America as an alternative to the US-led liberal order.<sup>19</sup>

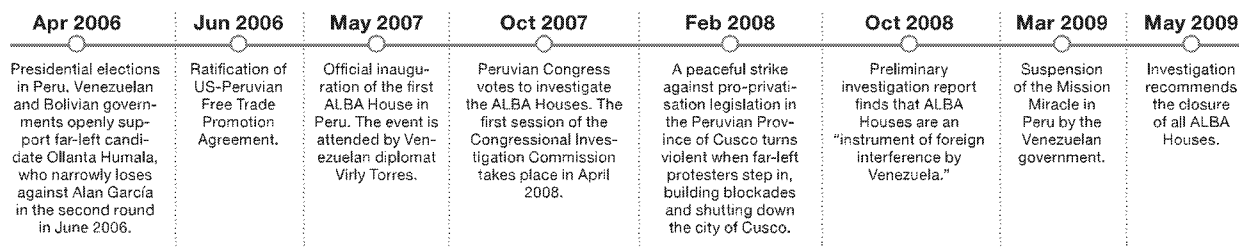
## Peru's left-wing opposition

- The investigation is not objective; it is an attempt to criminalise non-political charity work and persecute opposition parties by associating them with terrorist groups.<sup>20</sup>

## Venezuelan government

- ALBA Houses do not receive funding from Venezuela and have no connection to ALBA as an organisation. They are spontaneously set up by "private sympathisers with the Bolivarian project."<sup>21</sup>
- Refusal to use the term ALBA Houses, framing them as "Venezuelan friendship houses" to emphasise their informal status and undermine the claim of a connection between ALBA as an organisation and the ALBA Houses.<sup>22</sup>

# KEY EVENTS



# STRATEGIC LOGIC

The Venezuelan government pursues a geopolitical strategy which aims to foster its position as a regional hegemon in South America and balance against US dominance in the region.<sup>23</sup> This approach is rooted in the master narrative of a Bolivarian revolution and implemented through a range of integrated measures including 'social diplomacy', the direct delivery of

public services to other countries. These activities attempt to reinforce consent for Venezuela's foreign policy from the politicians of friendly nations, and create networks of influence to undermine the ruling authority of non-allied states such as Peru.

# MEASURES

**DIPLOMATIC.** ALBA House activities were supported by the Venezuelan and Bolivian embassies in Peru, especially by Venezuelan diplomat Virly Torres. She was not only a key figure in coordinating the transportation of patients to Bolivia and Venezuela and funding of the ALBA Houses, but also had links to the Bolivarian Continental Coordinator (CCB), an umbrella organisation for Bolivarian civil society groups with clear links to left-wing extremist groups.<sup>24</sup> President Chávez also openly supported presidential candidate Ollanta Humala in Peru's 2006 election.<sup>25</sup>

**INFORMATION.** ALBA House officials admitted that the educational classes offered by the ALBA Houses were not politically neutral but promoted Bolivarian ideas.<sup>26</sup> The Congressional Investigation concluded that healthcare services, such as the free eye surgeries under Mission Miracle, were combined with pro-Chávez information activities. For instance, during the flights transporting patients to Venezuela, videos and campaigning material were found that promoted the idea of a Bolivarian Revolution. This was supplemented by informal radio and TV channels set up to further disseminate pro-Chávez messages.<sup>27</sup>

**MILITARY.** Peruvian Congressman Rolando Sousa listed evidence indicating that the education and healthcare activities of the ALBA Houses were accompanied by paramilitary training in Peru, Bolivia and Venezuela.<sup>28</sup>

**FINANCIAL.** According to the Venezuelan embassy, the Venezuelan government only provided the financial and logistical means for Mission Miracle. However, the investigation and different media reports assessed that Venezuela also funded the ALBA Houses, opposition parties in Peru, especially Ollanta Humala, and left-wing extremist groups.

**LEGAL.** The legal status of the ALBA Houses was disputed. In Peru, NGOs are required to register with the Peruvian International Cooperation Agency (APCI) and report on their projects and funding arrangements. The ALBA Houses were established as "non-profit civil associations", thereby avoiding the status of an NGO to circumvent the official registration and monitoring processes.<sup>29</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS<sup>30</sup>

- Functioning healthcare and education system.
- Functioning democratic elections without foreign interference.
- Societal cohesion.
- Sovereignty, border security and control over migration movements.

## VULNERABILITIES

- Structural deficit of southern region: lack of healthcare, infrastructure and education; no targeted information and education for non-Spanish indigenous population.<sup>31</sup>
- Domestic left-wing violent extremism from 1980 – 2000, limited activity and resurgence in the early 2000s.

## THREATS

- Radicalisation and polarisation of society and potential resurgence of domestic terrorist activities.
- Interference in domestic political discourse and elections, aimed at undermining the democratic government.
- Establishment of parallel informal government structures through information, education and healthcare systems by foreign governments.

## EFFECTS

- Congressional investigation.
- Subsequent investigation of 38 ALBA House directors.<sup>32</sup>
- Suspension of Mission Miracle in Peru by Venezuela.
- Revision of legal framework regarding the authorisation of humanitarian aid provided by foreign states, as well as registration and monitoring of non-profit civil associations.

# Summary Endnotes

## 1 RUSSIAN SNAP EXERCISES IN THE HIGH NORTH endnotes

- <sup>1</sup> Dave Johnson, *Russia's Approach to Conflict – Implications for NATO's Deterrence and Defence* (Rome: NATO Defense College, April 2015).
- <sup>2</sup> Ibid.
- <sup>3</sup> Organization for Security and Co-operation in Europe (OSCE), *Vienna Document 2011 on Confidence and Security-Building Measures*, 30 November 2011.
- <sup>4</sup> Moscow Concerned about Growing Number of NATO Drills near Russian Borders – Diplomat," TASS, 15 March 2015.
- <sup>5</sup> Aslak Ballari and Robert Greiner, "Kan være Putin som ønsker å svare Norge," *NRK*, 16 March 2015.
- <sup>6</sup> David Stout, "Putin Puts Russia's Northern Fleet on 'Full Alert' in Response to NATO Drills," *Time Magazine*, 17 March 2015.
- <sup>7</sup> Expert Commission on Norwegian Security and Defence Policy, *Unified Effort* (Oslo: Norwegian Ministry of Defence, 2015), 15.

## 2 CONFUCIUS INSTITUTES endnotes

- <sup>1</sup> Eleanor Albert, "China's Big Bet on Soft Power," *Council on Foreign Relations*, 9 February 2018.
- <sup>2</sup> 首尔孔子学院. *Hanban official website*, [http://www.hanban.org/confuciusinstitutes/node\\_6848.htm](http://www.hanban.org/confuciusinstitutes/node_6848.htm)
- <sup>3</sup> Don Starr, "Chinese Language Education in Europe: The Confucius Institutes," *European Journal of Education* 44, No. 1 (2009): 65-82.
- <sup>4</sup> 关于孔子学院/课堂, *Hanban official website*, [http://www.hanban.org/confuciusinstitutes/node\\_10961.htm](http://www.hanban.org/confuciusinstitutes/node_10961.htm)
- <sup>5</sup> Quoted in: John Sudworth, "Confucius Institute: The Hard Side of China's Soft Power," *BBC News*, 22 December 2014.
- <sup>6</sup> Rachelle Peterson, *Outsourced To China: Confucius Institutes and Soft Power in American Higher Education* (New York: National Association of Scholars, 2017).
- <sup>7</sup> Joseph S. Nye, Jr., "Soft Power," *Foreign Policy* 80 (Autumn 1990): 153-171.
- <sup>8</sup> Eleanor Albert, "China's Big Bet on Soft Power," *Council on Foreign Relations*, 9 February 2018.
- <sup>9</sup> 孔子学院全球分布图. 中国干部学习网, *CCLN*, <http://study.ccln.gov.cn/uploadImage/danganziliao/laozhaopian/271437524467201.jpg>
- <sup>10</sup> James Bradshaw and Colin Freeze, "McMaster Closing Confucius Institute over Hiring Issues," *The Globe and Mail*, 7 February 2013.
- <sup>11</sup> Source: interview conducted by author; data anonymised to avoid compromising the respondent.
- <sup>12</sup> Source: interview conducted by author; data anonymised to avoid compromising the respondent.
- <sup>13</sup> Eleanor Albert, "China's Big Bet on Soft Power," *Council on Foreign Relations*, 9 February 2018.
- <sup>14</sup> "Sydney University Criticised for Blocking Dalai Lama Visit," *The Guardian*, 18 April 2013.

## 3 2007 CYBER ATTACKS ON ESTONIA endnotes

- <sup>1</sup> Andrzej Kozłowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014): 239-41.
- <sup>2</sup> Christina Mercer, "What is a DDoS Attack? What Happens During a DDoS Attack?" *Techworld*, 17 May 2017.
- <sup>3</sup> Ene Ergman quoted in: Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007.
- <sup>4</sup> "Declaration of the Minister of Foreign Affairs of the Republic of Estonia," *Estonian Government Website*, 1 May 2007.
- <sup>5</sup> Andrus Ansip, "Prime Minister Andrus Ansip's Speech in Riigikogu," *Estonian Government Website*, 2 May 2007.
- <sup>6</sup> Toomas Ilves (translated from German), "Interview: 'Ist ein Internetangriff der Ernstfall?'" *Frankfurter Allgemeine Zeitung*, 18 June 2007.
- <sup>7</sup> James Appathurai, "Press Briefing," *NATO*, 23 May 2007.
- <sup>8</sup> "NATO Sees Recent Cyber Attacks on Estonia as Security Issue," *DW*, 26 May 2007.
- <sup>9</sup> "Transcript of Remarks and Replies to Media Questions by Russian Minister of Foreign Affairs Sergey Lavrov Following Ministerial Meeting of Russia-NATO Council, Oslo, April 27, 2007," *The Ministry of Foreign Affairs of the Russian Federation*.
- <sup>10</sup> Vladimir Putin (translated), "Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War," *Kremlin.ru*, 9 May 2007.
- <sup>11</sup> Dmitry Peskov quoted in: "The Cyber Raiders Hitting Estonia," *BBC News*, 17 May 2007.
- <sup>12</sup> Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, 4 April 2009.
- <sup>13</sup> Sergei Ivanov quoted in: "Here We Go Again," *The Baltic Times*, 4 April 2007.
- <sup>14</sup> Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, 4 April 2009.
- <sup>15</sup> In *The Economist Intelligence Unit's 2007 e-readiness rankings*, Estonia ranked number one in Central and Eastern Europe in the categories "Business Environment," "Government Policy and Vision," and "Consumer and Business Adoption." Estonia also embraced e-democracy, being the first country in the world to offer internet voting in local elections in 2005, as well as in national parliamentary elections in 2007.
- <sup>16</sup> National Security Concept of the Republic of Estonia (2004), <https://www.files.ethz.ch/isn/156841/Estonia-2004.pdf>
- <sup>17</sup> "Population by Ethnic Nationality," *Statistics Estonia*, 9 June 2017, <http://www.stat.ee/34278>
- <sup>18</sup> Hanneli Rudi, "Eesti elanikud usaldavad enim televisiooni," *Postimees*, 13 July 2007.
- <sup>19</sup> Bruce Sterling, "Estonian Cyber Security," *Wired*, 9 January 2018.

## 4 US TRANSIT CENTER AT MANAS endnotes

- <sup>1</sup> The facility was originally called Ganci Air Base, then Manas Air Base, and renamed Manas Transit Center in 2009.
- <sup>2</sup> Transit Center at Manas (archived website), "Library," 5 August 2012.
- <sup>3</sup> As estimated by: Akbota Akylybayeva, "Military Cooperation between the United States and Kyrgyzstan: the Case of the Manas Airbase," *Weekly E-Bulletin* no. 51, Eurasian Research Institute, 19-25 January 2016.
- <sup>4</sup> Kemal Toktomushev, "Regime Security, Base Politics and Rent-Seeking: the Local and Global Political Economies of the American Air Base in Kyrgyzstan, 2001-2010," *Central American Survey* 34, no. 1 (2015): 58.
- <sup>5</sup> Scott Radnitz, "Memories of Manas: What Central Asia Taught America about Geopolitics," *The National Interest*, 30 June 2014.
- <sup>6</sup> Jim Nichol, "Kyrgyzstan and the Status of the US Manas Airbase: Context and Implications," *Congressional Research Service*, 1 July 2009, 1.
- <sup>7</sup> Alexander Cooley, "Manas Matters: The Changing Politics of the U.S. Military Base in Kyrgyzstan," *CSIS*, 8 December 2006, 2.
- <sup>8</sup> Ibid.
- <sup>9</sup> *Agreement between the Government of the United States of America and the Government of the Kyrgyz Republic Regarding the Transit Center at Manas International Airport and Any Related Facilities/Real Estate*, 13 May 2009, <https://www.state.gov/documents/organization/130490.pdf>
- <sup>10</sup> РИА Новости, "Президент Киргизии благодарен России за кредит и финансовую помощь," 3 February 2009.

- <sup>11</sup> Agreement between the Government of the United States of America and the Government of the Kyrgyz Republic Regarding the Transit Center at Manas International Airport and Any Related Facilities/Real Estate, 13 May 2009, <https://www.state.gov/documents/organization/130490.pdf>
- <sup>12</sup> E.g., see Akhilesh Pillalamarri, "The United States Just Closed Its Last Base in Central Asia," *The Diplomat*, 10 June 2014; Joshua Kucera, "Manas: Farewell, Or Good Riddance?" *EurasiaNet.org*, 8 June 2014.
- <sup>13</sup> E.g. documentary by Russian State Television Channel Rossiya: "Special Correspondent. Base. Film of Arkadiy Mamontov": Россия, Специальный корреспондент. База. Фильм Аркадия Мамонтова, 5 April 2009.

- <sup>14</sup> Andrzej Kozłowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* 3 (February 2014): 241-2.
- <sup>15</sup> РИА Новости, "Президент Киргизии благодарен России за кредит и финансовую помощь," 3 February 2009.
- <sup>16</sup> Radio Free Europe/Radio Liberty, "Kyrgyz President Calls Cooperation with Russia Crucial," 20 September 2012.
- <sup>17</sup> Alexander Cooley, "Manas Matters: The Changing Politics of the U.S. Military Base in Kyrgyzstan," *CSIS*, 8 December 2006, 2.

## 5 THE SPREAD OF SALAFISM IN EGYPT endnotes

- <sup>1</sup> Karim Sader quoted in: Marc Daou, "How Saudi Petrodollars Fuel Rise of Salafism," *France24*, 30 September 2012.
- <sup>2</sup> William Racimora, *Salafist/Wahhabite Financial Support to Educational, Social, and Religious Institutions* (Brussels: European Parliament, 2013).
- <sup>3</sup> Giorgio Cafiero, "Egypt and Saudi Arabia: Marriage on the Rocks?" *Huffington Post*, 12 June 2016.
- <sup>4</sup> Cheryl K. Chumley, "Saudi Arabia Accused of Giving Egypt \$1B to Oust Morsi," *Washington Times*, 30 July 2013.
- <sup>5</sup> Trevor Stanley, "Understanding the Origins of Wahhabism and Salafism," *The Jamestown Foundation*, 15 July 2005.
- <sup>6</sup> Saba Mahmood, *Politics of Piety: The Islamic Revival and the Feminist Subject* (Princeton: Princeton UP, 2011), 61.
- <sup>7</sup> Tom Perry, "Salafis Sense Best is Yet to Come in Egypt Vote," *Al Arabiya*, 2 December 2011.
- <sup>8</sup> Jacob Olidort, *The Politics of 'Quietist' Salafism* (Washington, D.C.: Brookings, 2015).
- <sup>9</sup> Nathan Field and Ahmed Hamam, "Salafi Satellite TV in Egypt," *Arab Media & Society*, 6 May 2009.
- <sup>10</sup> This was likely a response to the growing influence of the MB. As Salafis were mostly apolitical, the government deemed them less dangerous than the MB. Kent Davis-Packard, *A Ripple Beneath the Surface: Trends in Salafi Political Thought* (Washington, D.C.: Brookings, September 2014). The economic ties between the two countries brexercise influence over Egypt. The difficult economic situation in Egypt has forc

- <sup>11</sup> Marc Daou, "How Saudi Petrodollars Fuel Rise of Salafism," *France 24*, 30 September 2012.
- <sup>12</sup> William Racimora, *Salafist/Wahhabite Financial Support to Educational, Social, and Religious Institutions* (Brussels: European Parliament / Directorate-General for External Policies of the Union, 2013)
- <sup>13</sup> Giorgio Cafiero, "Saudi Arabia and Qatar: Dueling Monarchies," *Foreign Policy in Focus*, 26 September 2012.
- <sup>14</sup> "Dogma and Purity v Worldly Politics," *The Economist*, 20 October 2012.
- <sup>15</sup> Mohamed Nasser Hafez, "Ownership, Funding, and Editorial Policy in Private Media: Conference on Television and Radio Outlets in Egypt after the Revolution," 28-29 March 2012
- <sup>16</sup> "Norwegian Report: Saudi Intelligence Supports the Salafis to Hit Egypt in Sinai," *Alahdalsadik*, 11 August 2012.
- <sup>17</sup> William Racimora, *Salafist/Wahhabite Financial Support to Educational, Social, and Religious Institutions* (Brussels: European Parliament / Directorate-General for External Policies of the Union, 2013), 9.
- <sup>18</sup> Said Hijazi and Isra Talaat, «تدورات بالملايين من الخليج ورجال أعمال مصريين له الهدايا والمشايخ», *Elwatan News*, 14 June 2015.
- <sup>19</sup> "Sisi's Egypt: The March of the Security State," *Financial Times*, 19 December 2016.
- <sup>20</sup> Nada Ramadan, "Egyptians Furious over Islands Handover to Saudi Arabia," *The New Arab*, 11 April 2016.
- <sup>21</sup> "Salafism on the Rise in Egypt Cairo 00000202001.2 of 004," *The Telegraph*, 15 February 2011.

## 6 DISINFORMATION IN SWEDEN endnotes

- <sup>1</sup> Myndigheten för samhällsskydd och beredskap, "Opinioner 2016: Allmänhetens syn på samhällsskydd, beredskap, säkerhetspolitik och försvar," 2016.
- <sup>2</sup> Ben Nimmo, "Blowing the Whistle On Sputnik," *Atlantic Council's Digital Forensic Research Lab*, 31 May 2017; Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, 28 August 2016.
- <sup>3</sup> Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 788.
- <sup>4</sup> Ibid.

- <sup>5</sup> Damien Sharkov, "Russia's Lavrov Warns Sweden against NATO Membership," *Newsweek*, 29 April 2016; Michael Winiarski, "Russia Issues NATO Warning to Sweden," *DN*, 28 April 2016; "Putin Emphasizes that Sweden's Entry to NATO would Jeopardize Ties with Moscow," *TASS*, 1 June 2017.
- <sup>6</sup> Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 792.
- <sup>7</sup> Myndigheten för samhällsskydd och beredskap, "Opinioner 2016: Allmänhetens syn på samhällsskydd, beredskap, säkerhetspolitik och försvar," 2016.

## 7 HAMAS' USE OF HUMAN SHIELDS IN GAZA endnotes

- <sup>1</sup> Douglas Fischer, "Human Shields, Homicides, and House Fires: How a Domestic Law Analogy Can Guide International Law Regarding Human Shield Tactics in Armed Conflict," *American University Law Review* 57, no. 2 (December 2007): 488.
- <sup>2</sup> Raphael S. Cohen et al., *From Cast Lead to Protective Edge; Lessons from Israel's Wars in Gaza* (Santa Monica, CA: RAND, 2017), 45, 153-4.
- <sup>3</sup> Ibid. 102, 154.
- <sup>4</sup> *Case Western Reserve Journal of International Law* 43, no.1: <https://scholarlycommons.law.case.edu/jil/vol43/iss1/>
- <sup>5</sup> "Response to the Goldstone Report: Hamas and the Terrorist Threat from the Gaza Strip – the Main Findings of the Goldstone Report Versus the Factual Findings," *The Meir Amit Intelligence and Terrorism Information Center*, March 2010; "Deadly Hezbollah Chess Match," *The Washington Times*, 26 October 2006.
- <sup>6</sup> Harriet Sherwood, "Israeli Soldiers Convicted of Using Palestinian Boy as Human Shield," *The Guardian*, 3 October 2010.
- <sup>7</sup> Statement by spokesperson Mushir Al-Masri following a telephone alert issued by the IDF, which was planning to strike Hamas executive Waal Rajub Al-Shakra's house in Beit Lahiya. *Al-Aqsa TV*, 20 November 2006.
- <sup>8</sup> See: Israel Defense Forces, "Hamas Spokesperson Encourages Use of Human Shield," *Youtube Video*, 9 July 2014, at <https://www.youtube.com/watch?v=UXZEzbT0H1s>
- <sup>9</sup> Statement by spokesperson Iad al-Bazam; Hamas Facebook page, 13 July 2014.
- <sup>10</sup> "Operation Cast Lead Expanded," *Israel Ministry of Foreign Affairs*, 3 January 2009.

- <sup>11</sup> "Hamas Exploitation of Medical Institutions as 'Human Shield,'" *Israeli Security Agency*, 16 May 2009.
- <sup>12</sup> "Response to the Goldstone Report: Hamas and the Terrorist Threat from the Gaza Strip – the Main Findings of the Goldstone Report Versus the Factual Findings," *The Meir Amit Intelligence and Terrorism Information Center*, March 2010.
- <sup>13</sup> United Nations General Assembly, *Human Rights in Palestine and Other Occupied Arab Territories: Report of the United Nations Fact-Finding Mission on the Gaza Conflict*, 25 December 2009.
- <sup>14</sup> "Hezbollah's Human Shields," *The Washington Times*, 30 July 2006.
- <sup>15</sup> See for example: Neil Meads, "#BBCtrending: Are #GazaUnderAttack Images Accurate?" BBC, 8 July 2014; Sudarsan Raghavan, "A Reporter Explains What It's like Being Trapped in the Gaza Propaganda War," *The Washington Post*, 4 August 2014; Israel Defense Forces, "Hamas Social Media Rules: Describe Terrorists as Innocent Civilians," *IDF Website*, 21 July 2014.
- <sup>16</sup> "The Rafah Crossing – The Border with Gaza," in: *Global Security Watch – Egypt: A Reference Handbook*, eds. Denis Joseph Sullivan and Kimberly A. Jones (Santa Barbara: ABC-CLIO, 2008), 116-8
- <sup>17</sup> E.g. firing in proximity to civilians will usually be ordered only if there is an immediate threat to Israeli soldiers and/or civilians and/or physical assets.
- <sup>18</sup> Warning methods include text messages, phone calls, radio messages and air-dropped leaflets, but also dropping of non-lethal explosives.

## 8 THE 2010 SENKAKU CRISIS endnotes

- <sup>1</sup> Ito Masami and Mizuho Aoki, "Senkaku Collisions Video Leak Riles China," *The Japan Times*, 6 November 2010.
- <sup>2</sup> "U.S. Fudges Senkaku Security Pact Status," *The Japan Times*, 7 August 2010.
- <sup>3</sup> Keisuke Iida, *Japan's Security and Economic Dependence on China and the United States: Cool Politics, Lukewarm Economics* (Abingdon: Taylor & Francis, 2017).
- <sup>4</sup> Michael Green et al., *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone* (CSIS, Lanham: Rowman & Littlefield, 2017), 72.
- <sup>5</sup> Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, 22 September 2010.
- <sup>6</sup> "Irked Tourists Skip Japan," *Global Times*, 25 September 2010.
- <sup>7</sup> "China Beefs Up its Offshore Law Enforcement," *People's Daily Online*, 18 September 2010.
- <sup>8</sup> Huang Tun-yen and Jake Chung, "Isle Group Works for China: Source," *The Taipei Times*, 3 March 2013.
- <sup>9</sup> Chi Hung Kwan, "The Rise of China and Transformation of Japan-China Relations: Opportunities and Challenges for Japan," *RIETI*, 5 August 2014.
- <sup>10</sup> Yuka Hayashi, "China Row Fuels Japan's Right," *The Wall Street Journal*, 28 September 2010.

## 9 HUMANITARIAN AID IN THE RUSSO-GEORGIAN CONFLICT endnotes

- <sup>1</sup> *Independent International Fact-Finding Mission on the Conflict in Georgia, Report: Volume II*, September 2009, 436-7.
- <sup>2</sup> Ibid.
- <sup>3</sup> Ibid., 223-4.
- <sup>4</sup> "Beginning of the Meeting on Providing Humanitarian Assistance to the Population of South Ossetia," *Kremlin*, 9 August 2008.
- <sup>5</sup> S/PV.5953, 10 August 2008, 56.
- <sup>6</sup> "NATO Secretary General's Statement on the Deployment of Russian Railway Troops into Georgia," NATO, 3 June 2008.
- <sup>7</sup> S/PV.5952, 8 August 2008.
- <sup>8</sup> Abhijit Bhattacharjee and Mathew Varghese, *UNICEF's Response to Georgia Crisis: Real Time Evaluation*, March 2009, 22.
- <sup>9</sup> Greg Hansen, *Humanitarian Agenda 2015: Politics and Humanitarian Action in the Georgia Conflicts* (Medford, MA: Feinstein International Center, 2009), 17.
- <sup>10</sup> S/PV.5952, 8 August 2008, at 4.
- <sup>11</sup> "Russian Envoy: Repair of Abkhaz Railway a 'Humanitarian Act'," 2 June 2008.
- <sup>12</sup> *Independent International Fact-Finding Mission on the Conflict in Georgia, Report: Volume II*, September 2009, 147.
- <sup>13</sup> Ministry of Defence of Georgia, *National Security Concept of Georgia*, 2006.

## 10 CHINESE PUBLIC DIPLOMACY IN TAIWAN endnotes

- <sup>1</sup> Richard Bush, "What Xi Jinping Said about Taiwan at the 19th Party Congress," *The Brookings Institution*, 19 October 2017.
- <sup>2</sup> Deng Yuwen, "Is China Planning to Take Taiwan by Force in 2020?" *South China Morning Post*, 3 January 2018.
- <sup>3</sup> "Taiwanese/Chinese Identification Trend Distribution in Taiwan (1992/06-2017/12)," *Election Study Center at National Chengchi University*, 15 January 2018.
- <sup>4</sup> "Young Taiwanese Choose China Jobs over Politics," *Straits Times*, 20 August 2017.
- <sup>5</sup> Ralph Jennings, "China Demands Companies Stop Calling Taiwan A Country -- Here's What They'll Do," *Forbes*, 17 January 2018.
- <sup>6</sup> Chun-Yi Lee, "Cross-Strait Relations in 2018," *China Policy Institute: Analysis*, 28 December 2017.
- <sup>7</sup> Chun-Yi Lee, "Cross-Strait Relations in 2018," *China Policy Institute: Analysis*, 28 December 2017.
- <sup>8</sup> Li Zhenguang, "Taiwan Integral to National Rejuvenation," *China Daily*, 20 October 2017.
- <sup>9</sup> "'One China' Is Republic of China: MAC," *Focus Taiwan*, 17 April 2016.
- <sup>10</sup> "MAC: Beijing Needs a New Mindset to Find a New Model for Cross-Strait Interaction," *Mainland Affairs Council, Republic of China (Taiwan)*, accessed 20 April 2018.
- <sup>11</sup> 1985 Min-zhu Jin-bu Dang Dang-zhang, Dang-gang (The party plank of the Democratic Progressive Party).
- <sup>12</sup> Chien-Jung Hsu, "China's Influence on Taiwan's Media," *Asian Survey* 54, no.3 (May/June 2014): 515-39.
- <sup>13</sup> State Council Taiwan Affairs Office of the People's Republic of China, "Cross Strait Interactions and Exchanges," 2017.
- <sup>14</sup> Brenda Goh and Jess Macy Yu, "China Using Economic Incentives to Charm Tech-savvy Taiwanese Youth and Entrepreneurs," *Japanese Times*, 9 February 2018.
- <sup>15</sup> Edward White, "Alarm in Taiwan over Triad Ties to Pro-China Groups," *Financial Times*, 13 October 2017.
- <sup>16</sup> "关于印发《关于促进两岸经济文化交流合作的若干措施》的通知(Announcement of Measures to Promote Cross-Strait Economic and Cultural Exchanges and Cooperation), Taiwan Affairs Office of the State Council PRC, 28 February 2018.
- <sup>17</sup> Derek Grossman, Michael S. Chase and Logan Ma, "Taiwan's 2017 Quadrennial Defense Review in Context," *RAND Corporation*, 14 June 2017.
- <sup>18</sup> Richard C. Bush, Taiwan's Security Policy, *The Brookings Institution*, 3 August 2016.
- <sup>19</sup> Chien-Jung Hsu, "China's Influence on Taiwan's Media," *Asian Survey*, 11, no.3 (May/June 2014): 515-39.
- <sup>20</sup> "Young Taiwanese Choose China Jobs over Politics," *Straits Times*, 20 August 2017.
- <sup>21</sup> "Taiwanese/Chinese Identification Trend Distribution in Taiwan (1992/06-2017/12)," *Election Study Center at National Chengchi University*, 15 January 2018.

## 11 DETENTION OF ESTON KOHVER endnotes

- <sup>1</sup> The *Kaitsepolitseiamet* or *KAPO*.
- <sup>2</sup> "About Eston Kohver," *Ministry of the Interior, Republic of Estonia*, last updated on 28 September 2015.
- <sup>3</sup> "About Eston Kohver," *Ministry of the Interior, Republic of Estonia*, last updated on 28 September 2015.
- <sup>4</sup> Federal Security Service (FSB) is a governmental agency responsible for internal security, counterespionage and the fight against organised crime, terrorism, and smuggling of drugs, which is subordinated to the President of Russian Federation. Since 2003, the Federal Border Guard also falls under the responsibility of the FSB. Tiina Kaukvere, "Inimrõõvi uurimist raskendab asjaolu, et FSB allub presidendile," *Postimees*, 6 September 2014.
- <sup>5</sup> "About Eston Kohver," *Ministry of the Interior, Republic of Estonia*, last updated on 28 September 2015.
- <sup>6</sup> "DELFI FOTOD ja VIDEO: Kapo ametniku röövimispaigas Luhamaal laiuib Venemaa pool tihe võsa, näha on ka kaameraid," *Delfi.ee*, 6 September 2015.
- <sup>7</sup> Artem Kureev, "Estonian Spy Case: A Throwback to Cold War Era," *Russia Direct*, 20 August 2015.
- <sup>8</sup> Matti Aivar Lind, "VIDEOD: Vaata, kuidas Kohver Aleksei Dresseni vastu välja vahetatil Mehed tegid vahetuse käigus piiril paar sõna juttu," *Delfi.ee*, 26 September 2015.
- <sup>9</sup> Julian Borger, "Russians Open New Front after Estonian Official Is Captured in 'Cross-Border Raid'," *The Guardian*, 7 September 2014.
- <sup>10</sup> Status conflicts dispute over relative status (i.e. respect, recognition) positions in social hierarchy. Corinne Bendersky, Nicholas A. Hays, "Status Conflict in Groups," in *Organization Science* 23, no.2 (2011): 323-40.
- <sup>11</sup> "Areas of Activity," *Kaitsepolitseiamet*, website accessed 10 October 2018.
- <sup>12</sup> Georgi Beltadze, "Video: Vene meedia näitas videokaadred Kohvri kinnipidamisest," *Postimees*, 26 September 2015.
- <sup>13</sup> "Comment by Foreign Ministry Spokesperson Maria Zakharova on the Statements by Western Politicians Concerning the Judgment in the Eston Kohver Case," *Ministry of Foreign Affairs of the Russian Federation*, 20 August 2015.
- <sup>14</sup> "Russia Jails Estonian Intelligence Officer Tallinn Says Was Abducted over Border," *The Guardian*, 19 August 2015.
- <sup>15</sup> "Kaarel Kaas: side mahasurumine näitab, et röövimiskoha läheduses viibis ka kapo operatiivgrupp," *Delfi.ee*, 6 September 2014.

- <sup>16</sup> "DELFI FOTOD ja VIDEO: Kapo ametniku röövimispaigas Luhamaal laiuub Venemaa poolt tihke võsa, näha on ka kaameraid," *Delfi.ee*, 6 September 2014.
- <sup>17</sup> "Russia Jails Estonian Intelligence Officer Tallinn Says Was Abducted over Border," *The Guardian*, 19 August 2015.
- <sup>18</sup> "Comment by Foreign Ministry Spokesperson Maria Zakharova on the Statements by Western Politicians Concerning the Judgment in the Eston Kohver Case," *Ministry of Foreign Affairs of the Russian Federation*, 20 August 2015.
- <sup>19</sup> "Посольство РФ в Эстонии и МИД РФ ответили на претензии Госдепа США," *Regnum*, 21 August 2015.

- <sup>20</sup> "Ajakirjanik: Eesti ametnik rööviti kindlalt Eesti poolel," *Õhtuleht*, 6 September 2014.
- <sup>21</sup> Estonian Ministry of Defence, *National Security Concept of Estonia*, unofficial translation, adopted by the Riigikogu on 12 May 2010.
- <sup>22</sup> "Millions of Euros Allocated for Marking down Estonia's Eastern Border," *ERR.ee*, 20 February 2015.

## 12 FINNISH AIRSPACE VIOLATIONS endnotes

- <sup>1</sup> Thomas Frear, Lukasz Kulesa and Ian Kearns, *Dangerous Brinkmanship: Close Military Encounters Between Russia and the West in 2014* (London: European Leadership Network, November 2014), P6.
- <sup>2</sup> The act of getting a military aircraft airborne in response to an immediate threat such as the sighting of a hostile aircraft in one's airspace.
- <sup>3</sup> "NATO Tracks Large-Scale Russian Air Activity in Europe," *NATO*, 29 October 2014.
- <sup>4</sup> Thomas Frear, Lukasz Kulesa and Ian Kearns, *Dangerous Brinkmanship: Close Military Encounters Between Russia and the West in 2014* (London: European Leadership Network, November 2014), P6.
- <sup>5</sup> Sauli Niinistö and Vladimir Putin, "Press Statements and Answers to Journalists' Questions Following Russian-Finnish Talks," *Kremlin*, 1 July 2016.
- <sup>6</sup> "Finland Asks Russia to Explain Airspace Violations," *YLE*, 21 May 2014.
- <sup>7</sup> Sauli Niinistö and Vladimir Putin, "Press Statements and Answers to Journalists' Questions Following Russian-Finnish Talks," *Kremlin*, 1 July 2016.
- <sup>8</sup> "Finland Asks Russia to Explain Airspace Violations," *YLE*, 21 May 2014.
- <sup>9</sup> Juhani Karila and Alekski Teivanen, "Finnish Jets Were Unable to Respond to Russian Airspace Violations. Niinistö Confirms," *Helsinki Times*, 31 May 2014.
- <sup>10</sup> Sakari Suoninen and Jussi Rosendahl, "Finnish Reasons for Joining NATO 'Stronger than Ever': Defense Minister," *Reuters*, 18 June 2014.
- <sup>11</sup> Kati Pohjanpalo and Kasper Viita, "Finland's Fighter Jets on Alert as Russia Violates Airspace," *Bloomberg*, 29 August 2014.
- <sup>12</sup> David Stout, "NATO Accuses Russian Military Aircraft of Flagrantly Violating European Airspace," *Time*, 30 October 2014.
- <sup>13</sup> Finnish Ministry for Foreign Affairs (2016).
- <sup>14</sup> Kati Pohjanpalo and Kasper Viita, "Finland's Fighter Jets on Alert as Russia Violates Airspace," *Bloomberg*, 29 August 2014.
- <sup>15</sup> "Finnish Jets Were Unable to Respond to Russian Airspace Violations, Niinistö Confirms," *Helsinki Times*, 31 May 2014.
- <sup>16</sup> *The Effects of Finland's Possible NATO Membership: An Assessment*, Finnish Ministry for Foreign Affairs, April 2016.
- <sup>17</sup> Thomas Frear, Lukasz Kulesa and Ian Kearns, *Dangerous Brinkmanship: Close Military Encounters Between Russia and the West in 2014* (London: European Leadership Network, November 2014).

## 13 SOUTH STREAM PIPELINE endnotes

- <sup>1</sup> "An Open Letter to Obama," *Radio Free Europe/Radio Liberty*, 16 July 2009.
- <sup>2</sup> "Questions and Answers on the Third Legislative Package for an Internal EU Gas and Electricity Market," *European Commission*, 2 March 2011.
- <sup>3</sup> "The Kremlin's Gas Games in Europe," *Atlantic Council*, May 2017
- <sup>4</sup> *Anticorruption in Transition: A Contribution to the Policy Debate* (Washington, D.C.: The World Bank, 2000), 3.
- <sup>5</sup> Heather A. Conley et. al., *The Kremlin Playbook* (Washington D.C.: CSIS, 2016), 44.
- <sup>6</sup> "The Energy Community," *European Commission*, accessed 6 August 2018.
- <sup>7</sup> "Energy Stress Test," *European Commission*, accessed 6 August 2018.
- <sup>8</sup> "Bulgargaz," Български Енергиен Холдинг, accessed 23 March 2018.
- <sup>9</sup> Isabel Gorst, "Gazprom Ready for South Stream," *Financial Times*, 15 November 2012.
- <sup>10</sup> Shaun Walker, "Putin Blames EU as Russia Abandons Plans for South Stream Gas Pipeline," *The Guardian*, 1 December 2014.
- <sup>11</sup> Vihma, Antto, and Umur Turksen. "The Geoeconomics of the South Stream Pipeline Project." *Columbia SIPA Journal of International Affairs*, 1 January 2016.
- <sup>12</sup> Statement by President Junker, *European Commission*, 04 December 2014.
- <sup>13</sup> Jonathan Stern, Simon Pirani and Katja Yafimaya, *Does the Cancellation of South Stream Signal a Fundamental Reorientation of Russian Gas Export Policy?* (Oxford: The Oxford Institute for Energy Studies, 2015), 4
- <sup>14</sup> See for example: Vladimir Socor, "Gazprom Reveals Unaffordable Costs of South Stream Project," *The Jamestown Foundation*, 12 February 2009.
- <sup>15</sup> "Rumen Ovcharov: We Are Losing 600 Mn Dollars Annually from the Cancellation of South Stream," *Марица*, 3 December 2014.
- <sup>16</sup> "Интервью за Дойче Веле: «България ли спря Южен поток», *Blog of Ilian Vassilev*, 2 December 2014.
- <sup>17</sup> Ralitsa Petrova Hiteva and Tomas Maltby, "Standing in the Way by Standing in the Middle: The Case of State-owned Natural Gas Intermediaries in Bulgaria," *Geoforum* 54 (July 2014): 120-31.
- <sup>18</sup> According to German foreign intelligence service BND. Gerald Traufetter, "Fears Grow over Bulgaria's Russian Dependence," *Spiegel Online*, 12 May 2014.
- <sup>19</sup> Judy Dempsey, "Gazprom's Grip on Western Europe Tightens with Pipelines to Hungary," *New York Times*, 22 June 2006.
- <sup>20</sup> Ralitsa Petrova Hiteva and Tomas Maltby, "Standing in the Way by Standing in the Middle: The Case of State-owned Natural Gas Intermediaries in Bulgaria," *Geoforum* 54 (July 2014): 120-31.
- <sup>21</sup> "EU Takes Action over South Stream Pipeline," *The Economist*, 5 July 2014.
- <sup>22</sup> "Gazprom Renews Threat to Swap Bulgaria for Romania in South Stream," *Novonite*, 14 October 2010.

## 14 RUSSIAN LANGUAGE REFERENDUM IN LATVIA endnotes

- <sup>1</sup> "Results of the 2011 Population and Housing Census in Latvia," Centrālā statistikas parvalde, 2011.
- <sup>2</sup> "Usakovs Pulls an About-Face," *The Baltic Times*, 9 November 2011.
- <sup>3</sup> "Usakovs Pulls an About-Face," *The Baltic Times*, 9 November 2011.
- <sup>4</sup> "2012. gada 18. februāra tautas nobalsošana par likumprojekta "Grozījumi Latvijas Republikas Satversmē" pieņemšanu Rezultāti," *CVK*, accessed 11 October 2018.
- <sup>5</sup> "DP mudina 'Dzimto valodu' atklāt finansēšanas avotus; Lindermans noliedz saistību ar Kremli," *Delfi.lv*, 22 November 2011.
- <sup>6</sup> "Tiesa prokremļisko aktīvistu Lindermanu atbrīvo no apcietinājuma," *LSM.lv*, 21 May 2018.
- <sup>7</sup> Sanita Jemberga, Mikko Salu, and Šarūnas Černiauskas, "Kremlin's Millions," *re.baltica*, 27 August 2015.
- <sup>8</sup> Interview with Andis Kudors, Executive Director at the Centre for Eastern European Policy Studies, conducted on 10 April 2017.
- <sup>9</sup> Dite Liepa, "The Most Significant Language Policy Events in the Mass Media," in *The Language Situation in Latvia 2010-2015*, edited by Gunter Kļava (Riga: Latvian Language Agency, 2017), 231.
- <sup>10</sup> *On the Status of Those Former U.S.S.R. Citizens Who Do Not Have the Citizenship of Latvia or that of Any Other State*, law adopted by the Saeima on 25 April 1995, last amending law of 21 June 2007.
- <sup>11</sup> "Statistika – Iedzīvotāju reģistrs," *Latvian Office of Citizenship and Migration Affairs*.
- <sup>12</sup> Dite Liepa, "The Most Significant Language Policy Events in the Mass Media," in *The Language Situation in Latvia 2010-2015*, edited by Gunter Kļava (Riga: Latvian Language Agency, 2017), 232.
- <sup>13</sup> "High Commissioner Welcomes State Language Law in Latvia," *OSCE*, 9 December 1999.
- <sup>14</sup> Sanita Jemberga, Mikko Salu, and Šarūnas Černiauskas, "Kremlin's Millions," *re.baltica*, 27 August 2015.

- <sup>15</sup> Sergei Lavrov quoted in: Andis Kudors, "Russian Compatriot Policy and Languages Warfare in Latvia," *Centre for East European Policy Studies*, 11 January 2012.
- <sup>16</sup> In 2018, Gaponenko was charged with offences including "inciting ethnic hatred and assisting a foreign state in action against Latvia" although it is unclear to which activities these charges relate. "Additional Charges for Pro-Russia Activist," *LSM.LV*, 20 August 2018.
- <sup>17</sup> Aleks Tapinsh, "Russian Language Vote Shows Ethnic Split in Latvia," *Reuters*, 17 February 2012.
- <sup>18</sup> "Latvia Rejects Making Russian an Official Language," *BBC News*, 19 February 2012.
- <sup>19</sup> "Referendoomed: No Go for Russian Language in Latvia," *RT*, 20 February 2012.
- <sup>20</sup> David M. Herszenhorn, "Latvians Reject Russian as Second Language," *New York Times*, 19 February 2012.
- <sup>21</sup> Aleks Tapinsh, "Russian Language Vote Shows Ethnic Split in Latvia," *Reuters*, 17 February 2012.
- <sup>22</sup> David M. Herszenhorn, "Latvians Reject Russian as Second Language," *New York Times*, 19 February 2012.
- <sup>23</sup> "Latvia Rejects Making Russian an Official Language," *BBC News*, 19 February 2012.
- <sup>24</sup> Monika Hanley, "The Voice of the People," *The Baltic Times*, 15 February 2012.
- <sup>25</sup> "Politicians Blamed for Social Divide," *The Baltic Times*, 4 January 2012.
- <sup>26</sup> Andris Straumanis, "Diaspora Leaders Ask Latvians Worldwide to Vote against Referendum," *Latvians Online*, 16 January 2012.
- <sup>27</sup> "Referendums notiks; 18. Februārī visi dodamies balsot," *TV NET*, 20 January 2012.
- <sup>28</sup> "Transcript of the Meeting with the Participants in the International Club Valdai," *Kremlin.ru*, 21 September 2008; Ulrich Kühn, "Preventing Escalation in the Baltics: A NATO Playbook," *Carnegie Endowment for International Peace*, 28 March 2018.
- <sup>29</sup> Nina Kolyako, "Russian Ambassador: Observance of Human Rights Recommendations Would Have Allowed Latvia to Avoid Referendum," *The Baltic Course*, 10 February 2012.
- <sup>30</sup> *Ibid.*
- <sup>31</sup> Arturs Bikovs, Ilvija Brūge and Andris Spruds, *Russia's Influence and Presence in Latvia* (Brussels: European Reform, n.d.), 21.
- <sup>32</sup> Interview with Andis Kudors, Executive Director at the Centre for Eastern European Policy Studies, conducted on 10 April 2017.
- <sup>33</sup> Inga Sprunge, Donata Motuzaite, Gunita Gailāne, "Spreading Democracy in Latvia, Kremlin Style," *re:baltica*, 19 March 2012.
- <sup>34</sup> "Kozlovskis: krievu valodas referendumam nauda nāca arī no Krievijas," *DELFI*, 13 May 2012.
- <sup>35</sup> *Ibid.*
- <sup>36</sup> Interview with Andis Kudors, Executive Director at the Centre for Eastern European Policy Studies, conducted on 10 April 2017.
- <sup>37</sup> David M. Herszenhorn, "Latvians Reject Russian as Second Language," *New York Times*, 19 February 2012.
- <sup>38</sup> Corinne Deloy, "The Latvians Say 'No' En Masse to the Adoption of Russian as the Second Official Language of Their Country," *Fondation Robert Schuman*, 18 February 2012.

## 15 INSTITUTE OF DEMOCRACY AND COOPERATION endnotes

- <sup>1</sup> IDC homepage (English), accessed 15 May 2018.
- <sup>2</sup> "How The Kremlin Wields Its Soft Power in France," *Radio Free Europe / Radio Liberty*, 24 June 2014.
- <sup>3</sup> Cecile Vaissié, *Les Réseaux du Kremlin en France* (Paris: Les Petits Matins, 2016).
- <sup>4</sup> Exact sources of funding are not made public by the IDC.
- <sup>5</sup> Andrew Foxall, "The Kremlin's Sleight of Hand: Russia's Soft Power Offensive in the UK," *Henry Jackson Society: Russia Studies Centre*, Policy Paper No.3, February 2015.
- <sup>6</sup> *Ibid.*
- <sup>7</sup> Peter Rutland and Andrei Kazantsev, "The Limits of Russia's 'Soft Power,'" *Journal of Political Power* 9, no. 3 (2016): 395-413.
- <sup>8</sup> *Ibid.*
- <sup>9</sup> *Ibid.*
- <sup>10</sup> Vladimir Putin, "Russia and the Changing World," originally published in *Moskovskiy Novosti*, translated in *RT*, 27 February 2012.
- <sup>11</sup> Vladimir Putin, "Совещание послов и постоянных представителей России," *Kremlin*, 9 July 2012.
- <sup>12</sup> IDC website (english), accessed 15 May 2018.
- <sup>13</sup> Vladka Vojtiskova, Hubertus Schmid-Schmidfelden, Vit Novotny, and Kristina Potapova, "The Bear in Sheep's Clothing: Russia's Government-Funded Organizations in the EU," *Wilfried Martens Centre for European Studies Research Paper*, July 2016, 46-7.
- <sup>14</sup> Steven Lee Myers, "Snowden's Lawyer Comes With High Profile and Kremlin Ties," *New York Times*, 27 July 2013.
- <sup>15</sup> "Dr. Andranik Migranyan," *The Middlebury Institute of International Studies at Monterey*, accessed 7 May 2018.
- <sup>16</sup> "Russian Propaganda, Good and Bad," *The Economist*, 1 May 2008.
- <sup>17</sup> "John Laughland Addresses Conference Organised by the State Duma in Moscow," *IDC*, 25 November 2014.
- <sup>18</sup> "Миссия закончена. Ситуация с правами человека в США стала лучше," *газета.ru*, 28 June 2015.
- <sup>19</sup> "Нью-Йоркский Институт демократии и сотрудничества Андраника Миграняна закрывается," *газета.ru*, 28 June 2015.
- <sup>20</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND Corporation, 2018).
- <sup>21</sup> Cecile Vaissié, *Les Réseaux du Kremlin en France* (Paris: Les Petits Matins, 2016).
- <sup>22</sup> Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (New York: Rowman and Littlefield, 2015).
- <sup>23</sup> "New Russian Think Tank to Question Western Ways," *NBC News*, 28 January 2008.
- <sup>24</sup> "IDC at the European Parliament," *IDC*, 24 June 2015.
- <sup>25</sup> "Opinions/Tous nos auteurs: John Laughland," *RT France*, accessed 11 May 2018.
- <sup>26</sup> "How the Kremlin Wields Its Soft Power in France," *Radio Free Europe / Radio Liberty*, 24 June 2014.
- <sup>27</sup> *Defence and National Security Strategic Review*, République Française, 2017, 54.
- <sup>28</sup> *For a Transparent and Collaborative Government: France National Action Plan 2015-2017*, République Française.
- <sup>29</sup> For example: "Natalia Narochnitskaya Speaks in Rome on the Unity of Europe's Christian Civilisation," *IDC*, 24 May 2012.
- <sup>30</sup> *Defence and National Security Strategic Review*, République Française, 2017.
- <sup>31</sup> Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, 2016).
- <sup>32</sup> Following search data valid as of 17 October 2017.
- <sup>33</sup> Bruce Stokes, "Russia: Putin Held in Low Regard around the World," *Pew Research Center*, 8 May 2015.

## 16 ZAMBIAN ELECTIONS 2006 endnotes

- <sup>1</sup> Dominik Kopiriski and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 187.
- <sup>2</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 128.
- <sup>3</sup> Dominik Kopiriski and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 186-7.
- <sup>4</sup> *Ibid.*, 187.
- <sup>5</sup> *Ibid.*, 182.
- <sup>6</sup> Howard W. French, "In Africa, an Election Reveals Skepticism of Chinese Involvement," *The Atlantic*, 29 September 2011.
- <sup>7</sup> Godfrey Hampway and Peter Kragelund, "Trends in Sino-Zambian Relations," in *China's Diplomacy in Eastern and Southern Africa*, edited by Seifudein Adem (Ashgate, 2014).



- <sup>8</sup> Howard W. French, "In Africa, an Election Reveals Skepticism of Chinese Involvement," *The Atlantic*, 29 September 2011.
- <sup>9</sup> Miles Larmer and Alastair Fraser, "Of Cabbages and King Cobra: Populist Politics and Zambia's 2006 Election," *African Affairs* 106, no.425 (2007): 628.
- <sup>10</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 188.
- <sup>11</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 189; Aleksandra W. Gadzala, "From Formal- to Informal-Sector Employment: Examining the Chinese Presence in Zambia," *Review of African Political Economy* 37, no.123 (2010): 46; Hannah Postel, "Moving Beyond 'China in Africa': Insights from Zambian Immigration Data," *Journal of Current Chinese Affairs* 2 (2017): 156-62.
- <sup>12</sup> Kartik Jayaram, Omid Kassiri and Irene Yuan Sun, "The Closest Look Yet at Chinese Economic Engagement in Africa," *McKinsey*, June 2017.
- <sup>13</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 181-92.
- <sup>14</sup> Erin Conqay-Smith, "Zambian Election Results Check Chinese Influence in Africa," *PRi*, 25 September 2011; Miles Larmer and Alastair Fraser, "Of Cabbages and King Cobra: Populist Politics and Zambia's 2006 Election," *African Affairs* 106, no.425 (2007): 620.
- <sup>15</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 181-92.
- <sup>16</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 126.
- <sup>17</sup> Howard W. French, "In Africa, an Election Reveals Skepticism of Chinese Involvement," *The Atlantic*, 29 September 2011; "Interview: Zambia, China Benefit From Increasing Bilateral Trade, Investment," *FMPRC.gov.cn*, 19 May 2006.
- <sup>18</sup> John Reed, "China Issues Zambian Election Threat," *Financial Times*, 6 September 2006.
- <sup>19</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 188-9.
- <sup>20</sup> "Zambia to Strengthen Economic Cooperation with China: Official," *FMPRC.gov.cn*, 28 June 2005.
- <sup>21</sup> *Ibid.*
- <sup>22</sup> Peter Goodspeed, "King Cobra' Pits Zambia against China," *National Post*, 27 September 2006.
- <sup>23</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 188.
- <sup>24</sup> Howard W. French, "In Africa, an Election Reveals Skepticism of Chinese Involvement," *The Atlantic*, 29 September 2011.
- <sup>25</sup> Miles Larmer and Alastair Fraser, "Of Cabbages and King Cobra: Populist Politics and Zambia's 2006 Election," *African Affairs* 106, no.425 (2007): 611-37.
- <sup>26</sup> Godfrey Hampway and Peter Kragelund, "Trends in Sino-Zambian Relations," *China's Diplomacy in Eastern and Southern Africa*, edited by Seifudein Adem (Ashgate, 2014).
- <sup>27</sup> *Ibid.*
- <sup>28</sup> "China to Sever Ties with Zambia if Pro-Taiwan Leader Wins," *China Daily*, 5 September 2006.
- <sup>29</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 188.
- <sup>30</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 127.
- <sup>31</sup> "Zambia Welcomes Chinese Agricultural Know-How," *Ministry of Foreign Affairs of the People's Republic of China*, 23 March 2006; "China Provides Zambia with FM Transmitters," *Ministry of Foreign Affairs of the People's Republic of China*, 13 September 2005.
- <sup>32</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 130.
- <sup>33</sup> Aleksandra W. Gadzala, "From Formal- to Informal-Sector Employment: Examining the Chinese Presence in Zambia," *Review of African Political Economy* 37, no.123 (2010), 45.
- <sup>34</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 123-4.
- <sup>35</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011): 185.
- <sup>36</sup> Anders Bastholm and Peter Kragelund, "State-driven Chinese Investments in Zambia: Combining Strategic Interests and Profits," in *The New Presence of China in Africa*, edited by Meine Pieter van Dijk (Amsterdam: Amsterdam UP, 2009), 130.
- <sup>37</sup> *Ibid.*, 126-7.
- <sup>38</sup> Aleksandra W. Gadzala, "From Formal- to Informal-Sector Employment: Examining the Chinese Presence in Zambia," *Review of African Political Economy* 37, no.123 (2010): 41-59.
- <sup>39</sup> *Ibid.*
- <sup>40</sup> "Zambians Wary of 'Exploitative' Chinese Employers," *IRIN*, 23 November 2006.
- <sup>41</sup> Aleksandra W. Gadzala, "From Formal- to Informal-Sector Employment: Examining the Chinese Presence in Zambia," *Review of African Political Economy* 37, no.123 (2010): 41-59.
- <sup>42</sup> *Ibid.*
- <sup>43</sup> Dominik Kopyński and Andrzej Polus, "Sino-Zambian Relations: 'An All-Weather Friendship' Weathering the Storm," *Journal of Contemporary African Studies* 29, no.2 (2011), 190.
- <sup>44</sup> Godfrey Hampway and Peter Kragelund, "Trends in Sino-Zambian Relations," in *China's Diplomacy in Eastern and Southern Africa*, edited by Seifudein Adem (Ashgate, 2014).

## 17 SERBIAN ORTHODOX CHURCH endnotes

- <sup>1</sup> Jelena Milić, "The Russification of Serbia," *New Eastern Europe* XIII, no.4 (2014): 94-102; Jelena Dzombic, "Rightwing Extremism in Serbia," *Race & Class* 55, no.4 (2014): 108.
- <sup>2</sup> B. Aleksov, "The Serbian Orthodox Church," in: *Orthodox Christianity and Nationalism in Nineteenth Century Southeastern Europe* (Fordham University, 2014): 65-100.
- <sup>3</sup> Bureau of Democracy, Human Rights, and Labor. "Serbia: July-December, 2010 International Religious Freedom Report," *U.S. Department of State*, 13 September 2011.
- <sup>4</sup> Orysia Lutsevych, "Agents of the Russian World: Proxy Groups in the Contested Neighbourhood," *Chatham House*, 14 April 2016.
- <sup>5</sup> Elina Lange-Ionatamšvili et al., *Russia's Footprint in the Nordic-Baltic Information Environment* (Riga: NATO Strategic Communications Centre of Excellence, 2018), 25.
- <sup>6</sup> Vladimir Putin, "It Is Impossible to Move Forward Without Spiritual, Cultural and National Self-Determination"- Putin," translated and published in *RT*, 20 September 2013.
- <sup>7</sup> "Orthodox Churches Fight Back as Eastern Europe Pushes to Modernize, Secularize," *RadioFreeEurope / RadioLiberty*, 26 May 2013.
- <sup>8</sup> "POČELI RADOVI Kompanija 'Gasprom njeft' sa 4 miliona evra finansira mozaik u Hramu Svetog Save," *Blic*, 22 April 2016.
- <sup>9</sup> Jaroslaw Wiśniewski, "Russia Has a Years-Long Plot to Influence Balkan Politics. The U.S. Can Learn a Lot from It," *The Washington Post: Monkey Cage*, 19 September 2016.
- <sup>10</sup> "Putin Calls Kosovo Independence 'Terrible Precedent'," *The Sydney Morning Herald*, 23 February 2008.
- <sup>11</sup> "Survey of Serbian Public Opinion," *International Republican Institute*, 4-15 July 2015.
- <sup>12</sup> Maja Zivanovic, "Serbian Orthodox Church Plans to Change Name: Report," *Balkan Insight*, 6 March 2018.
- <sup>13</sup> Maja Zivanovic, "Serbian Orthodox Church Plans to Change Name: Report," *Balkan Insight*, 6 March 2018.
- <sup>14</sup> Aleksandar Vasovic, "Serbia's Orthodox Church to Change Name to Stress Kosovo Link," *Reuters*, 8 March 2018.
- <sup>15</sup> Jane Perlez, "Defying Milosevic, Thousands March in Serbian Capital," *The New York Times - Archives*, 1996.
- <sup>16</sup> David McKittrick, "Patriarch Pavle: Head of the Serbian Orthodox Church during the Kosovo War," *The Independent*, 4 December 2009.
- <sup>17</sup> "SERBIA: New Serbian Patriarch Says No Need to be Sceptical of EU," *Reuters*, 31 January 2010.

- <sup>18</sup> Jelena Milić, "The Russification of Serbia," *New Eastern Europe* XIII, no.4 (2014): 94-102.
- <sup>19</sup> Jelena Dzombic, "Rightwing Extremism in Serbia," *Race & Class* 55, no.4 (2014): 108.
- <sup>20</sup> "Failure to Protect: Anti-Minority Violence in Kosovo, March 2004," *Human Rights Watch*, 25 July 2004
- <sup>21</sup> Jelena Dzombic, "Rightwing Extremism in Serbia," *Race & Class* 55, no.4 (2014): 108.
- <sup>22</sup> Jelena Dzombic, "Rightwing Extremism in Serbia," *Race & Class* 55, no.4 (2014): 109.
- <sup>23</sup> Communication Service of the Moscow Patriarchate Department for External Church Relations, "Concerning the Growing Tension in Kosovo and Metohija," *The Russian Orthodox Church*, 5 February 2013.
- <sup>24</sup> "Russian, Serbian Patriarchs Criticize Serbian Government," *b92*, 17 July 2013.
- <sup>25</sup> "Primates of Russian and Serbian Churches Meet with Head of Serbia's Government, Mr. Aleksandar Vučić," *The Russian Orthodox Church*, 15 November 2014.
- <sup>26</sup> "Primates of Russian and Serbian Orthodox Churches Meet with President of Serbia, Mr. Tomislav Nikolić," *The Russian Orthodox Church*, 15 November 2014.
- <sup>27</sup> Elisabeth Braw, "Mixed Feelings in Macedonia as a Russian Orthodox Church Rises," *RadioFreeEurope / Radio Liberty*, 25 June 2015.
- <sup>28</sup> Dusan Tomovic, "Serbian Church Urges Montenegro NATO Referendum," *Balkan Insight*, 5 January 2016.
- <sup>29</sup> *Eyes Wide Shut: Russian Soft Power Gaining Strength in Serbia – Goals, Instruments and Effects* (Belgrade: Center for Euro-Atlantic Studies, 2016).
- <sup>30</sup> Elisabeth Braw, "Mixed Feelings in Macedonia as a Russian Orthodox Church Rises," *RadioFreeEurope / Radio Liberty*, 25 June 2015.
- <sup>31</sup> "Survey of Serbian Public Opinion," *International Republican Institute*, 24 November – 3 December 2015.
- <sup>32</sup> Orysia Lutsevych, "Agents of the Russian World: Proxy Groups in the Contested Neighbourhood," *Chatham House*, 14 April 2016.
- <sup>33</sup> "Kosovo's Orthodox Shrines Begin to Be Restored with Funds Provided from Russia," *The Russian Orthodox Church*, 3 August 2012.
- <sup>34</sup> Maja Zivanovic, "Serbs Doubt Prospect of EU Membership, Survey Shows," *Balkan insight*, 8 March 2017.
- <sup>35</sup> *National Security Strategy of the Republic of Serbia* (Belgrade: Republic of Serbia, October 2009), 7.
- <sup>36</sup> *National Security Strategy of the Republic of Serbia* (Belgrade: Republic of Serbia, October 2009), 7, 8.
- <sup>37</sup> Gordona Knezevic, "Serbia's First Openly Gay Minister Makes History," *RadioFreeEurope / RadioLiberty*, 10 August 2016.
- <sup>38</sup> Jelena Dzombic, "Rightwing Extremism in Serbia," *Race & Class* 55, no.4 (2014): 109.

## 18 COMMUNIST PARTY OF BOHEMIA AND MORAVIA endnotes

- <sup>1</sup> Mediální úsek ÚV KSČM, "Toleranční patent," *KSČM.cz*, 16 July 2018.
- <sup>2</sup> "Respekt: Zeman's People May Influence Issues such as Nuclear Tender," *Prague Daily Monitor*, 6 February 2018.
- <sup>3</sup> Lukáš Onderčánil, "Czech Election also Impacted by Hoaxes: Okamura's Disinformation Gesture," *The Slovak Spectator*, 4 November 2017.
- <sup>4</sup> Leo Luzar, "Mezinárodní bezpečnost a Rada bezpečnosti OSN," *KSČM.cz*, 11 December 2017; "Pokud vláda posílí vojenské mise, KSČM ji nepodpoří," *Novinky.cz*, 12 May 2018.
- <sup>5</sup> Mediální komise Plzeňského KV KSČM, "Nechceme tady americké válečníky!" *KSČM.cz*, 29 May 2018; "Vybudovat socialismus, vystoupit z NATO. KSČM má volební program," *Lidové noviny*, 24 June 2017.
- <sup>6</sup> Lenka Vichová and Roman Máca, *Jak poslanci KSČM na východě Ukrajiny pravdu hledali* (Prague: European Values, 2016).
- <sup>7</sup> *Annual Report of the Security Information Service for 2015* (Prague: Security Information Service, 2016); Robert Břešťan, "Exkluzivní rozhovor s ředitelem české kontrarozvědky BIS. Dezinformace, propaganda a ruský vliv v Česku," *HlidacíPes*, 10 July 2017.
- <sup>8</sup> Jakub Janda, Markéta Blažejovská and Jarkub Vlasák, *Impact of Disinformation Operations in the Czech Republic* (Prague: European Values, 2016); Robert Břešťan, "Exkluzivní rozhovor s ředitelem české kontrarozvědky BIS. Dezinformace, propaganda a ruský vliv v Česku," *HlidacíPes*, 10 July 2017.
- <sup>9</sup> František Vrabel, *How Russia Depicts the Czech Republic: Contextual Content Analysis Based on Big Data from the Internet* (Prague: Semantic Visions, 2016).
- <sup>10</sup> "Czech Government Says Nerve Agent Cited By Zeman Not Novichok," *Radio Free Europe*, 4 May 2018; @Alexey\_Pushkov, Tweet from 3 May 2018 at 12:51 at [https://twitter.com/Alexey\\_Pushkov/status/992129553492570113](https://twitter.com/Alexey_Pushkov/status/992129553492570113)

## 19 BRONZE NIGHT RIOTS endnotes

- <sup>1</sup> Jamie1045, "Pronkssõdur 20.06.2006 miiting," *YouTube Video*, 22 August 2006, <https://www.youtube.com/watch?v=pcZ8P717F2I>
- <sup>2</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 89.
- <sup>3</sup> Christian Lowe, "Russian Protesters 'Lay Siege' to Estonian Embassy," *Reuters*, 3 May 2007.
- <sup>4</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 90.
- <sup>5</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018).
- <sup>6</sup> Gunter Faure and Teresa M. Mensing, *The Estonians: The Long Road to Independence* (n.p., 2012), 293.
- <sup>7</sup> Francis Tapon, "The Bronze Soldier Explains Why Estonia Prepares for a Russian Cyberattack," *Forbes*, 7 July 2018.
- <sup>8</sup> Igor Zevelev, "The Russian World in Moscow's Strategy," *CSIS*, 22 August 2016.
- <sup>9</sup> "Putin in Veiled Attack on Estonia," *BBC News*, 9 May 2007.
- <sup>10</sup> *Ibid.*
- <sup>11</sup> European Parliament, "Debates. CRE 22/05/2007-18, 18. Estonia," European Parliament, 22 May 2007. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070522+ITEM-018+DOC+XML+V0//EN&language=EN>
- <sup>12</sup> "Monument of Contention: How the Bronze Soldier Was Removed," *ERR.ee*, 25 April 2017.
- <sup>13</sup> *Ibid.*
- <sup>14</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 90.
- <sup>15</sup> "Transcript of Remarks and Replies to Media Questions by Russian Minister of Foreign Affairs Sergey Lavrov Following Ministerial Meeting of Russia-NATO Council, Oslo, April 26, 2007," *The Ministry of Foreign Affairs of the Russian Federation*, 27 April 2007.
- <sup>16</sup> Adrian Blomfield, "War of Words over Bronze Soldier," *The Telegraph*, 5 February 2007.
- <sup>17</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 94.
- <sup>18</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 93-94.
- <sup>19</sup> Kaitsepoltseiamet, *Annual Review 2007*, 15.
- <sup>20</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 93.
- <sup>21</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 93.
- <sup>22</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 100.
- <sup>23</sup> "Disquiet in Baltics over Sympathies of Russian Speakers," *Reuters*, 24 March 2014.
- <sup>24</sup> Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 101.
- <sup>25</sup> "Ansiipühistas kohtumise Gerhard Schröderiga" *Eesti Päevaleht*, 30 April 2007.
- <sup>26</sup> Dario Cavegn, "Monument of Contention: How the Bronze Soldier Was Removed," *ERR.ee*, 25 April 2017.
- <sup>27</sup> European Parliament, "European Parliament Resolution of 24 May 2007 on Estonia, P6\_TA(2007)0215," European Parliament, 24 May 2007. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6+TA-2007-0215+0+-DOC+XML+V0//EN&language=EN>
- <sup>28</sup> Hanneli Rudi, "Eesti elanikud usaldavad enim televisiooni," *Postimees*, 13 July 2007.

## 20 RUSSKIY MIR FOUNDATION IN THE BALTICS endnotes

- <sup>1</sup> Vádislava Vojtišková, Vít Novotný, Hubertus Schmid-Schmidfelden and Kristina Potapova, *The Bear in Sheep's Clothing: Russia's Government-Funded Organisations in the EU* (Brussels: Wilfried Martens Centre for European Studies, 2016), 42.
- <sup>2</sup> "About Foundation," *Russkiy Mir Foundation*, website accessed 22 November 2018.
- <sup>3</sup> Andis Kudors, "The 'Russian World' as a Vacuum-Cleaner," *Centre for East European Policy Studies*, 24 March 2014.
- <sup>4</sup> Greg Simons, "Perception of Russia's Soft Power and Influence in the Baltic States," *Public Relations Review* 41, no.1 (2014): 1-13.
- <sup>5</sup> Bertelsmann Stiftung, BTI 2018 Country Report – Latvia (Gütersloh: Bertelsmann Stiftung, 2018).
- <sup>6</sup> Inga Sprunge, Gunita Gailane, and Donata Motuzaite, "Spreading Democracy in Latvia, Kremlin Style," *The Baltic Times*, 21 March 2012.
- <sup>7</sup> "A Survey of Russian Federation Foreign Policy," *Ministry of Foreign Affairs of the Russian Federation*, 2007.
- <sup>8</sup> Ambiguous Threats and External Influences in the Baltic States, Asymmetric Operations Working Group, November 2015.
- <sup>9</sup> Andrew Foxall, The Kremlin's Sleight of Hand: Russia's Soft Power Offensive in the UK, Henry Jackson Society Russia Studies Centre, *Policy Paper* No.3, February 2015.
- <sup>10</sup> Vera Zakem, Paul Saunders and Daniel Antoun, Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union (CNA, 2015).
- <sup>11</sup> As an example, Russian ambassador opens RMF centre in Daugavpils: Natalia Petrova, "Открывшийся сегодня в Даугавпилсе Центр Русского языка и культуры будет доступен всем горожанам," *Gorod.lv*, 26 March 2010.
- <sup>12</sup> Nina Kolzako, "Putin's 'Russkiy Mir' Spent over EUR 170,000 on Supporting Compatriots in Latvia," *The Baltic Course*, 22 March 2012.
- <sup>13</sup> "Immortal Regiment Campaign in Europe," *Russkiy Mir Foundation*, 9 May 2016.
- <sup>14</sup> Taken from the various security policies from the Baltic states.
- <sup>15</sup> Central Statistical Bureau of Latvia, "Iedzīvotāju skaits Latvijā turpina samazināties, Rīgā vērojams pieaugums," 30 May 2017.
- <sup>16</sup> Statistics Estonia, "Minifacts about Estonia 2017", June 2017, 12.
- <sup>17</sup> Latvijas Fakti, "Latvijas iedzīvotāju medijpratība: kvantitatīvais pētījums", June 2017, 7, 12-13.
- <sup>18</sup> LETA, "Septembrī visskatītākais TV kanāls Latvijā bija TV3," TVNet, 11 October 2017; "Teledaudzskatītāji vēroja septembrikuus 2017," *KantarEmor*, 11 October 2017.
- <sup>19</sup> See for example: Ammon Cheskin, "Identity and Integration of Russian Speakers in the Baltic States: A Framework for Analysis," *Ethnopolitics* 14, no. 1 (2015): 72-93.

## 21 CRIMINAL NETWORKS IN THE DONBAS endnotes

- <sup>1</sup> Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe," *European Council on Foreign Relations*, 18 April 2017.
- <sup>2</sup> "Anti-Corruption Glossary: Grand Corruption," *Transparency International*, website accessed 26 February 2018.
- <sup>3</sup> "A Year after Maidan, Ukraine Is Still the Most Corrupt Country in Europe," *Transparency International*, 3 December 2014.
- <sup>4</sup> Maria Romanenko, "UPDATED: Ukraine's Interior Minister's Son Released Pending Trial," *Hromadske International*, 31 October 2017.
- <sup>5</sup> "Ukraine's Yanukovich Wanted for Embezzlement: Interpol," *Reuters*, 12 January 2015.
- <sup>6</sup> "Ukraine's Senior Defense Officials Detained on Charges of UAH 149 Mln Embezzlement," *UNIAN*, 11 October 2017.
- <sup>7</sup> Conny Abel, Svetlana Savitskaya and Valentina Rigamonti, "Europe and Central Asia: An Overall Stagnation," *Transparency International*, 25 January 2017.
- <sup>8</sup> Taras Kuzio, *Ukraine: Democratization, Corruption, and the New Russian Imperialism* (Santa Barbara, CA: Praeger Security International, 2015), 412.
- <sup>9</sup> Taras Kuzio, *Ukraine: Democratization, Corruption, and the New Russian Imperialism* (Santa Barbara, CA: Praeger Security International, 2015), 412.
- <sup>10</sup> Michael Bird, Lina Vdovii and Yana Tkachenko, "The Donbass Paradox," *The Black Sea*, n.d., accessed 27 February 2018.
- <sup>11</sup> Jack Losh, "How Ukraine's War Became Big Business for the Underworld," *VICE News*, 22 February 2016.
- <sup>12</sup> "Fundamental Principles of the Activities," *Security Service of Ukraine*, website accessed 27 February 2018.
- <sup>13</sup> "Actions and Principles of Operation," *National Anti-Corruption Bureau of Ukraine*, website accessed 27 February 2018.
- <sup>14</sup> "FAQ," *National Anti-Corruption Bureau of Ukraine*, website accessed 27 February 2018.
- <sup>15</sup> "Breaking Down the Surkov Leaks," *The Atlantic Council - Digital Forensic Research Lab*, 25 October 2016.
- <sup>16</sup> "Moscow's Man on Minsk," *The Atlantic Council - Digital Forensic Research Lab*, 1 September 2017.
- <sup>17</sup> "Rinat Akhmetov," *Forbes*, website accessed 27 February 2018.
- <sup>18</sup> Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, Lessons from Russia's Operations in Crimea and Eastern Ukraine. Santa Monica, CA: RAND Corporation, 2017. [https://www.rand.org/pubs/research\\_reports/RR1498.html](https://www.rand.org/pubs/research_reports/RR1498.html).
- <sup>19</sup> Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, Lessons from Russia's Operations in Crimea and Eastern Ukraine. Santa Monica, CA: RAND Corporation, 2017. [https://www.rand.org/pubs/research\\_reports/RR1498.html](https://www.rand.org/pubs/research_reports/RR1498.html).
- <sup>20</sup> Vlad Lavrov and Yuriy Onyshkov, "EU Hope Fade as Gas Lobby Triumphs," *Kyiv Post*, 16 December 2011.
- <sup>21</sup> Vitalii Rybak, "Yes, Ukraine's Oligarchs Own the Airwaves, but Their Days Are Numbered," *Atlantic Council*, 29 January 2018.
- <sup>22</sup> Illia Ponomarenko, "Secrecy Blankets Corruption in Ukraine's Defense Sector," *Kyiv Post*, 15 September 2017.
- <sup>23</sup> Askold Krushelnysky, "Ukraine's Anti-Corruption Agency Alleges Fraud in Arms Industry," *Foreign Policy*, 21 December 2017.
- <sup>24</sup> "TOP 5 Ukrainian Oligarchs and their Impact on the Economy," *Ukraine Crisis Media Center*, 6 April 2017.
- <sup>25</sup> Christopher Miller, "Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies," *Mashable*, 30 December 2014.
- <sup>26</sup> "Ukraine Arrests Official Who Doubled as 'Agent of Russian Intelligence,'" *Deutsche Welle*, 21 December 2017.
- <sup>27</sup> "8 Thousand Ukrainian Officers Have Defected to the Separatists," *Meduza*, 14 August 2015.
- <sup>28</sup> *Ukraine 2020 – Policy Dialogue: Supporting Ukraine's European Integration* (Kyiv and Washington, D.C.: U.S.-Ukraine Foundation, 2012).
- <sup>29</sup> Taras Kuzio, "Ukraine's Relations with the West since the Orange Revolution," *European Security* 21, no.3 (2012): 395-413.
- <sup>30</sup> Andrew Higgins, "In Ukraine, Corruption Is Now Undermining the Military," *The New York Times*, 19 February 2018.
- <sup>31</sup> "Poll Shows Most Ukrainians Consider Fight against Corruption Unsuccessful," *Kyiv Post*, 12 January 2018.

## 22 CIVIL DISORDER IN BAHRAIN 2011 endnotes

- <sup>1</sup> Ahmed K. Al-Rawi, "Sectarianism and the Arab Spring: Framing the Popular Protests in Bahrain," *Global Media and Communication* 11, no.1 (2015): 25-42.
- <sup>2</sup> PBS News Hour, "Bahrain's Foreign Minister: We Haven't Been 'Acting as Complete Angels,'" 18 May 2011, <https://www.youtube.com/watch?v=T2ljl5zDVM>.
- <sup>3</sup> Bahrain Independent Commission of Inquiry, "Report of the Bahrain Independent Commission of Inquiry," 23 November 2011.
- <sup>4</sup> Simon Mabon, "The Battle for Bahrain: Iranian-Saudi Rivalry," *Middle East Policy Council*, Summer 2012.
- <sup>5</sup> Bahrain Independent Commission of Inquiry, "Report of the Bahrain Independent Commission of Inquiry," 23 November 2011, 289-396.
- <sup>6</sup> Ibid.
- <sup>7</sup> Mohamad A. Al Khalifa, *Bahrain-Iran Relations in Modern Times* (Monterey, CA: Naval Postgraduate School / Master's thesis, September 2014).
- <sup>8</sup> Simon Mabon, "The Battle for Bahrain: Iranian-Saudi Rivalry," *Middle East Policy Council*, Summer 2012.
- <sup>9</sup> "State Department Terrorist Designations of Ahmad Hasan Yusuf and Alsayed Murtadha Majeed Ramadhan Alawi," *US Department of State*, 17 March 2017.
- <sup>10</sup> "Bahrain's King Makes Veiled Charge against Iran," *Independent*, 21 March 2011.
- <sup>11</sup> "Iran Censures Brutality of 4 Arab States," *Press TV*, 23 February 2011.
- <sup>12</sup> "Iran Recalls Ambassador from Bahrain in Protest," *CBS News*, 17 March 2011.
- <sup>13</sup> Gus Lubin, "Iran Will Respond With 'All Power And Potentials At Its Disposal To Halt The Oppression Of The People Of Bahrain,'" *Business Insider*, 17 March 2011.
- <sup>14</sup> "Bahrain: Gulf Troops Needed Against Iran Threat," *VOA*, 17 April 2011.
- <sup>15</sup> Firouz Sedarat, "Satellite TV News, Serials Widen Iranian-Arab Gulf," *Reuters*, 14 December 2011.
- <sup>16</sup> Sebastian Usher, "Iran's Leaders Harness Media Power," *BBC News*, 14 March 2006.
- <sup>17</sup> National Action Charter translated in: Sayel F. Al-Serhan, Ahed A. Mashagbeh, and Mohammed Bani Salameh, "Challenges Facing National Security in the Arab Gulf States: A Case Study of Bahrain," *International Journal of Humanities and Social Science* 7, no.12 (December 2017).
- <sup>18</sup> Jane Kinninmont, *Bahrain: Beyond the Impasse* (London: Chatham House/Royal Institute of International Affairs, 14 March 2006).
- <sup>19</sup> Ibid.
- <sup>20</sup> "Interior Minister: People Have Greater Trust in Our Security Abilities," *Bahrain News Agency*, 25 November 2015.

## 23 PAKISTANI INVOLVEMENT IN YEMEN endnotes

- <sup>1</sup> Jon Boone and Saeed Kamali Dehghan, "Pakistan's Parliament Votes against Entering Yemen Conflict," *The Guardian*, 10 April 2015.
- <sup>2</sup> Louis Ritzinger, "Why Pakistan Is Staying Out of Yemen," *National Interest*, 27 April 2015.
- <sup>3</sup> Jack Detsch, "China's Grand Plan for Pakistan's Infrastructure," *The Diplomat*, 21 April 2015.
- <sup>4</sup> Asad Hashim, "Pakistan Tight-Lipped on Saudi Arabia Troop Mission," *Al Jazeera*, 22 February 2018.
- <sup>5</sup> Khalid Iqbal, "Yemen Crisis and Pakistan: A Holistic View," in *Policy Perspectives* 12, no. 2 (2015): 76.
- <sup>6</sup> Mohammad Mukashaf, "Pakistan Declines Saudi Call for Armed Support in Yemen Fight," *Reuters*, 10 April 2015.
- <sup>7</sup> Mohammad Mukashaf, "Pakistan Declines Saudi Call for Armed Support in Yemen Fight," *Reuters*, 10 April 2015.
- <sup>8</sup> "Putting the Brakes On," *Express Tribune*, 2 April 2015.
- <sup>9</sup> Asad Hashim, "Pakistan Debates Military Involvement in Yemen," *Al Jazeera*, 6 April 2015.
- <sup>10</sup> Jon Boone and Saeed Kamali Dehghan, "Pakistan's Parliament Votes against Entering Yemen Conflict," *The Guardian*, 10 April 2015.
- <sup>11</sup> Farheen Rizvi, "Why Pakistan Will Fight Saudi's Wars but Not Its Own," *Huffington Post*, 31 March 2015.
- <sup>12</sup> Asad Hashim, "Pakistan Debates Military Involvement in Yemen," *Al Jazeera*, 6 April 2015.
- <sup>13</sup> "Pakistan Struggles to Balance Saudi, Iran Ties in Tense Middle East," *World Politics Review*, 16 March 2016.
- <sup>14</sup> Sameer Lalwani, "Will Pakistan Draw Closer to Saudi Arabia to Balance Iran?" *War on the Rocks*, 24 February 2016.
- <sup>15</sup> Ayesha Tanzeem, "Pakistan Walks Tightrope Over Yemen Crisis," *Voice of America*, 2 April 2015.
- <sup>16</sup> "The China-Pakistan Economic Corridor," *Al Jazeera*, 4 May 2015.

## 24 OPERATION PARAKRAM endnotes

- <sup>1</sup> S. Kalyanaraman, "Operation Parakram: An Indian Exercise in Coercive Diplomacy," *Strategic Analysis* 26, no. 4(2002): 478-92; V.K. Sood and Pravin Sawhney, *Operation Parakram: The War Unfinished* (New Delhi: Sage, 2003), 51-103.
- <sup>2</sup> Walter Ladwig, "A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine," *International Security* 32, no.3 (Winter 2007-2008): 158-90.
- <sup>3</sup> Ahmed Rashid, *Descent into Chaos: The U.S. and the Disaster in Pakistan, Afghanistan, and Central Asia* (New York: Penguin, 2009): 116.
- <sup>4</sup> Patrick Bratton, "Signals and Orchestration: India's Use of Compellence in the 2001-02 Crisis," *Strategic Analysis* 34, no.4 (2010): 605.
- <sup>5</sup> Sumit Ganguly and Devin T. Hagerty, *Fearful Symmetry: India-Pakistan Crises in the Shadow of Nuclear Weapons* (Seattle, WA: University of Washington Press, 2005), 168, 171.
- <sup>6</sup> Patrick Bratton, "Signals and Orchestration: India's Use of Compellence in the 2001-02 Crisis," *Strategic Analysis* 34, no.4 (2010): 605.  
Sumit Ganguly and Devin T. Hagerty, *Fearful Symmetry: India-Pakistan Crises in the Shadow of Nuclear Weapons* (Seattle, WA: University of Washington Press, 2005), 168, 171.
- <sup>7</sup> S. Kalyanaraman, "Operation Parakram: An Indian Exercise in Coercive Diplomacy," *Strategic Analysis* 26, no. 4(2002): 478-92.
- <sup>8</sup> Press Trust Of India, "Op Parakram Most Punishing Mistake: Ex-Navy Chief," *The Indian Express* (Archive), 5 November 2011.
- <sup>9</sup> Patrick Bratton, "Signals and Orchestration: India's Use of Compellence in the 2001-02 Crisis," *Strategic Analysis* 34, no.4 (2010): 605.
- <sup>10</sup> Patrick Bratton, "Signals and Orchestration: India's Use of Compellence in the 2001-02 Crisis," *Strategic Analysis* 34, no.4 (2010): 605.
- <sup>11</sup> "The Indian Military Doctrine – The Sundarji Doctrine," SS24, 11 September 2013.
- <sup>12</sup> Francisco Aguilar, Randy Bell, Natalie Black, Sayce Falk, Sasha Rogers, Aki J. Peritz, *An Introduction to Pakistan's Military* (Cambridge, MA: Belfer Center for Science and International Affairs, 2011), 8.
- <sup>13</sup> S. Paul Kapur, "Ten Years of Instability in a Nuclear South Asia," *International Security* 33, no.2 (2008), 73.
- <sup>14</sup> Narendra Kumar, *Pakistan: A Military Challenge in the Backdrop of Nuclear Symmetry* (New Delhi: Centre for Land Warfare Studies, 2011), 2.
- <sup>15</sup> Ahmed Rashid, *Descent into Chaos: The U.S. and the Disaster in Pakistan, Afghanistan, and Central Asia* (New York: Penguin, 2009): 116.
- <sup>16</sup> Rajesh M. Basrur, "The Lessons of Kargil as Learned by India," in: *Asymmetric Warfare in South Asia: The Causes and Consequences of the Kargil Conflict*, edited by Peter R. Lavoy, (Cambridge: Cambridge UP, 2009), 326; Ahmed Rashid, *Descent into Chaos: The U.S. and the Disaster in Pakistan, Afghanistan, and Central Asia* (New York: Penguin, 2009): 116.; "2001-02 India-Pakistan Standoff," *Revolvey*, accessed 7 October 2017; Sharad Joshi, *The Practice of Coercive Diplomacy in the Post-9/11 Period*, Graduate School of Public and International Affairs in partial fulfillment for the degree of Doctor of Philosophy, *University of Pittsburgh*, 2006, 53.
- <sup>17</sup> Sharad Joshi, *The Practice of Coercive Diplomacy in the Post-9/11 Period*, Graduate School of Public and International Affairs in partial fulfillment for the degree of Doctor of Philosophy, *University of Pittsburgh*, 2006, 55.
- <sup>18</sup> Quinn J. Rhodes, *Limited War under the Nuclear Umbrella: An Analysis of India's Cold Start Doctrine and its Implications for Stability on the Subcontinent* (Monterey, CA: Naval Postgraduate School, 2010), 20.
- <sup>19</sup> George Fernandes, "The Dynamics of Limited War," Inaugural address of Defence Minister George Fernandes at the national seminar on 'The Challenges of Limited War: Parameters and Option' organised by the Institute of Defence Studies & Analyses, New Delhi, *Strategic Affairs*, 1-15 October 2000.

- <sup>20</sup> "Parliament Attack: Advani Points towards Neighbouring Country," *Rediff*, 14 December 2001.
- <sup>21</sup> "Pakistan, India 'Move Missiles' to Border," *CNN*, 26 December 2001.
- <sup>22</sup> "Pakistan, India 'Move Missiles' to Border," *CNN*, 26 December 2001.
- <sup>23</sup> Sarah Left, "Indian PM Calls for 'Decisive Battle' over Kashmir," *The Guardian*, 22 May 2002.
- <sup>24</sup> "Pakistan, India 'Move Missiles' to Border," *CNN*, 26 December 2001.
- <sup>25</sup> Ahmed Rashid, *Descent into Chaos: The U.S. and the Disaster in Pakistan, Afghanistan, and Central Asia* (New York: *Penguin*, 2009): 116.
- <sup>26</sup> Atul Aneja, "G-8 Informed of New Delhi Viewpoint," *The Hindu*, 30 December 2001.
- <sup>27</sup> Rajesh M. Basrur, "К вопросу о ядерной доктрине Индии," *Ядерный контроль* 75, no.1 (2005).
- <sup>28</sup> "The Indian Military Doctrine – The Sundarji Doctrine," *SS24*, 11 September 2013.
- <sup>29</sup> "2002 – Kashmir Crisis," *Global Security*, accessed 15 September 2017.
- <sup>30</sup> Stephen Burgess, "Pakistan's Security Dilemma and Quest for Strategic Stability," in: *Strategic Stability in Asia*, edited by Amit Gupta (London: *Routledge*, 2008), 133.
- <sup>31</sup> Francisco Aguilar, Randy Bell, Natalie Black, Sayce Falk, Sasha Rogers, Aki J. Peritz, *An Introduction to Pakistan's Military* (Cambridge, MA: *Belfer Center for Science and International Affairs*, 2011), 20.
- <sup>32</sup> Amit Gupta, "The Reformist State: The Indian Security Dilemma," in: *Strategic Stability in Asia*, edited by Amit Gupta (London: *Routledge*, 2008), 115.
- <sup>33</sup> *Ibid.* 13-5.
- <sup>34</sup> *Ibid.* 15-6.
- <sup>35</sup> Amit Gupta, "The Reformist State: The Indian Security Dilemma," in: *Strategic Stability in Asia*, edited by Amit Gupta (London: *Routledge*, 2008), 121.
- <sup>36</sup> Stephen Burgess, "Pakistan's Security Dilemma and Quest for Strategic Stability," in: *Strategic Stability in Asia*, edited by Amit Gupta (London: *Routledge*, 2008), 127.
- <sup>37</sup> Sajad Padder, *The Composite Dialogue between India and Pakistan: Structure, Process and Agency*, Working Paper No. 65, South Asia Institute, Department of Political Science, *Heidelberg University*, 2012, 10.
- <sup>38</sup> Rob Johnson, *A Region in Turmoil: South Asian Conflicts since 1947* (London: *Reaktion*, 2005), 27-35.
- <sup>39</sup> Francisco Aguilar, Randy Bell, Natalie Black, Sayce Falk, Sasha Rogers, Aki J. Peritz, *An Introduction to Pakistan's Military* (Cambridge, MA: *Belfer Center for Science and International Affairs*, 2011), 8.
- <sup>40</sup> T.V. Paul, "Causes of the India-Pakistan Rivalry," in: *The India-Pakistan Conflict: An enduring Rivalry*, edited by T.V. Paul (Cambridge: *Cambridge UP*, 2005), 5.
- <sup>41</sup> "Comparison Results of World Military Strengths," *Global Fire Power*, accessed 25 October 2017; Francisco Aguilar, Randy Bell, Natalie Black, Sayce Falk, Sasha Rogers, Aki J. Peritz, *An Introduction to Pakistan's Military* (Cambridge, MA: *Belfer Center for Science and International Affairs*, 2011), 32.
- <sup>42</sup> Aditi Phadnis, "Parakram Cost Put at Rs 6,500 Crore," *Rediff*, 16 January 2003.
- <sup>43</sup> S. Kalyanaraman, "Operation Parakram: An Indian Exercise in Coercive Diplomacy," *Strategic Analysis* 26, no. 4(2002): 478-82; M.S. Zaitsev, "Military Strategy of India," *MGIMO Review of International Relations* 53, no.2 (2017): 55.
- <sup>44</sup> T.V. Paul, "Causes of the India-Pakistan Rivalry," in: *The India-Pakistan Conflict: An enduring Rivalry*, edited by T.V. Paul (Cambridge: *Cambridge UP*, 2005), 16.
- <sup>45</sup> Muhammad Umer, "The Hot Reality of Cold Start," *The News*, 19 April 2016.
- <sup>46</sup> T.V. Paul, "Causes of the India-Pakistan Rivalry," in: *The India-Pakistan Conflict: An enduring Rivalry*, edited by T.V. Paul (Cambridge: *Cambridge UP*, 2005), 16.

## 25 SNAP EXERCISES AND CRIMEA endnotes

- <sup>1</sup> Johan Norberg, "The Use of Russia's Military in the Crimean Crisis," *Carnegie Endowment for International Peace*, 13 March 2014.
- <sup>2</sup> *Ibid.*
- <sup>3</sup> Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: *RAND*, 2017), 24.
- <sup>4</sup> *Ibid.*
- <sup>5</sup> Ewan MacAskill, "Putin's Military Exercises Are More Than a Game," *The Guardian*, 23 April 2014.
- <sup>6</sup> Lucy Ash, "How Russia Outfoxes Its Enemies," *BBC News*, 29 January 2015.
- <sup>7</sup> Hannah Strange and Roland Oliphant, "Ukraine Revolution: 150,000 Russian Troops on Alert as US Warns Putin," *The Telegraph*, 26 February 2014.
- <sup>8</sup> Morgan Maier, *A Little Masquerade: Russia's Evolving Employment of Maskirovka* (Fort Leavenworth, KS: *US Army Command and General Staff College*, 2016), 10-11.
- <sup>9</sup> Organization for Security and Co-operation in Europe (OSCE), *Vienna Document 2011 on Confidence and Security-Building Measures*, 30 November 2011.
- <sup>10</sup> Rüdiger Lütkeking, "Military Confidence-Building and Conventional Arms Control in Europe against the Background of the Ukraine Crisis," in: *OSCE Yearbook 2014* (Baden-Baden: *Nomos*, 2015), 275-82.
- <sup>11</sup> Steve Gutterman, "Putin Puts Troops in Western Russia on Alert in Drill," *Reuters*, 26 February 2014.
- <sup>12</sup> Hannah Strange and Roland Oliphant, "Ukraine Revolution: 150,000 Russian Troops on Alert as US Warns Putin," *The Telegraph*, 26 February 2014.
- <sup>13</sup> "Вимагаємо від Уряду Росії негайно відкликати свої війська з Криму, - А.Яценюк," *Ukraine Government Portal*, 1 March 2014.
- <sup>14</sup> Claire Phipps and Ben Quinn, "Ukraine Pulls Forces out of Crimea as Russia Takes over Military Bases," *The Guardian*, 24 March 2014.
- <sup>15</sup> Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: *RAND*, 2017), 24.
- <sup>16</sup> Roy Allison, "Russian 'Deniable' Intervention in Ukraine: How and Why Russia Broke the Rules," *International Affairs* 90, no.6 (2014): 1258.
- <sup>17</sup> Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: *RAND*, 2017), 24.
- <sup>18</sup> National Security Strategy of Ukraine 2007, as updated in 2012. Ukrainian version: <http://zakon0.rada.gov.ua/laws/show/389/2012/paran18#n18>

## 26 ELECTRONIC WARFARE DURING ZAPAD 2017 endnotes

- <sup>1</sup> "Raidjums: Kurzemē novērotos mobilo sakaru traucējumus, iespējams, radījis Krievijas ierīce," *Diena*, 8 October 2017.
- <sup>2</sup> "Russians Jammed Flights/GPS," *NewsInEnglish.no*, 6 October 2017.
- <sup>3</sup> "Iekšlietu ministrija: Numura 112 traucējumi nebija saistīti ar mācībām Zapad," *Diena*, 6 October 2017.
- <sup>4</sup> Aaron Mehta, "Lessons from Zapad – Jamming, NATO and the Future of Belarus," *DefenseNews*, 22 November 2017.
- <sup>5</sup> "Elektroniskais karš – vai esam gatavi? "Zapad-2017" mācības," *Latvijas Avīze*, 28 October 2017.
- <sup>6</sup> Daniel Brown, "Russian-Backed Separatists Are Using Terrifying Text Messages to Shock Adversaries - and It's Changing the Face of Warfare," *BusinessInsider*, 14 August 2018.
- <sup>7</sup> Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025* (Tallinn: International Centre for Defence and Security / Estonian Ministry of Defence, 2017).
- <sup>8</sup> Matthieu Boulègue, "Five Things to Know About the Zapad-2017 Military Exercise," *Chatham House*, 25 September 2017.
- <sup>9</sup> Gederts Gelzis and Robin Emmott, "Russia May Have Tested Cyber Warfare on Latvia, Western Officials Say," *Reuters*, 5 October 2017.
- <sup>10</sup> Jonathan Marcus, "Zapad: What Can We Learn from Russia's Latest Military Exercise?" *BBC News*, 20 September 2017.
- <sup>11</sup> Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025* (Tallinn: International Centre for Defence and Security / Estonian Ministry of Defence, 2017).
- <sup>12</sup> Joseph Trevithick, "Russia Jammed Phones and GPS in Northern Europe during Massive Military Drills," *The Drive*, 16 October 2017.
- <sup>13</sup> "State Secretary: Latvia Should Not Panic Too Much about Zapad 2017," *Baltic News Network*, 13 September 2017.

- <sup>14</sup> Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025* (Tallinn: International Centre for Defence and Security / Estonian Ministry of Defence, 2017).
- <sup>15</sup> Ministry of Defence of the Republic of Latvia, *The National Security Concept (informative section)*, 2015, 6.
- <sup>16</sup> Samuel Bendett, "America Is Getting Outclassed by Russian Electronic Warfare," *The National Interest*, 19 September 2017.
- <sup>17</sup> Heather A. Conley, Jeffrey Rathke and Matthew Melino, *Enhanced Deterrence in the North: A 21st Century European Engagement Strategy* (Washington, D.C.: CSIS, February 2018), 15.

- <sup>18</sup> Anders Puck Nielsen, "Jamming of Phones and GPS During Zapad Causes Concerns," *Romeo Squared*, 27 October 2017.
- <sup>19</sup> Andrew Metrick and Kathleen H. Hicks, *Contested Seas: Maritime Domain Awareness in Northern Europe* (Washington, D.C.: CSIS, 2018), 8.
- <sup>20</sup> Joseph Trevithick, "Russia Jammed Phones and GPS in Northern Europe during Massive Military Drills," *The Drive*, 16 October 2017.
- <sup>21</sup> Aaron Mehta, "Lessons from Zapad – Jamming, NATO and the Future of Belarus," *DefenseNews*, 22 November 2017.

## 27 RUSSIAN ESPIONAGE IN SWEDEN endnotes

- <sup>1</sup> Anna Ringstrom, "Sweden Security Forces Fear Russian Military Operations," *Reuters*, 18 March 2015.
- <sup>2</sup> Alistair Scrutton, "Swedish Spy Chief Warns of Rise of Islamist Threat," *Reuters*, 27 May 2014.
- <sup>3</sup> Justin Wise, "US Suspected Russia Was behind 2016 Cyberattacks against Swedish News Organizations: Report," *The Hill*, 10 August 2018.
- <sup>4</sup> SÄPO annual reports, available via: <http://www.sakerhetspolisen.se/en/swedish-security-service/reports.html>
- <sup>5</sup> "Foreign Intelligence Services' Modus Operandi," *Säkerhetspolisen*, website accessed on 7 August 2018.
- <sup>6</sup> Erica Larsson, Ellika Nilsson and Andreas Liebermann, "'Misstänkt ryskt spionage ökar i norra Sverige," *SVT Nyheter*, 20 September 2016.
- <sup>7</sup> "Försvarsministern: 'Spioneri är en realitet'," *SVT Nyheter*, 20 September 2016.
- <sup>8</sup> Margot Wallström, "The Government's Statement of Foreign Policy 2018," *Government of Sweden*, 14 February 2018.
- <sup>9</sup> Niklas Pollard, "Sweden Steps Up Hunt for 'Foreign Underwater Activity'," *Reuters*, 18 October 2014.
- <sup>10</sup> "Sabotaget i Häglared – ny podcast från BT dokumentär," *Borås Tidning*, 6 May 2018.
- <sup>11</sup> Naomi Lubick, "Sweden Expels Russian Research Plane Amid Spying Concerns," *Science / AAAS*, 24 May 2016.
- <sup>12</sup> Erica Larsson, Ellika Nilsson and Andreas Liebermann, "'Misstänkt ryskt spionage ökar i norra Sverige," *SVT Nyheter*, 20 September 2016.
- <sup>13</sup> "Främmande dykarfarkost kan ha kränkt Sverige i Gävle hamn," *Dagens Nyheter*, 25 September 2017.
- <sup>14</sup> "Misstänkt spioneri i stor skala mot militärövningen Aurora," *Dagens Nyheter*, 12 October 2017.
- <sup>15</sup> "Russia Says Military Neutrality of Sweden, Finland Is Crucial for Security," *RadioFreeEurope / RadioLiberty*, 21 February 2017.
- <sup>16</sup> Swedish Security Service, "Årsrapport 2014," 2014.
- <sup>17</sup> "Säpo: Total ryska agenter i Sverige," *Aftonbladet*, 17 March 2016.
- <sup>18</sup> Tomas Hirst, "Russia Tells Sweden that Hunting for Its Submarines is a 'Mindless Waste of Swedish Taxpayer Money'," *Business Insider*, 14 April 2015.
- <sup>19</sup> "Misstänker ryskt spionage mot norra Sverige," *Norrbattenskuriren*, 20 September 2016.
- <sup>20</sup> "Misstänkt spioneri i stor skala mot militärövningen Aurora," *Dagens Nyheter*, 12 October 2017.
- <sup>21</sup> "Okända flygfarkoster dök upp vid nattlig militärövning," *Dagens Nyheter*, 4 July 2016.
- <sup>22</sup> Hans Nilsson, "Misstänkt spionage mot flygbasen i Hagshult," *Värnamo Nyheter*, 16 September 2016; Claes Carlson, "Experten varnar för terror-spioneri," *Expressen*, 14 September 2016.
- <sup>23</sup> "Misstänkt spioneri i stor skala mot militärövningen Aurora," *Dagens Nyheter*, 12 October 2017.
- <sup>24</sup> "Säpo: Suspected Spies Found Working in Swedish Agencies," *Swedish Radio*, 16 March 2017.
- <sup>25</sup> "Säpo: 'Omfattande' ryskt spionage," *Ny Teknik*, 18 March 2015.
- <sup>26</sup> Jani Pirttialo Sallinen, "Säpo varnar myndigheter för 'outsourcing' utomlands," *Svenska Dagbladet*, 17 March 2016.
- <sup>27</sup> Gerald O'Dwyer, "Sweden Steps Up Cyber Defence Measures," *Computer Weekly*, 8 January 2018.
- <sup>28</sup> "Two Swedish Diplomats to Be Expelled from Russia: Reports," *The Local*, 28 November 2017.

## 28 RELIGIOUS EXTREMISM IN THE NETHERLANDS endnotes

- <sup>1</sup> "Saudi Influences in the Netherlands: Links between the Salafist Mission, Radicalisation Processes and Islamic Terrorism," *AIVD*, 6 January 2005.
- <sup>2</sup> Beatrice De Graaf, "The Nexus between Salafism and Jihadism in the Netherlands," in *CTC Sentinel* 3, no.3 (March 2010): 17-22.
- <sup>3</sup> AIVD, "Annual Report 2017."
- <sup>4</sup> AIVD, "The Transformation of Jihadism in the Netherlands: Swarm Dynamics and New Strength," September 2014, 46.
- <sup>5</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015, 7.
- <sup>6</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015, 7.
- <sup>7</sup> "Measures to Combat Financial Flows from Countries that are Not Free," Government of the Netherlands, 29 March 2018.
- <sup>8</sup> "Measures to Combat Financial Flows from Countries that are Not Free," Government of the Netherlands, 29 March 2018.
- <sup>9</sup> Milena Holdert, "Geheime lijsten financiering moskeeën onthuld," Nederlandse Omroep Stichting, 23 April 2018.
- <sup>10</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015.
- <sup>11</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015, 7.
- <sup>12</sup> Centraal Bureau voor de Statistiek, "Helft Nederlanders is Kerkelijk of Religieus," 22 December 2016.
- <sup>13</sup> Yoram Stein, "Salafisten geen gevaar? Lees je eigen rapport!" NRC, 30 September 2010.
- <sup>14</sup> Milena Holdert, "Geheime lijsten financiering moskeeën onthuld," Nederlandse Omroep Stichting, 23 April 2018.
- <sup>15</sup> AIVD, "Right-Wing-Extremism and the Extreme Right in the Netherlands," 11 July 2011.
- <sup>16</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015.
- <sup>17</sup> *Ibid.*
- <sup>18</sup> AIVD, "Annual Report 2015."
- <sup>19</sup> "30 Islamic Organisations in NL Have Requested Funding from Kuwait, Saudi Arabia," *Dutch News*, 24 April 2018.
- <sup>20</sup> *Ibid.*
- <sup>21</sup> Peter Mandaville and Shadi Hamid, *Islam as Statecraft: How Governments Use Religion in Foreign Policy* (Washington, D.C.: Brookings, November 2018).
- <sup>22</sup> Milena Holdert, "Geheime lijsten financiering moskeeën onthuld," Nederlandse Omroep Stichting, 23 April 2018.
- <sup>23</sup> AIVD, "Saudi Influences in the Netherlands," 2005.
- <sup>24</sup> AIVD, "De democratische rechtsorde en islamitisch onderwijs: buitenlandse invulling en anti-integratieve tendensen," February 2002.
- <sup>25</sup> AIVD and NCTV, "Salafism in the Netherlands: Diversity and Dynamics," 2015, 7.
- <sup>26</sup> Shervin Nekuee, "Het probleem is niet de islam, maar wahabisme," NRC, 27 January 2015.
- <sup>27</sup> Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "Uitreizigers, terugkeerders en thuisblijvers," 9 November 2017.
- <sup>28</sup> Marcel Wiegman, "Spanningen leiden tot geweld in moskee in Nieuw-West," 21 November 2018.

## 29 CYBER ATTACKS ON ROK & US endnotes

- <sup>1</sup> Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, 9 July 2009.
- <sup>2</sup> Confirmed by the South Korean National Intelligence Service. "N. Korean Ministry Behind July Cyber Attacks: Spy Chief," *Yonhap News Agency*, 30 October 2009.
- <sup>3</sup> Ju-min Park, "Exclusive: North Korea's Unit 180, the Cyber Warfare Cell that Worries the West," *Reuters*, 21 May 2017.
- <sup>4</sup> James Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict," *Center for Strategic and International Studies*, October 2009.
- <sup>5</sup> Jennifer Epstein, "Report: N. Korea behind cyberattack," *POLITICO*, 5 July 2011.
- <sup>6</sup> Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, 9 July 2009.
- <sup>7</sup> Jenny Jun, Scott LaFoy and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," *Center for Strategic and International Studies*, 2015.
- <sup>8</sup> Jenny Jun, Scott LaFoy and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," *Center for Strategic and International Studies*, 2015.
- <sup>9</sup> Adam Albarado, *When Norms Fail: North Korea and Cyber as an Element of Statecraft* (Montgomery, AL: Air War College, 2017), 22.
- <sup>10</sup> Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, 9 July 2009; Matthew Shaer, "North Korean Hackers Blamed for Sweeping Cyber Attack on US Networks," *The Christian Science Monitor*, 8 July 2009.
- <sup>11</sup> Jam Kim, "More Web attacks, North Korea Suspected," *Reuters*, 9 July 2009.
- <sup>12</sup> "Governments Hit by Cyber Attack," *BBC*, 8 July 2009.
- <sup>13</sup> David E. Sanger, David D. Kirkpatrick and Nicole Perloth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, 15 October 2017.
- <sup>14</sup> "North Korea Launched Cyber Attacks, Says South," *The Guardian*, 11 July 2009.
- <sup>15</sup> Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, 9 July 2009; Matthew Shaer, "North Korean Hackers Blamed for Sweeping Cyber Attack on US Networks," *The Christian Science Monitor*, 8 July 2009.
- <sup>16</sup> "Governments Hit by Cyber Attack," *BBC*, 8 July 2009.
- <sup>17</sup> "North Korea Launched Cyber Attacks, Says South," *The Guardian*, 11 July 2009.
- <sup>18</sup> Ian Kelly, "Daily Press Briefing - July 9," *US Department of State*, 9 July 2009.
- <sup>19</sup> "U.S. Eyes N. Korea for 'Massive' Cyber Attacks," *MSNBC*, 7 July 2009.
- <sup>20</sup> Ian Kelly, "Daily Press Briefing - July 9," *US Department of State*, 9 July 2009.
- <sup>21</sup> "U.S. Eyes N. Korea for 'Massive' Cyber Attacks," *MSNBC*, 7 July 2009.
- <sup>22</sup> "Military and Security Developments Involving the Democratic People's Republic of Korea 2013: Annual Report to Congress," *Department of Defense*, 2013, 11.
- <sup>23</sup> Ben Arnoldy, "Cyberattacks Against US, S. Korea Signal Anger - Not Danger," *The Christian Science Monitor*, 9 July 2009.
- <sup>24</sup> Pam Benson, Richard Allen Greene and Soh Jie-ae, "U.S. Government Sites among Those Hit by Cyberattack," *CNN*, 8 July 2009.

## 30 CASAS DEL ALBA IN PERU endnotes

- <sup>1</sup> "Perú investigaría 'Casas del ALBA' por supuesta injerencia," *Reuters*, 30 October 2007.
- <sup>2</sup> The ALBA Houses are one part of a larger network of various "friendship houses" that promote solidarity with ALBA and its member states. The final report of the congressional investigation counts 148, including 58 ALBA Houses, cf. "Informe Final de la "Comisión Investigadora Multipartidaria sobre la constitución, funcionamiento, organización, financiamiento, actividades y otros aspectos de las denominadas 'Casas de la Alternativa Bolivariana para las Américas' y los vínculos que podrían tener con actividades ilícitas, grupos terroristas residuales o intromisión de otros gobiernos en asuntos internos de nuestro país." (Congressional Investigation, Final Report), 11 May 2009, 193.
- <sup>3</sup> Andres Oppenheimer, "Alan García, Chávez y Las Casas del Alba," *El Comercio*, 18 March 2008.
- <sup>4</sup> Joseph Poliszuk, "Peru: The Cold War of ALBA," *El Universal*, 9 July 2008. As part of Mission Miracle, approx. 14,000-17,000 Peruvians were sent to a newly built health centre in the Bolivian town Copacabana, in close proximity to the Peruvian border. While Bolivia claims the establishment of the clinic was not connected to Mission Miracle, in fact 93 per cent of the patients were Peruvians and the clinic was almost entirely run by Cuban doctors, cf. Congressional Investigation, "Final Report," 217-20. Additionally, around 1,700-5,000 Peruvian patients were transported to Venezuela via free flights provided by the Venezuelan government.
- <sup>5</sup> Congressional Investigation, "Final Report," 207-9.
- <sup>6</sup> Nicole Ferrand, "Chavez moves into Peru," *Center for Security Policy*, 7 April 2008.
- <sup>7</sup> Congressional Investigation, "Final Report", 214-15.
- <sup>8</sup> Congressional Investigation, "Final Report," 211-12.
- <sup>9</sup> Congressional Investigation, "Final Report," 227, 229.
- <sup>10</sup> "Cierran 162 de las 326 casas de la ALBA," *El Correo*, 2 July 2008.
- <sup>11</sup> "Venezuela suspendió la Misión Milagro en el Perú," *La Razon*, 12 March 2009.
- <sup>12</sup> Congressional Investigation, "Final Report," 205-6.
- <sup>13</sup> "Venezuela niega que haya injerencia en Perú," *La Prensa*, 13 March 2008.
- <sup>14</sup> Günther Maihold, "Foreign Policy as Provocation. Rhetoric and Reality in Venezuela's External Relations under Hugo Chávez," *SWP Research Paper* (Berlin: German Institute for International and Security Affairs, January 2009).
- <sup>15</sup> Ibid.
- <sup>16</sup> Nicole Ferrand, "Ollanta Humala. Peru's Worst Nightmare," *Center for Security Policy*, 22 May 2009.
- <sup>17</sup> "Alan García dispuesto a enfrentar la estrategia bolivariana en Perú," *Noticias 24*, 17 March 2008.
- <sup>18</sup> "Perú investigaría 'Casas del ALBA' por supuesta injerencia," *Reuters*, 30 October 2007.
- <sup>19</sup> Andres Oppenheimer, "Alan García, Chávez y Las Casas del Alba," *El Comercio*, 18 March 2008.
- <sup>20</sup> "Humala defiende funcionamiento de Casas del Alba y cuestiona ingreso de personal militar de EEUU," *Andina*, 24 May 2008; Joseph Poliszuk, "Peru: The Cold War of ALBA," *El Universal*, 9 July 2008.
- <sup>21</sup> "Venezuela niega que haya injerencia en Perú," *La Prensa*, 13 March 2008.
- <sup>22</sup> US Embassy Lima, "GOP Investigates Venezuelan Government Interference," Wikileaks Cable: 08LIMA489\_a, dated 8 March 2008.
- <sup>23</sup> Javier Corrales, "Using Social Power to Balance Soft Power: Venezuela's Foreign Policy," *The Washington Quarterly* 32, no.4: 97-102.
- <sup>24</sup> US Embassy Lima, "The Alba House Threat," Wikileaks Cable: 08LIMA663\_a, dated 16 April 2008.
- <sup>25</sup> While Ollanta Humala narrowly lost against Alan García in 2006, he became president five years later in 2011. However, it is not possible to assess in what way the ALBA Houses and other initiatives by Venezuela may have contributed to Humala's increasing support and subsequent win in 2011. Moreover, Humala took a more moderate stance and tried to distance himself from the Chávez administration in his 2011 election campaign.
- <sup>26</sup> US Embassy Lima, "The Alba House Threat," Wikileaks Cable: 08LIMA663\_a, dated 16 April 2008.
- <sup>27</sup> Congressional Investigation, "Final Report," 223-24.
- <sup>28</sup> James Roberts and Edwar Escalante, "Fighting for Freedom in Rural Peru: 'ALBA Houses' Threaten Democracy," *The Heritage Foundation*, 18 August 2008, 6.
- <sup>29</sup> Nicole Ferrand, "Peru's Reaction to Venezuelan Intervention," *The Americas Report*, 10 August 2007.
- <sup>30</sup> Peru Ministry of Defense, "Libro Blanco de la Defensa Nacional" (Defense White Paper 2005), 61-6.
- <sup>31</sup> James Roberts and Edwar Escalante, "Fighting for Freedom in Rural Peru: 'ALBA Houses' Threaten Democracy," *The Heritage Foundation*, 18 August 2008, 4-8.
- <sup>32</sup> "Investigarán a 38 directivos de llamadas Casas del Alba," *La Razon*, 12 May 2009.













## Awali, Elabe

---

**From:** G7RRM@international.gc.ca  
**Sent:** Friday, May 3, 2019 5:51 PM  
**To:** thomasowen.ripley@canada.ca;  
Andrew.Lefrank@cbsa-asfc.gc.ca; Shen, Riri; tamara.trotman@canada.ca;  
Elise.Renaud@canada.ca;  
Ashley.MCCAULEY@forces.gc.ca; Lori.Wilkinson@rcmp-grc.gc.ca;  
chris.beall@canada.ca; Emily.Geday@canada.ca; Diaczuk, Shane;  
andrew.barrett@rcmp-grc.gc.ca  
**Cc:** Tara.Denham@international.gc.ca; Marketa.Geislerova@international.gc.ca;  
Mohammad.Rostami@international.gc.ca  
**Subject:** RRM Canada: Alberta Elections Analysis and NATO StratCom Report  
**Attachments:** 1. Alberta Elections Analysis.docx; 2. Hybrid Threats - A Strategic Communications Perspective-compressed.pdf

Dear colleagues,

Please see attached the following report produced by RRM Canada:

**1. Alberta Elections Analysis**

This report analyzes open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019.

Additionally, the following report from the NATO Strategic Communications Centre of Excellence is also attached:

**2. Hybrid Threats - A Strategic Communications Perspective**

This report is the result of a two-year study conducted by the NATO Strategic Communications Centre of Excellence. It is designed to help national authorities understand, prepare for, identify and respond to hybrid threats.

Feedback/comments are always welcome.

Kind regards,

G7 Rapid Response Mechanism | Mécanisme de réponse rapide du G7  
Centre for International Digital Policy | Centre pour la politique numérique internationale  
[G7RRM@international.gc.ca](mailto:G7RRM@international.gc.ca)  
125 Sussex Drive | 125 promenade Sussex  
Global Affairs Canada | Affaires mondiales Canada  
Government of Canada | Gouvernement du Canada



Government  
of Canada

Gouvernement  
du Canada

Canada



TOGETHER • ENSEMBLE

**CANADA**

UN SECURITY COUNCIL CANDIDATE  
CANDIDAT AU CONSEIL DE SÉCURITÉ DE L'ONU

2021-2022

## ALBERTA ELECTION ANALYSIS

## PURPOSE

This report analyses open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019. Prepared in support of the [G7 Rapid Response Mechanism \(RRM\)](#), the report was penned by RRM Canada. The RRM is mandated to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

## KEY FINDINGS

Based on primary and secondary research, RRM Canada concludes that there were very likely **no significant foreign interference campaigns** targeting the Alberta election in the online space in April 2019. However, coordinated inauthentic activity was detected:

- **RRM Canada identified accounts that demonstrated coordinated inauthentic behaviour.** RRM Canada judges the activity is very unlikely to comprise one third of the online conversation as reported by [Press Progress on April 11, 2019](#).
- RRM Canada identified cases of social media accounts, which were **likely inauthentic, coordinated behaviour**<sup>1</sup> around online discussions about the Alberta election. However, the majority of these accounts were very likely not foreign.
- RRM Canada identified known national far-right and hate group actors who have previously disseminated material, **using similar tactics as known malign foreign actors.**
- RRM identified **accounts tied to lobbying groups** that were unaffiliated with a political party spreading disinformation online in the run-up to the Alberta election.
- The Alberta election provides an example of a situation where there may be evidence of **coordinated inauthentic behaviour undertaken by Canadian actors**, making the identification of foreign interference more difficult.

## Alberta Election Findings

[1] RRM Canada reviewed social media data to search for obvious cases of coordinated, inauthentic behaviour with the objective of identifying any potential foreign activities. Based on available information, it is very unlikely there was any foreign interference. The two largest components of the graph are made up of supporters of the former Premier Notley and Premier Kenney, as expected in an election campaign [Annex A].

[2] RRM Canada assesses that none of the major communities taking part in online conversations related to the elections are driven by foreign interference. The presence of automated inauthentic activities does not appear central or crucial to the overall conversation or activity.

---

<sup>1</sup> Scale of Estimative Language: Almost No Chance – [0 – 10]; Very Unlikely/Very Improbable – [11 – 29]; Unlikely/Improbable – [30 – 39]; Roughly Even Chance – [40 – 59]; Likely/Probable – [60 – 69]; Very Likely/Very Probable – [70 – 89]; Almost Certainly – [90 – 100]

[3] RRM Canada's findings stand opposite to the [April 11, Press Progress report](#), which claimed that a third of accounts talking about the Alberta election were bots. **RRM Canada's findings, using multiple tools and methods, judges that the online activity is very unlikely to comprise one third of bots.** The article appears to rely only on the online tool mentionsmap as a metric for "bot activity", which is not a proper means of assessment for inauthentic account behaviour or bot activity. RRM Canada therefore does not support the findings articulated in the Press Progress Report.

[4] RRM Canada identified communities that **demonstrated a suspicious account creation pattern that is indicative of troll or bot activity.** Recent spikes in account creation suggest the presence of accounts developed for a specific purpose; however, **the community was determined to very likely be domestic,** as it was mainly comprised of supporters of the United Conservative Party (UCP). A second small community was identified as supporters of the People's Party of Canada, which had similar suspicious patterns of account creation. This pattern was not identified within communities of supporters of the Alberta Liberal Party or Alberta New Democratic Party. The overall number of accounts is a small percentage of a larger collection [Annex B]. This highlights a key point, namely that **domestic actors are also emulating the tactics used by foreign actors, within the context of provincial elections. This behaviour will make it increasingly difficult to distinguish national from foreign interference efforts in the upcoming Federal election.**

[5] The RRM identified a small group of anonymous accounts pushing a pro-separation movement in Alberta and the Prairies. Though Alberta has an official separatist party, <https://albertaindependence.ca/>, these accounts do not appear affiliated with this movement. Creating false separatist movements or amplifying domestic ones is a known tactic in foreign interference. Though unaffiliated, at this time, RRM Canada cannot tie this small group of accounts to any foreign entity.

[6] In its review of the data of this election, RRM Canada found no evidence supporting a broad, coordinated campaign to influence the Alberta election. **RRM Canada assesses that automated inauthentic behaviour and trolling activities are very likely domestic in nature;**

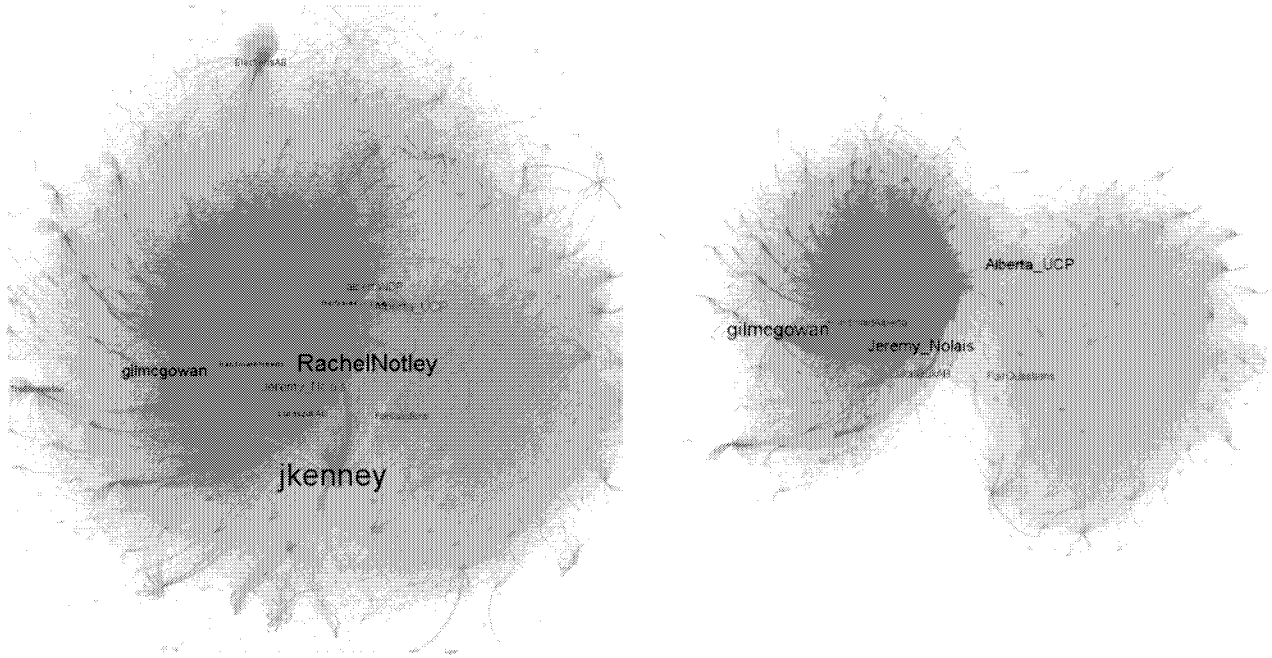
Released: May 1, 2019

**Disclaimer:** G7 Rapid Response Mechanism Canada (RRM Canada) monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.



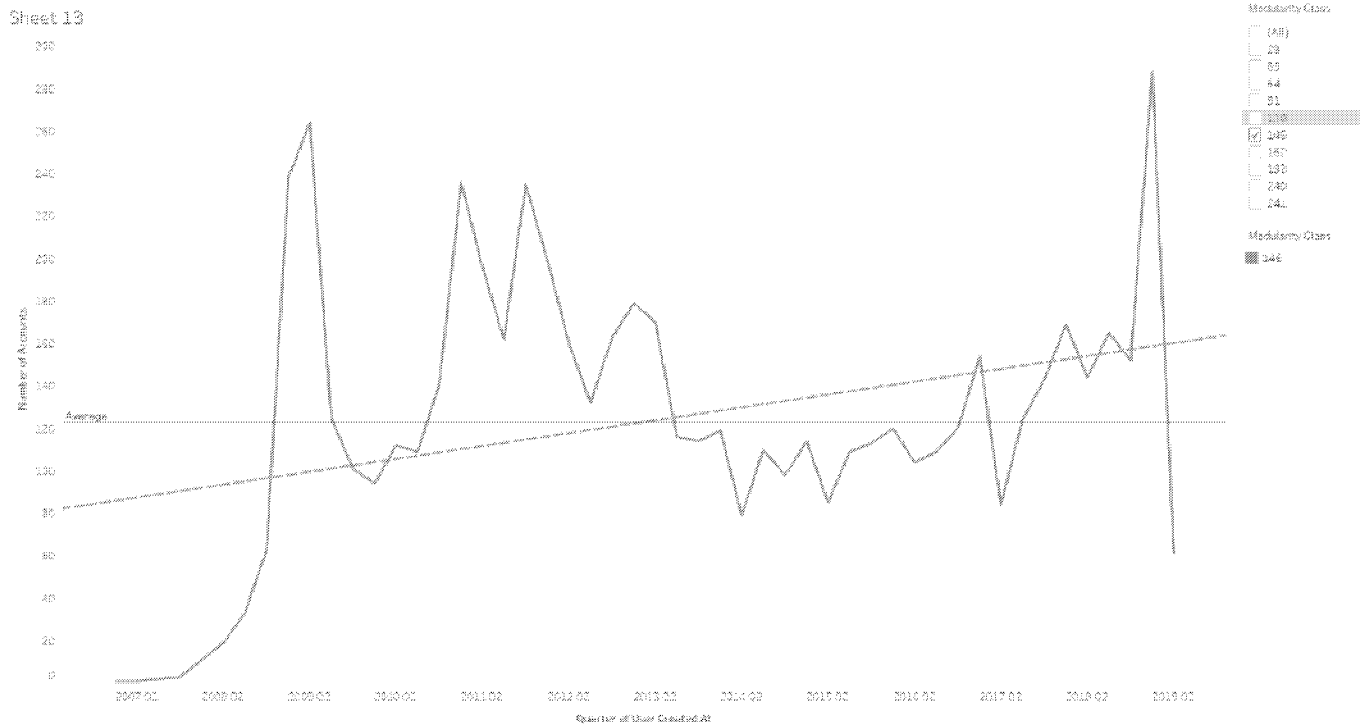
**Annex A**

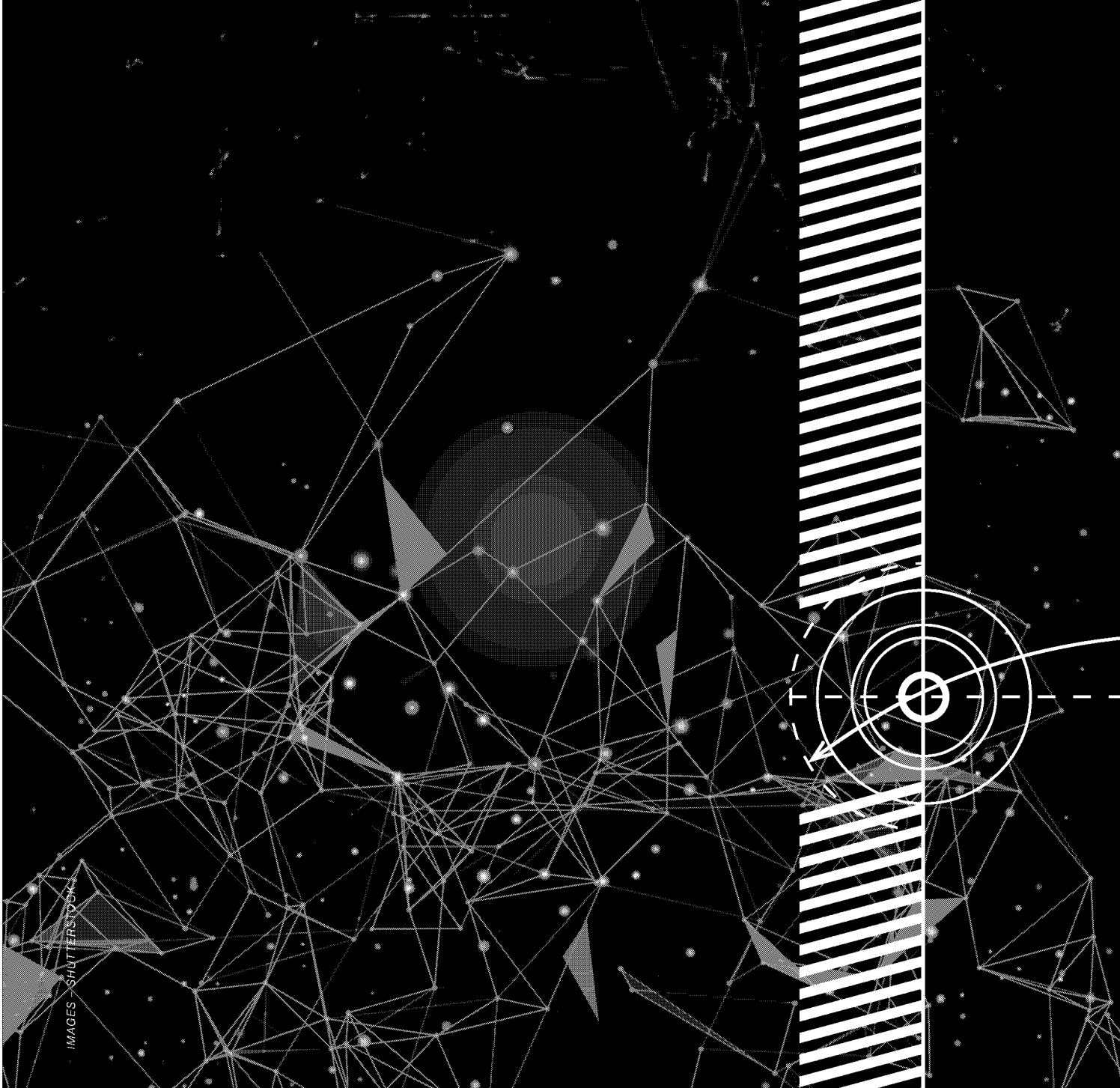
This Annex is a visual representation of RRM Canada’s data collection illustrating a high level of normality in the online conversation related to the Alberta provincial election. The analysis of activity would have been noteworthy for RRM Canada if there were other communities that rivaled the main political communities in size, but were predominately unknown actors, or actors from another geographical location.



Annex B

A review of the account creation dates of accounts in the community of UCP supporters. The size of the final spike is an indicator of inauthentic activity. One indicator of bot activity is a large number of recently-created accounts. In this case, a large spike in accounts created in Q1 2019 is suggestive of inauthentic activity by either automated accounts or anonymous accounts. This combined with a qualitative evaluation of the accounts by RRM Canada, as well as their posting behaviours and the social network analysis; these are indications of likely inauthentic behaviour.





IMAGES SHUTTERSTOCK

# Hybrid Threats

A Strategic Communications Perspective





# Hybrid Threats

A Strategic Communications Perspective

## Acknowledgements

### Project Director

Ben Heap

### Project Assistants

Sophia Krauel, Jente Althuis

### Research Assistants

Alexandra Clifton, Tara Flores, Leonie Haiden, Pia Hansen, Torsten Hertig

### Contributing Authors

Dr Sean Aday, Dr Māris Andžāns, Dr Una Bērziņa-Čerenkova, Dr Francesca Granelli, John-Paul Gravelines, Dr Mills Hills, Miranda Holmstrom, Adam Klus, Irene Martinez-Sanchez, Mariita Mattiisen, Dr Holger Molder, Dr Yeganeh Morakabati, Dr James Pamment, Dr Aurel Sari, Dr Vladimir Sazonov, Dr Gregory Simons, Dr Jonathan Terra

Global Influence, Hersh Consulting, Latvian Institute of International Affairs (LIIA), Norwegian Defense Research Establishment (FFI)

### With thanks to

Henrik Aagardh-Twetman, Devin Ackles, Iona Allan, Vārin Alme, Ruta Apeikyte, Uku Arold, Professor Christina Archetti, Matt Armstrong, Sebastian Bay, Andreas Beger, Gita Bērziņa, Beata Bialy, Dr Neville Bolt, Mira Boneva, Erik Brattberg, Henry Collis, Dr Patrick Cullen, Linda Curika, Thomas Frear, Lucy Froggatt, Melissa Hersh, Brady Hills, Ivars Indans, Jakub Janda, Dr Ivo Juurvee, Alise Krauja, Dr Torbjørn Kveberg, Elina Lange-Ionatamisvili, Dr Andrew Mumford, Piret Pernik, Dr Vladimir Rauta, Dr Sophie Roberts, Connor Seefeldt, Dr Antti Sillanpaa, Bernd Sölter, Zane Štāla, Jan Stejskal, Sanda Svetoka, Dr Claire Yorke, Deniss Žukovs

King's Centre for Strategic Communications, The European Centre of Excellence for Countering Hybrid Threats, European Union External Action Service

### Layout by Inga Ropsa

Media enquiries to Linda Curika: [info@stratcomcoe.org](mailto:info@stratcomcoe.org)

# About this report

## Aim

This report is the product of a research project undertaken by the NATO Strategic Communications Centre of Excellence (NATO StratCom COE), at the request of the governments of Lithuania and Estonia. The project was designed to deepen our understanding of the wide range of measures which come under the umbrella of 'hybrid threats'. Such measures aim to influence the political decision-making of a targeted nation in a way which hurts their national security interests, predominantly conducted in the 'grey zone' between peace, crisis and war.

## Scope

The project broadens the framing of current debates on hybrid threats beyond the most common empirical reference points, which tend to relate to the Russian Federation. A standardised framework is used to analyse case studies which are assessed to offer examples of hybrid threats.

Analysis has been conducted from the perspective of 'Strategic Communications', which is articulated for this report not simply as a suite of capabilities disseminating messages to explain actions or intentions in support of strategy but as a basic function of statecraft. Strategic Communications is therefore considered both as an overarching philosophy to be inculcated into organisational culture and as a cross-government process, central to integrating the instruments of national power.

The research focuses on the national level, where the primary responsibility lies for understanding, identifying and responding to hybrid threats. In this main volume, summaries of 30 cases are provided, of which a representative selection of 10 cases are analysed in detail in a separate annex. In order to limit the scope of the project, this phase of research focuses solely on state actors.

## Purpose

The case studies are not intended to be definitive accounts of a particular scenario or provide templated solutions to similar situations, nor does the inclusion of any particular state actor necessarily conclude malicious intent. The report encourages the reader to take a '360-degree view' of an issue area, deepening their knowledge of factors and considerations relevant to threat assessment.

This report is designed to help the reader develop two complementary viewpoints. First, being agile and adaptive enough to deal with emerging security challenges where the identity and intent of adversaries may be unclear or deliberately deceptive. Threats may also be constituted by the synergy of many different, apparently unconnected measures.

Second, the *Strategic Communications mindset*. This is the notion that *everything communicates*. The key to an effective strategy is therefore to understand actors and audiences, then integrate policies, actions and words across government in a coherent way to build national resilience and leverage strategic influence.

# CONTENTS

<b>EXECUTIVE SUMMARY</b>	7
<b>Executive Summary</b>	8
<b>A STRATEGIC COMMUNICATIONS APPROACH TO HYBRID THREATS</b>	17
<b>About hybrid threats</b>	18
<b>The Strategic Communications mindset</b>	21
<b>Strategic Communications at the national level</b>	22
<b>Research approach</b>	24
<b>KEY FINDINGS AND RECOMMENDATIONS</b>	26
<b>10 key recommendations</b>	27
<b>Analysis of thematic areas</b>	37
<b>CASE STUDY SUMMARIES</b>	47
1. RUSSIAN SNAP EXERCISES IN THE HIGH NORTH	48
2. CONFUCIUS INSTITUTES	50
3. 2007 CYBER ATTACKS ON ESTONIA	52
4. US TRANSIT CENTER AT MANAS	54
5. THE SPREAD OF SALAFISM IN EGYPT	56
6. DISINFORMATION IN SWEDEN	58
7. HAMAS' USE OF HUMAN SHIELDS IN GAZA	60
8. THE 2010 SENKAKU CRISIS	62
9. HUMANITARIAN AID IN THE RUSSO-GEORGIAN CONFLICT	64
10. CHINESE PUBLIC DIPLOMACY IN TAIWAN	66
11. DETENTION OF ESTON KOHVER	68
12. FINNISH AIRSPACE VIOLATIONS	70
13. SOUTH STREAM PIPELINE	72
14. RUSSIAN LANGUAGE REFERENDUM IN LATVIA	74
15. INSTITUTE OF DEMOCRACY AND COOPERATION	76
16. ZAMBIAN ELECTIONS 2006	78
17. SERBIAN ORTHODOX CHURCH	80
18. COMMUNIST PARTY OF BOHEMIA AND MORAVIA	82
19. BRONZE NIGHT RIOTS	84
20. RUSSKIY MIR FOUNDATION IN THE BALTICS	86
21. CRIMINAL NETWORKS IN THE DONBAS	88
22. CIVIL DISORDER IN BAHRAIN 2011	90
23. PAKISTANI INVOLVEMENT IN YEMEN	92
24. OPERATION PARAKRAM	94
25. SNAP EXERCISES AND CRIMEA	96
26. ELECTRONIC WARFARE DURING ZAPAD 2017	98
27. RUSSIAN ESPIONAGE IN SWEDEN	100
28. RELIGIOUS EXTREMISM IN THE NETHERLANDS	102
29. CYBER ATTACKS ON ROK & US	104
30. CASAS DEL ALBA IN PERU	106



# EXECUTIVE SUMMARY

# Executive Summary

This report is the result of a two-year study conducted by the NATO Strategic Communications Centre of Excellence. It is designed to help national authorities understand, prepare for, identify and respond to hybrid threats. The research focuses on state actors and uses a standardised framework to analyse 30 case studies taken from a range of geopolitical scenarios. It does so from the perspective of Strategic Communications, which is articulated not simply as a means of supporting national strategy through coordinated messaging but as a mechanism for integrating all actions taken by a government, central to both the development and implementation of strategy.

## About hybrid threats

- The final communique from the 2018 NATO summit in Brussels stated that NATO nations had “come under increasing challenge from both state and non-state actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict.”<sup>1</sup> The term ‘hybrid’ has been used to describe a wide array of measures, means and techniques including, but not limited to: disinformation; cyber attacks; facilitated migration; espionage; manipulation of international law; threats of force (by both irregular armed groups and conventional forces); political subversion; sabotage; terrorism; economic pressure and energy dependency.
- NATO defines hybrid threats as a ‘type of threat that combines conventional, irregular and asymmetric activities in time and space’.<sup>2</sup> This provides the essence of something produced by the synergy of different measures but used alone it is too broad. Most current definitions of hybrid threats lean heavily on Russian actions in Ukraine and Crimea, but this risks neglecting one of the key aspects of hybrid threats, that of **adaptability**.
- While discussions surrounding the essential nature of ‘hybridity’ are likely to continue, the underlying phenomena the term encapsulates remain very real.<sup>3</sup> This report therefore focuses on the **characteristics of hybrid threats**. These are actions which:
  - Are coordinated and synchronised across a wide range of means.
  - Deliberately target democratic states’ and institutions’ systemic vulnerabilities.
  - Use a wide range of means.
  - Exploit the threshold of detection and attribution as well as the border between war and peace.
  - Aim to influence different forms of decision-making at the local (regional), state, or institutional level.
  - Favour and/or gain the agent’s strategic goals while undermining and/or hurting the target.<sup>4</sup>
- A key aspect of hybrid threats is **ambiguity** – hostile actions that are difficult for governments to identify, attribute or publicly define because the responsible actor or overall intent is unclear or deliberately obscured.<sup>5</sup> The effects from hybrid threats can be diffuse and may only materialise over time.
- **Attribution** is ultimately a political endeavour by individual governments based on an assessment of the measures involved and an understanding of actors and their interests. It is unlikely that governments will find conclusive evidence that ‘proves’ hostile intent, or be able to publish sensitive intelligence. Threat

<sup>1</sup> “Brussels Summit Declaration, issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11-12 July 2018,” *North Atlantic Treaty Organization*, 11 July 2018.

<sup>2</sup> NATO Standardization Office (NSO), *AAP-6, NATO Glossary of Terms and Definitions* (2018 edition), 62.

<sup>3</sup> Elie Tenenbaum, “Hybrid Warfare in the Strategic Spectrum: A Historical Assessment”, in ‘*NATO’s response to Hybrid Threats*’, eds Guillaume Lasconjaras and Jeffrey A. Larsen (NATO Defense College 2017), 95-112.

<sup>4</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018), p10.

<sup>5</sup> Andrew Mumford and Jack McDonald, *Ambiguous Warfare*, report produced for the Development, Concepts and Doctrine Centre, October 2014.

assessments can differ between nations and international organisations (such as NATO or the EU) which can further hamper effective and coordinated responses.

- The way in which hybrid threats are interpreted is complex and significantly affected by **context**. For instance, an airspace violation can be regarded as either accidental or a deliberate act of provocation. Military exercises can be perceived as reassurance or deterrence and a foreign-sponsored political foundation can be seen as fostering intercultural exchange or undermining democratic values.
- The realm of hybrid threats is characterised by the interplay between information, perception, interpretation and decision-making. An appreciation of how actors and audiences interact, form opinions and make decisions should therefore be the basis of understanding the hybrid threat environment.

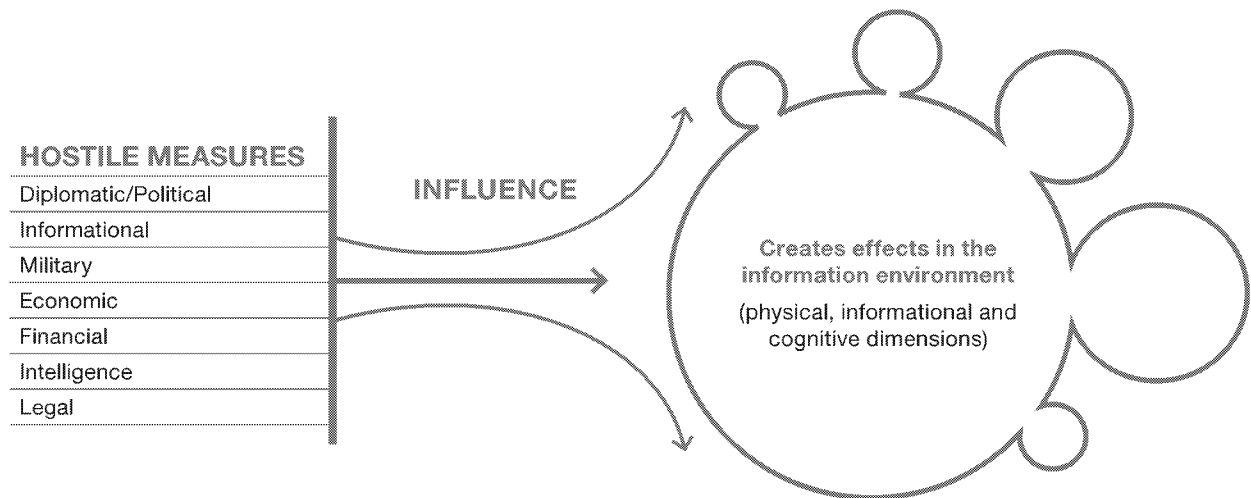
## Hybrid threats as levers of influence

- Hybrid threats have the malign intent of manipulating the **political decision-making processes** of a targeted nation by influencing the behaviours and attitudes of key audiences such as media organisations, the general public and political leaders.
- Hybrid threats can therefore be considered as **information or influence activities**. These are actions which influence audience perception and decision-making. Such activities are not limited to the 'Information' instrument but involve the combination of different instruments of power, including Diplomatic, Economic and Military.
- Understanding the way hybrid threats act as levers of influence requires a shift from focusing on the real, physical world where events and actions occur, to the conceptual realm where information exists and communication takes place. The Information Environment (IE) is a model which enables this.
- The **Information Environment (IE)** is a model for understanding how actors and audiences interact, how people see the world around them and consequently make decisions based on the meaning they deduce from it. It is a *conceptual space* consisting of three interrelated dimensions: **cognitive** (where people think, understand and decide); **physical** (individuals, organisations and infrastructure) and **informational** (facts, knowledge and data).<sup>6</sup> The IE is often used as a shorthand for the media environment but this belies its utility in offering a way to understand the interaction between all activities – ranging from military force posture to the construction of pipelines – and what they communicate to audiences.
- Analysis of the IE can help understand how hybrid threats exploit vulnerabilities, such as cultural divides or grievances, to undermine the targeted nation while benefiting the responsible actor's strategic interests. Addressing domestic issues and building societal resilience is a key component of countering hybrid threats.
- All activities undertaken by an actor affect the IE and influence decision-making in the cognitive dimension. So, while information can be an enabler *to* national power, the ability to influence audiences comes *from* the synergy of national instruments, including diplomatic, informational, military and economic measures.<sup>7</sup>
- The synergy of different hostile measures can exploit vulnerabilities across the full range of state systems of a targeted nation – political, military, economic, social, information and infrastructure (known as the PMESII spectrum).

---

<sup>6</sup> U.S. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations, incorporating change 1* (Washington D.C., 2014), 1-2.

<sup>7</sup> The standard model of the instruments of national power is DIME but in the context of hybrid threats, NATO adds Financial, Intelligence and Legal to make DIMEFIL, which is used for the analysis in this research.



## The Strategic Communications mindset

- Enabled by an understanding of the IE, Strategic Communications as a response to hybrid threats provides a holistic approach to communication, based on values and interests and encapsulating everything a nation can do to achieve strategic objectives in a contested environment.
- The term 'Strategic Communications' is often used interchangeably to refer to both the function which coordinates cross-government activities and the communications themselves. This report focuses on the former and articulates Strategic Communications as being predominantly a philosophy or *mindset* but also a *process* and a *capability*.
- To be effective, the concepts of Strategic Communications need to be endorsed as a guiding principle across all government departments and levels. This is Strategic Communications as a *mindset*, which is an appreciation that **everything – words, actions, images, policies – communicates**.
- Strategic Communications as a *process* can provide a more **effective orchestration of government activity**, integrating activities across the instruments of power to leverage strategic influence and build national resilience.
- Such a process might need resourcing with a *capability* (such as the 'Department of Strategic Communications'), to enable planning and integration of cross-government activities such as media handling, marketing and engagement. However, rather than simply establishing new, specialist structures, governments would benefit from establishing a communication culture at all levels.

## Strategic Communications at the national level

- The first step in the process of Strategic Communications is to **understand the Information Environment**. Considerations of human perception and behaviour should be central in understanding the dynamics of hybrid threats, how they are perceived, interpreted and attributed.
- Communication, including all actions, images, words and policies, should be **collective and integrated**. Every action a government takes (or does not take) communicates something, so all personnel in every department and branch are communicators.
- Actions to address hybrid threats should be guided by a **national strategy** which has consensus of support amongst the population and is endorsed from the top down by political leadership. Communication considerations should be at the centre of the development and implementation of strategy from the outset.
- National authorities need to have structures that are **flexible, decentralised and adaptive**. Hybrid threats are characterised by the synchronisation of different instruments and adaptability to context and vulnerabilities. Preparation, agility and responsiveness should be key considerations in dealing with such activities.

- Attributing hybrid threats to an adversary is a political endeavour by national governments which requires an evaluation of the geopolitical context and the strategic logic underlying adversarial measures. This assessment relies on the trust of the public. **Credibility should be protected as a vital resource.**

## Research approach

- The research attempts to broaden the discussion on hybrid threats beyond the current emphasis on the Russian Federation. It aims to assist the reader understand the factors to be considered when identifying and responding to the full range of hostile measures a nation might face.
- The project identified 250 scenarios from the end of the Cold War until the present day as potential examples of hybrid threats. A representative selection of 30 cases are analysed to understand the ways in which hybrid threats might materialise. The case studies are not intended to be definitive accounts of a particular scenario or provide templated solutions to similar situations, nor does the inclusion of any particular state actor necessarily conclude malicious intent.
- The project uses a standardised analytical framework to align the case study research and ensure comparability of the findings across the different cases. It structures the analysis according to the ways in which adversaries use different channels and means to exploit vulnerabilities and undermine the target's national security interests while advancing their strategic objectives.
- The analytical framework covers the full range of adversarial measures across the DIMEFIL continuum and tries to capture the way in which they might be synchronised and integrated to create effects.
- To understand attribution and interpretation of hybrid threats, narratives, context and an assessment of the underlying strategic logic of adversarial measures are analysed.
- The case studies are grouped together into sixteen thematic areas of threat. In accordance with the 'fog' of ambiguity that characterises hybrid activity, this is not intended to be a categorisation which can be used to objectively define different measures and means. Instead, it is meant to raise awareness for the diverse fields and channels through which hybrid threats can occur, ranging from the exploitation of ethnic identities and energy dependency to espionage and bribery.

### Thematic areas of threat

Territorial violation	Non-Government Organisations (NGOs)	Government Organised Non-Government Organisations (GONGOs)	Espionage and infiltration
Exploitation of ethnic or cultural identities	Media	Lawfare	Agitation and civil unrest
Cyber operations	Religious groups	Academic groups	Coercion through threat or use of force
Energy dependency	Political actors	Economic leverage	Bribery and corruption

- Based on the comparison of the case studies across all thematic areas, the project identified practical lessons and guidelines for decision-makers at the national level where the main responsibility lies for understanding, identifying and responding to hybrid threats. The key findings are summarised and captured in the following top ten recommendations, applying the Strategic Communications mindset to the challenge of hybrid threats.

# Summary of Key Findings and Recommendations

**The findings from this report focus on how to apply the Strategic Communications mindset to the challenge of hybrid threats.**

## **1. Everything communicates.**

All policies, actions and words influence decision-making, therefore communication should be integral to strategy and considered from the outset of planning. National authorities preparing for, and responding to, hybrid threats should appreciate that communication is not limited to words – every action (or inaction) can influence the attitudes and behaviours of key audiences. Strategic Communications is therefore not limited to certain functions and capabilities – such as public affairs and press offices – but is an organisational responsibility, with everyone working to achieve desired outcomes derived from overarching objectives.

## **2. Whole-of-government.**

Hybrid threats are generated from a mix of adversarial measures to influence political decision-making of the targeted nation, therefore an integrated approach across government is needed to effectively identify and address such threats. What works in one situation may not work in another, so governments need to be agile and able to anticipate and identify potential threats, then integrate and coordinate their response across a range of levels and channels. This requires timely decision-making and a coherent, sustained response to reinforce government credibility and legitimacy.

## **3. Understand the strategic logic.**

In order to understand an adversary's strategic logic, national authorities should grasp the underlying thinking and calculation behind adversarial measures. This entails assessing their potential aims, and the way in which different instruments are integrated and synchronised to achieve these objectives. Such an understanding would allow governments to identify potential vulnerabilities and key target audiences, anticipate future developments through horizon scanning, and adjust their preparation and response.

## **4. Determine what you want to protect and identify vulnerabilities.**

Hybrid threats deliberately target and exploit existing vulnerabilities of the target state, often opportunistically. Domestic issues such as systemic corruption and social divisions can be exploited by malign state actors. Weakness in national security institutions and a lack of public confidence in government may be seen as domestic political issues, but these vulnerabilities enhance the ability of hostile actors to affect critical functions and damage national security interests. Nations should continually assess their vulnerabilities in an honest and transparent manner and articulate this in national security policy.

## **5. Build resilience.**

Resilience describes the ability of a state and society to withstand pressure and recover from crises or shocks which may be the result of a hybrid threat. Improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost-benefit calculation. Deterrence through resilience is therefore a key component of reducing a nation's susceptibility to hybrid threats.

**6. Activity should be based on values, with clear objectives.**

Governments need to be clear about their strategic aims and ensure that statements and actions are consistent with core values. They should understand that employing measures or taking positions which appear to be deceptive or inauthentic will undermine their credibility. Democracies should also be aware that appearing to deal harshly with a suspicious actor – such as with civil society or media organisations – might provide the justification for autocratic governments to crack down on disagreeable foreign-sponsored NGOs or media outlets in their own country.

**7. Be proactive.**

A proactive approach would enable governments to maintain dominance over evolving narratives and frame events in a manner favourable to their interests. Instead of merely responding to threats as they materialise, governments should anticipate events and issues that are likely to be exploited by adversaries. This can reduce risk by not merely ‘countering’ an adversary’s activities, but pre-emptively steering public discourse in a preferred direction and building resilience, thus reducing the likelihood of unintentionally reinforcing an adversary’s preferred narrative of events.

**8. Understand the information environment.**

The ultimate purpose of any hybrid threat is to affect the political decision-making of the target nation by influencing key target audiences. Adversarial activity may be undertaken to make a political statement, alter perceptions and attitudes of the general public, degrade levels of trust and confidence in government, or create confusion and a sense of insecurity. This is why consistent, coherent and factual government communications tailored to different key audiences is crucial to maintain trust and cohesion.

**9. Learn to operate in shades of grey.**

Hybrid threats can be complex, adaptive and inflict damage on national security before they are detected. Ambiguity surrounding intent and attribution impairs decision-making and complicates effective responses. Compelling and credible evidence may not be publicly available, and so the role of government communication becomes particularly important. Official statements should be specific and coherent, capture the nuances of the situation and give enough factual, credible information to inspire public confidence in the government. Governments should not spend too much time on trying to decipher deliberately ambiguous messages and actions, but instead frame events in a manner favourable to their aims.

**10. Not every activity is a threat.**

Defining an activity as a threat and attributing it to a state actor is ultimately a political endeavour, and governments should be mindful not to inflate the threat level for political ends, either deliberately or inadvertently. As hybrid threats target a nation’s weaknesses, it is a challenge to distinguish hostile influence from legitimate social grievances or failings of the government. Policy-makers should resist the temptation to blame external actors as a convenient way of shifting blame for domestic failings. Inflating or misattributing hybrid threats can affect the government’s credibility in the long-run and risks unnecessary escalation.

# Summary of case studies

Highlighted cases are covered in detail in a separate annex.

Case Study	Thematic Area	Summary
1 Russian snap exercises in the High North	Coercion through threat or use of force	The Russian military engaged in snap manoeuvres in response to Norwegian military activity in Finnmark and the US Exercise Dragoon Ride, despite both being announced well in advance. Although the Russian snap exercise of March 2015 was not interpreted as a threat by Norway it sparked a wider debate on whether the spirit of the OSCE's Vienna Document had been breached.
2 Confucius Institutes	Government Organised Non-Government Organisations (GONGOs)	The Confucius Institute (CI) is funded by the Chinese government and has secured partnerships with universities in many NATO nations. While the CI presents itself as a non-profit educational institution, it has frequently been described as a Chinese 'soft power' instrument. The institutes' structural integration and funding arrangement with their Western partner universities have led to concern about intellectual freedom and self-censorship on sensitive issues, such as Taiwan.
3 2007 cyber attacks on Estonia	Cyber operations	The first major occurrence of cyber warfare targeted the Estonian government, media, banks and other websites in 2007. This cyber attack coincided with the relocation of the controversial Bronze Soldier Memorial. The malicious network traffic had indications of political motivation and Russian-language origin.
4 US Transit Center at Manas	Economic leverage	The US Transit Center at Manas in Kyrgyzstan was established to support Operation Enduring Freedom in Afghanistan. Being increasingly wary of the prospect of a permanent US presence in Central Asia, the Russian Federation exerted significant pressure on the Kyrgyz government, coupled with offers of economic assistance. Despite generous US lease payments and economic aid, as well as extensive outreach efforts to the Kyrgyz population, the Transit Center at Manas was closed in 2014.
5 The spread of Salafism in Egypt	Political actors; Religious groups	The Kingdom of Saudi Arabia (KSA) has long supported Salafite ideology in Egypt, particularly by funding Salafite TV channels and charities. After the 2011 revolution, Salafism developed a political arm: the Salafite Nour Party's surprising financial advantage and electoral success gave rise to much suspicion of KSA funding, especially since the party has often supported KSA-friendly policies. Support of a friendly ideology allows the KSA to counter the regional influence of the Muslim Brotherhood; dominate the interpretation of Islam; and gain influence in Egyptian politics.
6 Disinformation in Sweden	Media	<i>Sputnik</i> published an article in response to the enhancement of Gotland's defences by the Swedish military. This article misquoted senior Swedish politicians and commentators, and deliberately distorted the truth to support Russia's position. This case provides a typical example of the systematic means by which contentious debates on national security are exploited as part of wider influence strategies by pro-Russian actors.
7 Hamas' use of human shields in Gaza	Lawfare	In an attempt to counter negative opinions of their use of lethal force, in their 2014 Operation Protective Edge, the Israeli Defence Forces (IDF) used a broad range of information activities designed to encourage civilians in Gaza to evacuate from certain areas before conducting military strikes against Hamas. Hamas took advantage of this to encourage 'human shields', which temporarily put Hamas into a win-win situation by restricting the IDF's freedom of action.
8 The 2010 Senkaku crisis	Economic leverage; Territorial violation	China embargoed Rare Earth Elements (REE) following its manufactured Senkaku Crisis with Japan in 2010. A Chinese fishing vessel deliberately rammed the Japanese Coast Guard near the disputed islands, leading to the detention of the Chinese trawler captain by the Japanese. Beijing immediately demanded the captain's release and encouraged anti-Japanese protests across the Chinese mainland. This incident provided a narrative that explained why Chinese customs officials chose to embargo the REE.
9 Humanitarian aid in the Russo-Georgian conflict	Lawfare	In 2008, the Russian Federation used 'humanitarian' assets in support of the separatist populations of Abkhazia and South Ossetia, two regions of Georgia which both declared independence in the early 1990s. The Russian government used what it termed 'humanitarian assistance' as an instrument to pursue broader geo-strategic goals that were not humanitarian in nature.
10 Chinese public diplomacy in Taiwan	Exploitation of ethnic or cultural identities	China's use of public diplomacy to further its 'One China' policy towards Taiwan is addressed to two key target audiences: the Taiwanese population, where they seek to bolster support for unification, and third countries, where the aim is to isolate Taiwan. The results have been mixed: while eschewing military confrontation, it has reduced diplomatic recognition by the international community yet failed to shift Taiwanese opinion, which remains confident of US support.



11	Detention of Eston Kohver	Espionage and infiltration; Territorial violation	Eston Kohver, a member of the Estonian security service, was detained by the Russian Federation in 2014 during an operation to counter organised crime in a disputed border region; he was then portrayed as a Western spy in the Russian media. Not only did this incident risk embarrassing the Estonian government, it increased friction between different groups in the country (e.g. the far right, pro-Russians, and anti-NATO activists).
12	Finnish airspace violations	Territorial violation	From March 2014 there was a marked increase in close military encounters between Russia and NATO aligned nations. These included airspace violations, near-miss mid-air collisions and maritime encounters. In the same year NATO scrambled and intercepted more than 100 airplanes in European airspace, more than three times than it did in the previous year.
13	South Stream pipeline	Energy dependency	Western nations must balance value, reliability, and security in the provision of its energy. This tension was brought into focus by the Russian Federation's South Stream pipeline project, which offered a competitive (if less secure) alternative to the EU-proposed Nabucco Pipeline and hence threatened its viability. Moreover, it encouraged certain NATO/EU member states to contravene EU legislation by supporting South Stream.
14	Russian language referendum in Latvia	Exploitation of ethnic or cultural identities	A referendum on whether to designate Russian as an official language was held in Latvia in 2012. Although unsuccessful, it exposed – and temporarily aggravated – divisions over language, ethnicity and identity in Latvia. While the issue initially came to prominence because of a campaign by Latvian nationalists, the Russian Federation used an existing network of individuals to exploit the situation.
15	Institute of Democracy and Cooperation	Academic groups; NGOs	The Institute of Democracy and Cooperation (IDC) presents itself as an independent think tank, despite an evident bias towards the Russian Federation and antipathy towards many NATO values. Although no formal connection can be proven with the Russian state, the latter is alleged to provide funding and there are informal links with board members and directors.
16	Zambian elections 2006	Economic leverage; Political actors	The Zambian government welcomed Chinese investment in construction and mining, but a significant part of the population was unhappy with China's influence which they saw as privileged and threatening. This anti-Chinese sentiment became a pivotal issue during the 2006 presidential elections, with opposition candidate Michael Sata pledging to expel Chinese investors and making overtures to recognise Taiwan as a sovereign state. China took the position that if Sata won and established diplomatic ties with Taiwan, bilateral relations with Zambia would suffer and further investments put on hold.
17	Serbian Orthodox Church	Religious groups	The Serbian Orthodox Church has an outlook that can reasonably be described as pro-Russian; in particular, it actively organises demonstrations against the independence of Kosovo and "Western liberal values" such as LGBT rights. Most significantly, the Church can lend credibility to political messages towards Orthodox audiences, and may choose to extend such legitimacy and deploy its influence in a way more directly hostile to NATO and the NATO nations.
18	Communist Party of Bohemia and Moravia	Political actors	The Communist Party of Czechia and Moravia (KSČM) mirrors and normalises Russian narratives within the media and parliament of the Czech Republic: specifically, anti-NATO and anti-EU views are kept alive. The party encourages political radicalism and anti-system rhetoric. Two of its MPs visited the Donbas region in 2016 to lend legitimacy to Russian action in Ukraine.
19	Bronze night riots	Exploitation of ethnic or cultural identities; agitation and civil unrest	Violent protests broke out in Estonia after the relocation of the Bronze Soldier statue and the reburial of associated remains in 2007. There are radically different interpretations of the monument throughout Estonia: from the Russian perspective, the monument symbolises their victory in the Great War, while for many Estonians it represents the beginning of Soviet occupation. The riots, which resulted in the death of one Russian protester, were encouraged by Russian media and statements by Russian officials.
20	Russkiy Mir Foundation in the Baltics	Government Organised Non-Government Organisations (GONGOs)	The Russkiy Mir Foundation (RMF) is a cultural and educational institution that promotes Russian language and culture across over 100 countries. RMF has constructed a network of influencers among NATO nations, especially those bordering the Russian Federation. Such organisations are capable of activity which is hostile to the host nation and may contribute to cleavages in those societies.
21	Criminal networks in the Donbas	Bribery and corruption	Russian financial and military support for separatists in Ukraine encouraged organised criminal activity in Donetsk and Luhansk in 2014 – regions considered a safe haven for criminals. This took place alongside more familiar tactics, such as the questionable use of a referendum; unmarked soldiers of Russian origin; and encouragement of civil unrest. The consequent perception of Ukraine as a failed state threatens its territorial integrity, national security, and participation in NATO/EU structures.

22	Civil disorder in Bahrain 2011	Agitation and civil unrest; exploitation of ethnic or cultural identities	In 2011, the Kingdom of Bahrain – a majority Shia nation ruled by a Sunni minority – experienced mass protests which were inspired by the so-called 'Arab Spring'. Some of the most prominent demands of the protesters included political reform and a stop to systematic discrimination against Shia Muslims. It is likely that deliberate agitation by Iran, particularly by way of overt public statements and media channels, contributed to the escalation. Alleged Iranian interference was used as justification by the Bahraini regime to justify repression in the following years.
23	Pakistani involvement in Yemen	Economic leverage	Pakistan's decision not to join the Saudi-led intervention in Yemen in 2015 exemplifies a highly dynamic system of alliances and counter-alliances that Islamabad had to navigate while balancing multiple competing interests. Equilibrium was achieved in this case by stationing troops to protect the Saudi border, while refusing to deploy military force within Yemen.
24	Operation Parakram	Coercion through threat or use of force	The India-Pakistan standoff (2001–2002) was one the biggest conflicts between India and Pakistan after 1971, which had a nuclear dimension and several hybrid aspects (e.g., cross-border terrorism, Islamic radicalisation). Operation Parakram was India's response to terrorist actions as a part of a strategy of coercive diplomacy.
25	Snap exercises and Crimea	Coercion through threat or use of force	Russian snap exercises during the annexation of Crimea were the latest in a string of exercises meant to show that the Russian Federation was ready for confrontation and to deter activity in its sphere of influence. Specifically, it was a case of 'pressure and shield' - pressure by indigenous insurgents, shielded by large combat ready forces across the border.
26	Electronic warfare during Zapad 2017	Territorial violation	In September 2017, parts of Latvia experienced a major cellular network outage. At around the same time, commercial aircrafts reported GPS outages while flying over Eastern Finnmark in Norway. Officials of both countries linked these incidents to Russian Electronic Warfare (EW) capabilities which were tested during the military exercise Zapad. Although experts concluded that the jamming was aimed at Russian forces during the exercise, and that spill-overs to neighbouring countries were likely unintended side-effects, officials pointed out that transparency would be desirable to avoid future misunderstandings.
27	Russian espionage in Sweden	Espionage and infiltration	According to the Swedish Security Service, Russian espionage activities in Sweden have been increasing since 2014. In many cases, attribution was not possible, not least due to the challenges attached to reporting on intelligence gathering. A crucial aspect is the (intended or unintended) information effect resulting from espionage activities: many commentators decried the development of what they consider national hysteria surrounding the issue, despite the substantial threat.
28	Religious extremism in the Netherlands	Religious groups	The Dutch intelligence and security service raised concerns in 2017 that, after being mostly stagnant for several years, the influence of extremist forms of Salafism was rising in the Netherlands. This manifested itself in an increase in hate speech and a shift from moderate Islam to fundamentalist teaching in mosques, increasing the threat of radicalisation and violence. The government needed to respond without creating a backlash against all Muslims, and transparently deal with cases of Gulf funding of religious outreach.
29	Cyber attacks on ROK & US	Cyber operations	In July 2009, tweaked versions of extant malware were used by the Democratic People's Republic of Korea (DPRK) to execute Distributed Denial of Service (DDoS) attacks to flood certain websites in the Republic of Korea (ROK) and the United States (US) with data traffic and make them unavailable.
30	Casas del ALBA in Peru	NGOs	In 2007, Peruvian officials accused the Venezuelan government of using development aid to interfere in its domestic affairs, claiming that in concert with Bolivia, Venezuela was supporting around 58 'ALBA Houses' (Casas del ALBA) in Peru. These houses provided charitable work such as literacy classes and healthcare to impoverished rural Peruvian communities. The Peruvian government argued that the ALBA Houses were promoting the Venezuelan regime, supporting left-wing extremism and inciting protests to subvert the Peruvian government.

# A STRATEGIC COMMUNICATIONS APPROACH TO HYBRID THREATS

This chapter outlines the overall approach guiding the research. It summarises the definitional challenges surrounding 'hybrid' terminology and introduces the concept of Strategic Communications as a function of basic statecraft.

## About hybrid threats

There is nothing new about the idea of using a wide range of instruments to achieve strategic ends without resorting to direct, interstate warfare.<sup>1</sup> Yet the character of warfare continues to evolve – the ongoing information revolution being a significant factor – offering adversaries new opportunities to exploit the spectrum of conflict beyond the utility of force.<sup>2</sup>

NATO understands the need to adapt and address these new modes of geopolitical rivalry but formulating distinctions has proven problematic. This is reflected in the variety of contexts that ‘hybrid’ terms are used in political discourse and the research community’s continued discussions regarding its essential nature.<sup>3,4</sup> Since being introduced to the lexicon of security and defence, the definitions of hybrid ‘threat’ and its close relations ‘war’ and ‘warfare’ have changed in tandem with the conflicts they have been used to describe.<sup>5,6</sup> Despite intense academic inquiry and widespread usage of the terms in NATO and national strategies, a consensus definition of ‘hybridity’ remains elusive.<sup>7</sup> This does not necessarily mean that the term should be abandoned, or that addressing the problem should be delayed until the labels are agreed upon. Despite the lack of conceptual clarity in definitions, the underlying phenomena the term encapsulates remain very real and a matter of urgent concern for the NATO nations.<sup>8</sup>

NATO defines hybrid threats as a ‘type of threat that combines conventional, irregular and asymmetric activities in time and space’.<sup>9</sup> This provides the essence of something produced by the synergy of different measures but used alone it is too broad. Most current definitions of hybrid threats lean heavily on Russian actions in Ukraine and Crimea, but this risks neglecting one of the key aspects of hybrid threats: adaptability. Hybrid threats do not follow a set pattern, and can be generated by a wide range of actors creatively using whatever means and measures available to achieve their strategic objectives. The adversary prefers to stay short of the threshold of conventional warfare but may eventually resort to the direct application of force. It should be expected that future threats will evolve in this way, with adversaries tailoring their means and measures to a targeted nation’s vulnerabilities.

A lack of conceptual clarity has meant that discussions over the nature of hybridity often become mired in narrow and outdated views of conflict, with the terms becoming merely an endeavour of political rhetoric, being ‘exaggerated, demonised and mobilised’ for political purposes.<sup>10</sup> This report takes a pragmatic approach which accepts a degree of conceptual obscurity but addresses the underlying security issues by focusing on the *characteristics* of hybrid threats. For the purposes of this research, hybrid threats are actions which:

- Are coordinated and synchronized
- Deliberately target democratic states’ and institutions’ systemic vulnerabilities.
- Use a wide range of means.
- Exploit the thresholds of detection and attribution as well as the border between war and peace.
- Aim to influence different forms of decision-making at the local (regional), state, or institutional level
- Favour and/or gain the agent’s strategic goals while undermining and/or hurting the target.<sup>11</sup>

Hybrid threats, by their very nature, are about creating effects that influence political decision-making. These effects can be diffuse, developing over a long period of time and not noticeable until it is too late. This ambiguity means that they can be difficult for governments to identify, attribute or publicly define because the responsible actor, or overall intent, is unclear or deliberately obscured.<sup>12</sup> Such activity is often described as taking place in the ‘grey zone’ between peace, crisis and war. It is often unlikely that governments will find ‘smoking gun’ evidence that provides credible and compelling proof of hostile intent, or be able to publish sensitive intelligence to support their analysis.

The way in which hybrid threats are interpreted and attributed is complex and significantly affected by context. For instance, an airspace violation can be regarded as either accidental or a deliberate act of provocation. Military exercises can be perceived as reassurance or deterrence and a foreign-sponsored political foundation can be seen as fostering intercultural exchange or undermining democratic values. These interpretations lead

to threat assessments that shape attitudes among publics and government officials alike. The judgement of whether an activity is considered hostile is ultimately a political decision taken by individual nations, with each nation seeing threats differently based on their own experience. This creates a challenge for how international organisations such as NATO and the EU should respond.

The realm of hybrid threats is therefore characterised by the interaction of information, perception, interpretation, and decision-making. An appreciation of how actors and audiences interact, form opinions and make decisions should therefore be the basis of understanding the hybrid threat environment.

## Hybrid threats as levers of influence

An inherent characteristic of any hybrid threat is a malicious intent to influence the attitudes and behaviours of key audiences, such as populations and political leaders. Mastering the dynamics of these levers of influence provides the basis for any government wishing to develop an effective strategy to protect their security interests and project power. Understanding this system requires a shift from focusing on the real, physical world, where events and actions occur, to the conceptual realm where information exists and communication takes place. This means placing less emphasis on 'real' domains such as land, sea and air, and adopting an approach which gives primacy to understanding actors, information and audiences, of which the physical world is one component. Such an approach would need to enable the analysis of a wide range of subjects, from energy dependency to military exercises.

To provide such a framework, this report proposes that hybrid threats be viewed as 'information' or 'influence' activities. These are actions which influence decision-making by creating changes in the conceptual system known as the *Information Environment* (IE). This is a term which is often used to refer to just the media environment but this belies the utility of it as a way of understanding how all actions (and non-actions) can influence decision-making. The IE is not, as many might understand it, a separate realm of contestation – changes in the IE influence physical actors and systems and vice versa.<sup>13</sup> The IE is a *conceptual space* consisting of three interrelated dimensions: **cognitive** (where people think, understand and decide); **physical** (individuals, organisations and infrastructure) and **informational** (facts, knowledge and data).<sup>14</sup> By this definition there is no limit on the IE and as it does not conform to spatial boundaries it is difficult to conceptualise both visually and verbally.<sup>15,16</sup> In essence the IE is a model for understanding how actors and audiences interact, how people see the world around them and consequently make decisions based on the meaning they deduce from it. Political leaders often instinctively think this way, such as when they refer to deterrence and reassurance measures. It is commonplace for actions to be described as 'sending a message' or a 'strong signal' but what is often lacking is a framework for placing such activities in the broader context of national strategy and integrating them with other measures in a coherent way.

Using the IE as a system to understand adversaries and the audiences they are likely to target is a departure from a more traditional approach which emphasises actions in the physical dimension with information as an afterthought. This challenges the 'DIME' model of national power (Diplomatic, Information, Military, Economic) which places 'Information' as a separate and apparently equal instrument.<sup>17</sup> All activities undertaken by an actor affect the IE and influence decision-making in the cognitive dimension. So, while information can be an enabler *to* national power, the ability to influence audiences comes *from* the synergy of national instruments, including diplomatic, military and economic measures. If these instruments are coordinated and work together harmoniously to achieve strategic objectives, the chances of success are increased and the less risk is assumed. The principles of Strategic Communications can enable this integration by understanding how hybrid threats affect the IE, then in response orchestrating statecraft in a manner that transcends traditional ministerial domains.

## Considerations for the different characteristics of hybrid threats

Characteristics	Description	Considerations
Coordinated and synchronised across a wide range of means.	<ul style="list-style-type: none"> <li>■ Activity which involves all instruments of national power: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal.</li> <li>■ Mixture of overt and covert, military and non-military, conventional and unconventional means; can involve state and/or non-state actors such as criminal groups and extremist organisations.</li> <li>■ Threats can be the result of a combination of different measures which create synergistic effects.</li> </ul>	<ul style="list-style-type: none"> <li>■ Nations should have the ability to continually monitor the Information Environment (IE), identify the use of measures and the reach and effect they have on key target audiences.</li> <li>■ A cross-government effort is needed to identify patterns and changes in adversarial behaviour.</li> </ul>
Deliberately targets democratic states' and institutions' systemic vulnerabilities.	<ul style="list-style-type: none"> <li>■ Vulnerabilities are weaknesses in a nation's system which can be political, military, economic, social, informational or infrastructure-related.</li> <li>■ Vulnerabilities can range from domestic shortcomings in security, infrastructure, or public goods and services, to social vulnerabilities such as cultural fracture lines or grievances.</li> </ul>	<ul style="list-style-type: none"> <li>■ Vulnerabilities should be continually assessed and addressed across the full range of critical functions.</li> <li>■ Build resilience with a whole-of-society approach, including civil society, private sector, media organisations, NGOs, think tanks.</li> <li>■ Nations should be aware that their relationship with other states may be the target.</li> </ul>
Exploits the thresholds of detection and attribution as well as the border between war and peace.	<ul style="list-style-type: none"> <li>■ Attribution of responsibility can be challenging, and the degree of state involvement may be unclear.</li> <li>■ Thresholds of war and peace can be stretched depending on context.</li> <li>■ Blurred lines between peace and conflict and between normality and crisis hamper identification and attribution.</li> </ul>	<ul style="list-style-type: none"> <li>■ Attribution is a political endeavour.</li> <li>■ Attribution should be done on a case-by-case basis and relies on government credibility to be convincing.</li> <li>■ Importance of legal domain in supporting arguments.</li> <li>■ Attribution and monitoring should not impede free speech.</li> </ul>
Aims to influence different forms of decision making at the local (regional), state, or institutional level.	<ul style="list-style-type: none"> <li>■ Can target public opinion or officials on the local or national level.</li> <li>■ Local / municipal level institutions can be especially vulnerable as they often do not receive the same attention as national issues.</li> <li>■ Exploits lack of accountability and transparency or poor governance.</li> </ul>	<ul style="list-style-type: none"> <li>■ Governments should build resilience at all levels of government through awareness building and training.</li> <li>■ Vulnerability assessments need to be comprehensive and conducted on a regular basis.</li> <li>■ Identify potentially vulnerable target audience groups and plan resilience strategies accordingly.</li> </ul>
Designed to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.	<ul style="list-style-type: none"> <li>■ Hybrid activity may be used to directly achieve strategic objectives, but may not necessarily be an end in itself; it may serve to generate influence by investing in actors or networks.</li> <li>■ Aimed at changing the behaviour or attitudes of the government or population in a way that damages national security interests.</li> </ul>	<ul style="list-style-type: none"> <li>■ Understand the overall strategic logic of adversaries.</li> <li>■ Attribution needs to be clear and supported by the maximum amount of releasable information or intelligence.</li> </ul>

# The Strategic Communications mindset

'Strategic Communications' (and Strategic Communication) is a label which is applied to different, yet related functions. It can be used to refer to both the internal machinery that coordinates cross-government communication activities and the communications themselves. This report focuses on the former and for simplicity suggests a generic definition of Strategic Communications as the 'coordination of actions, words and images to influence the behaviour and attitudes of key audiences to achieve strategic goals.'<sup>18</sup> It is understood predominantly as a *mindset* but also as a *process* and a *capability*.<sup>19</sup>

The boundaries between the different facets of Strategic Communications are blurred and this is reflected in the ongoing debate as to whether Strategic Communications should be considered as the "communication of strategy, or communication as strategy".<sup>20</sup> In the former, the role of communication is limited to the implementation of strategy, in a predominantly subordinate role. The strategists decide on the strategy and then coordinated activities such as press conferences and media campaigns message in support, typically as a reactionary measure in times of crisis. It is in this context of a coordination *capability* that policy-makers refer to 'getting the right message out' and 'counter-narratives'. Yet this perspective neglects the ways in which every government activity communicates, including actions, words and policies.

By contrast, communication as a primary instrument of strategy is considered as an integral part of government decision-making from the outset and placed at the heart of strategy development. Strategic Communications when applied as a *process* enables this by focusing on audience insight and providing a unifying lens to understand the full array of adversarial measures, how they are interpreted, affect perceptions and influence decision-making. This forms the basis of a response which incorporates all available means and ways to build societal resilience, forge international coalitions and attribute threats effectively.

The process of Strategic Communications can therefore provide a more effective orchestration of government activity to drive and coordinate decision-making in a way favourable to the national interest. It needs to be endorsed as a guiding principle across all government departments and levels in order to be practiced efficiently. This principle is encapsulated in the articulation of Strategic Communications as a philosophy or *mindset*. This is an appreciation that everything communicates, therefore everyone in government is responsible for what is being communicated.

The application of Strategic Communications as a process can act as the connecting membrane between strategy and action, integrating efforts across government and enabling unity of effort towards common strategic ends. Such an approach would maximise the use of available resources and reduce the risk of failure. This requires a Strategic Communications mindset absorbed into all levels of government and views foreign policy through the lens of communication, identifying relevant audiences and understanding how they form opinions and make decisions. There will inevitably be specialist capability requirements, such as assessment and analysis of the IE, or the planning and integration of cross-government activities such as media handling, marketing, and engagement. However, rather than assigning the responsibility of Strategic Communications to a single entity, governments would benefit from fostering a culture that communication is core business.<sup>21</sup> In this way, when the mindset is stronger, less process is required.<sup>22</sup>

In practice, these two approaches – communication at the core of strategy development or subsequently in the implementation phase – are not mutually exclusive. They are often integrated to varying degrees, either deliberately or as a characteristic of how governments function. This is reflected in the balance that governments need to find between expanding their pool of specialist communications capabilities and encouraging a Strategic Communications culture which is integral to every department, policy and strategy.<sup>23</sup>

# Strategic Communications at the national level

This report does not propose that those working in the field of Strategic Communications at the national level make a bid to take over the functions of government that define the means and ways of strategy. It proposes that every hybrid threat can be considered as an act of communication, ultimately influencing political decision-making in a way which benefits the adversary and hurts the targeted nation. The underlying concepts and principles of Strategic Communications can therefore provide a useful guide to effective statecraft in understanding, identifying and countering hybrid threats.

The most important principle that underpins Strategic Communications is the requirement to **understand the Information Environment**. Considerations of human perception should be central in understanding the dynamics of hybrid threats, how they are perceived, interpreted and attributed. It is clearly not feasible to consider the entirety of the IE, therefore analysis should be focusing on relevant topics and on the constituent parts of a hybrid threat: *actors* (political leaders, civil society, military), *channels* (military, information, law, cyber, economy) and *means* (disinformation, cyber attacks, bribery) and understanding how these might exploit vulnerabilities to damage national security interests. Continuous assessment should establish baselines of normality and identify changes in patterns. This demands information sharing both within and between governments and the ability to synthesise different types of intelligence and information. Implicit in any assessment of the IE is the ability to assess the effectiveness of government activities to inform adjustments to strategy.

Communication should be a whole-of-government activity which is **collective and integrated**. Based on a comprehensive understanding and continuous assessment of the information environment, governments should have a clear understanding of what measures and means are available to reach key audiences. This could be anything from economic sanctions to a change in military force posture. These should be integrated and employed in a coherent manner to achieve desired strategic effects and outcomes.

Actions taken to address hybrid threats should be guided by a **strategy**. Communications considerations should be at the centre of the development and implementation of strategy from the outset and this process should be supported by the availability of appropriate resources, particularly qualified personnel. National strategy should have a broad consensus of support amongst the population and be endorsed from the top down by political leadership. This includes formulating the strategic position a nation wishes to take and how it intends that to be articulated across the whole of government, including ministries such as culture, education and home affairs. Such an approach ensures that whatever 'story' (or national narrative) the government wishes to communicate is empowered at all levels, coherent and consistent.

National authorities need to have structures that are **flexible, decentralised and adaptive** and able to emphasise preparation, agility and responsiveness. The nature of hybrid threats means there are no set playbooks or manuals that can be followed. Adversaries will continue to develop, test and employ measures that target vulnerabilities wherever they materialise. Rather than establishing formal structures, fostering a culture of Strategic Communications across all government departments will allow a nation to retain the initiative.

Attributing hybrid threats to an adversary is a political endeavour which relies on the trust of the public, so **credibility should be protected as a vital resource**. Any government action which needlessly erodes public confidence will limit the courses of action available to both prepare and respond to hybrid threats. Government branches should understand that even if there is no obvious connection between their particular area of responsibility and national security, their actions can weaken national resilience.



---

#### Endnotes

- <sup>1</sup> For background and examples see Frank G. Hoffman, "The hybrid character of modern conflict", in *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict*, Council for Emerging National Security Affairs (2011). Kindle version, locn 716.
- <sup>2</sup> For an overview see Bruce D. Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology* 12, no.1 (1995), 59–66.
- <sup>3</sup> Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism. The Journal of Complex Operations* 7, no. 4 (2018), 31-47.
- <sup>4</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018).
- <sup>5</sup> Most scholars attribute the term to William J. Nemeth in *Future War and Chechnya: A Case for Hybrid Warfare* (Monterey: Naval Postgraduate School, 2002).
- <sup>6</sup> Patrick Cullen and Erik Reichborn-Kjennerud, *Countering Hybrid Warfare Baseline Assessment* (Multinational Capability Development Campaign (MCDC) 2015-2016, October 2016), 5.
- <sup>7</sup> *Ibid.*
- <sup>8</sup> Elie Tenenbaum, "Hybrid Warfare in the Strategic Spectrum: A Historical Assessment". Chapter in 'NATO's response to Hybrid Threats', eds Guillaume Lasconjarías and Jeffrey A. Larsen (NATO Defense College 2017) p112.
- <sup>9</sup> NATO Standardization Office (NSO), AAP-6, *NATO Glossary of Terms and Definitions* (2018 edition), 62.
- <sup>10</sup> Benjamin Tallis and Michal Šimečka, *Collective Defence in the Age of Hybrid Warfare* (Prague: Institute of International Relations, 2016).
- <sup>11</sup> Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE, 2018), p10.
- <sup>12</sup> Andrew Mumford and Jack McDonald, *Ambiguous Warfare*, report produced for the Development, Concepts and Doctrine Centre, October 2014.
- <sup>13</sup> Christopher Paul, Colin P. Clarke, Bonnie L. Triesenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* (Santa Monica: RAND Corporation, 2018), ix.
- <sup>14</sup> U.S. Joint Chiefs of Staff, Joint Publication 3-13: Information Operations, incorporating change 1 (Washington D.C., 2014), 1-2.
- <sup>15</sup> Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 253.
- <sup>16</sup> Christopher Paul, Colin P. Clarke, Bonnie L. Triesenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* (Santa Monica: RAND Corporation, 2018), 3..
- <sup>17</sup> The UK, for instance, defines only three instruments of power – diplomatic, military and economic – with information considered as an enabler for all of them (see UK Ministry of Defence (MOD), *Joint Doctrine Note 1/12: Strategic Communication: The Defence Contribution* (Swindon: The Development, Concepts and Doctrine Centre, MOD, 2012). NATO Standardization Office (NSO), AJP-01, NATO Allied Joint Doctrine (February 2017) considers information as a separate instrument and says StratCom is 'delivered through the instruments of power via policy, words and actions is an important element of operations planning and execution', 1-3.
- <sup>18</sup> Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates* (Santa Barbara: Praeger, 2011).
- <sup>19</sup> For more on this see Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016; Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates* (Santa Barbara: Praeger, 2011) and UK Ministry of Defence (MOD), *Joint Doctrine Note 1/12: Strategic Communication: The Defence Contribution* (Swindon: The Development, Concepts and Doctrine Centre, MOD, 2012).
- <sup>20</sup> Kenneth Payne, "Thoughts on the Psychology of 'Strategic Communication,'" Paper presented at the KCL Insurgency Research Group and CIWAG US Naval War College Conference, 'Strategic communications: the Cutting Edge,' 10 May 2011.
- <sup>21</sup> Paul Cornish, Julian Lindley-French and Claire Yorke, *Strategic Communications and National Strategy: A Chatham House Report* (London: Chatham House, The Royal Institute of International Affairs, September 2011).
- <sup>22</sup> Brett Boudreau, *We have met the enemy and he is us* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 276
- <sup>23</sup> Paul Cornish, Julian Lindley-French and Claire Yorke, *Strategic Communications and National Strategy: A Chatham House Report* (London: Chatham House, The Royal Institute of International Affairs, September 2011).

# Research approach

**Problem statement.** The start point for this research is a requirement for NATO nations to better understand and counter the broad range of threats they face from state actors, which sit in the low-intensity, indirect end of the spectrum of influence. Such threats, in certain circumstances, may be a precursor to the use of conventional military force but are predominantly characterised by the use of different instruments to undermine and weaken the governing authority without resorting to open conflict. National authorities therefore require the ability both to identify when such threats materialise and to integrate and coordinate all measures available in response.

**Purpose.** This publication provides the first large-scale systematic analysis of hybrid threats, covering a wide spectrum of different methods of influence, across a range of geographic regions. It broadens the framing of most previous research beyond the common empirical reference points relating to the behaviour of the Russian Federation. The findings and recommendations aim to assist decision-makers, practitioners and policymakers working at the national level develop an effective approach to prepare for, identify and respond to hybrid threats which is based on the underlying concepts of Strategic Communications.

**Selection of case studies.** Initial research identified over 250 scenarios assessed as featuring activity which was potentially an example of a hybrid threat. These activities may have impacted national security interests by exploiting a vulnerability and affecting a nation's critical functions, i.e. by weakening the military, economic or political strength of a governing authority. The inclusion of an actor in a scenario does not necessarily mean that their actions were intended to be hostile. Part of the research was therefore to interrogate this proposition of hostility and also accept that the results may not necessarily be conclusive.

**Analysis of case studies.** With over 250 scenarios identified, this research is based on a large selection of case studies. However, ambiguity as a key characteristic of hybrid threats impedes a quantitative analysis. The research methodology employs a mixed-methods qualitative approach. Individual case studies have been conducted by experts in the respective regions with the necessary language skills and background information. The researchers conducted interviews with subject matter experts and all case studies have been peer-reviewed. To ensure the comparability of the findings, a standard analytical framework, developed through a series of workshops, has been applied. The different components of the analytical framework cover the analysis of contextual factors, key actors, themes and narratives as well as the range of measures employed, their underlying strategic logic and the potential impact of these activities on national security interests.

**Categorisation of case studies.** Sixteen areas of thematic threat were identified to group case studies together for analysis. The thematic areas are designed as a typology to serve as a framework to help understand the wide range of means and ways that hybrid activity can manifest itself – military and non-military, conventional and unconventional, overt and covert, state and non-state. The thematic areas often overlap, as hostile influence usually involves more than one thematic area.

# OVERVIEW OF ANALYTICAL FRAMEWORK

## CONTEXT

This section provides an overview of background knowledge that needs to be understood in order to appreciate narratives and actor behaviour against the background of broader historical and political developments relevant to the case.

## ACTORS AND NARRATIVES

This section identifies key actors and looks at the core themes and narratives of all parties involved.

## MEASURES

This section looks at all measures employed by an adversary, and the strategic logic behind the application of different instruments of power.

The **STRATEGIC LOGIC** describes the underlying thinking and calculation of adversarial measures. Different measures are broken down into functional components according to the DIMEFIL spectrum: diplomatic, information, military, economic, financial, intelligence and legal.

**Diplomatic.** The principal instrument for engaging with other states and foreign groups to advance values, interests, and objectives, and to solicit foreign support. The credible threat of force reinforces, and in some cases enables the diplomatic process.<sup>1</sup>

**Information.** Information remains an important instrument of national power and a strategic resource critical to national security.<sup>2</sup>

**Military.** The use of military capabilities, predominantly through coercion generates effects through the application of force (to include the threat of force) to compel or deter an adversary. The military also has capabilities that can be used in non-conflict situations.<sup>3</sup>

**Economic.** The use of economic inputs and flows to influence decision-making.<sup>4</sup>

**Financial.** The control of the creation, flow, and access to "stores of value" wields power. Although finance is generally an operation of real and virtual currency, anything that can serve as a "medium of exchange" provides those who accept the medium with a method of financial transaction.<sup>5</sup>

**Intelligence.** Intelligence, as an instrument of national power provides the national leadership with the information needed to realise national goals and objectives while providing military leadership with the information needed to accomplish missions and implement national security strategy. Planners use intelligence to identify the adversary's capabilities and centres of gravity.<sup>6</sup>

**Legal.** The attitude of the population, degree of control provided by competing (non-state government) enforcers of law, and traditions of civic order – or lack thereof – are key components of the overall law enforcement environment. All of these varying conditions will contribute to the degree of lawlessness in any given society.<sup>7</sup>

## NATIONAL SECURITY INTERESTS

This section looks at the outcomes and effects of adversarial measures. This is a series of lenses to facilitate a '360 degree' view of a situation and to assess any impact of adversarial measures. Consideration is given to the different levels (local, regional, national) at which effects are assessed to have occurred. The main area of focus is the effects section, particularly on political decision-making, public opinion and the development of themes and narratives.

A **critical function** is something that the nation is trying to protect or sustain. Critical functions are activities or operations distributed across the PMESII spectrum which if affected could lead to a disruption of services that a working system such as a state and its society depends on. Critical functions can be broken down into a combination of actors, infrastructures (such as national power grids) and processes (for example legal, technical, political).<sup>8</sup>

A **vulnerability** in a critical function presents an adversarial actor with a possible condition for exploitation, depending on the means at its disposal.<sup>9</sup> Any factors associated with a weakness in the critical function of a nation may be considered a vulnerability. Vulnerabilities can therefore be anything from lack of public trust in the government to high reliance on technology.

A **threat** is anything that can exploit a vulnerability and achieve an effect or effects on a critical function. A threat to national security is an action or a sequence of events that 1) threatens drastically and over a relatively brief span of time to degrade the quality of life for inhabitants of a state or 2) threatens significantly to narrow the range of policy choices available to the government of a state, or to private, non-governmental entities (persons, groups, corporations) within the state. A threat is what the nation is trying to protect against.

An **effect** is a change in behaviour or state of a system and is the outcome or impact of a threat. Describes short term effects on target(s) behaviour. Assessing this change requires a baseline or status quo for comparison. Where possible, longer term effects are considered.

<b>Political.</b> Relating to the distribution of responsibility and power at all levels of governance – both formally constituted authorities and informal or covert political powers.	<b>Military.</b> Relating to the military and paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given environment.	<b>Economic.</b> Individual and group behaviours related to producing, distributing, and consuming of resources.	<b>Social.</b> The cultural, religious, and ethnic makeup within a bounded environment and the beliefs, values, customs, and behaviours of society members.	<b>Information.</b> Describes the nature, scope, characteristics, and effects of individuals, organisations, and systems that collect, process, disseminate, or act on information.	<b>Infrastructure.</b> The basic facilities, services, and installations needed for the functioning of a community or society.
--	--	---	--	--	---

<sup>1</sup> "Instruments of National Power," *The Lightning Press*, website accessed 29 October 2018.

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

<sup>4</sup> US Headquarters Department of the Army, *Army Special Operations Forces Unconventional Warfare*, September 2008.

<sup>5</sup> Ibid.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Patrick J. Cullen and Erik Reichborn-Kjennerud, *Understanding Hybrid Warfare*, Multinational Capability Development Campaign Project, January 2017.

<sup>9</sup> Ibid.

# KEY FINDINGS AND RECOMMENDATIONS

This chapter presents the main lessons identified from the research. The findings are cross-referenced to the 30 case studies that follow. This chapter also outlines a typology of different threats.

# 10 key recommendations

## 1. Everything communicates

**All policies, actions and words influence decision-making, therefore communication should be integral to strategy and considered from the outset of planning. National authorities preparing for, and responding to, hybrid threats should appreciate that communication is not limited to words – every action (or inaction) can influence the attitudes and behaviours of key audiences. Strategic Communications is therefore not limited to certain functions and capabilities – such as public affairs and press offices – but is an organisational responsibility, with everyone working to achieve desired outcomes derived from overarching objectives.**

Communication is not just what is said. Images, actions and policies all have an information effect. Actions – both your own, and those of an adversary – can be perceived to ‘send a message’, intended or not. Decision-makers need to recognise the importance of integrating communication into planning from the outset, and be adequately supported and trained by experienced communications practitioners.

- Military force posture and presence can achieve strategic information effects such as deterrence, reassurance or disruption: *Operation Parakram (24), Snap exercises and Crimea (25)*
- When an adversary government does not react to accusations of hostile or disruptive activity, this can imply hostile intent, especially when silence is deliberately used to increase uncertainty and confusion: *Electronic warfare during Zapad 2017 (26)*
- High-profile responses, such as formal investigations into hostile activities, can send a strong political statement and build resilience by deterring malign influence: *Casas del ALBA in Peru (30)*

**Audience insight.** Care must be taken to understand the diversity of audiences, their attitudes, values, motivations and – importantly – where their trust lies. Nations should adequately resource target audience analysis and invest in personnel with language skills and in-depth knowledge of history, religion and cultural norms. This knowledge should be applied to monitoring and analysis, and used to support Strategic Communications planning and the development of credible and resonant narratives.

- Efforts to change audience attitudes and behaviours can be more persuasive and cost-effective when organisations have an in-depth understanding of the issues that people really care about: *US Transit Center at Manas (4)*

**The messenger matters.** Whether a message is promoted by high-ranking politicians, subject-matter experts, academics, celebrities, or religious leaders has a profound effect on how the message is interpreted by an audience. Similarly, the medium chosen for the message – be it an online awareness campaign, a political speech, or a movie – can change the impact of a message. Audience insight is crucial to understand how different messengers might change the way in which a message is interpreted, which specific key groups hold the balance on opinions, and which information channels are the most used and trusted.

- In cases where official channels are likely to have a minimal effect on key audiences, governments should identify and work together with civil society groups that might be more effective messengers: *Religious extremism in the Netherlands (28)*

## 2. Whole-of-government

Hybrid threats are generated from a mix of adversarial measures to influence political decision-making of the targeted nation, therefore an integrated approach across government is needed to effectively identify and address such threats. What works in one situation may not work in another, so governments need to be agile and able to anticipate and identify potential threats, then integrate and coordinate their response across a range of levels and channels. This requires timely decision-making and a coherent, sustained response to reinforce government credibility and legitimacy.

**Work across departments.** To identify and counter hostile measures from malign actors, responses need to be coordinated across government and span the civil-military divide. Different branches of government should establish mechanisms for effective cooperation and use synergies to their full potential.

- Identifying and countering potential threats requires the ability to assess adversarial activity across the full spectrum of military and non-military means to understand an adversary's overall objectives: *US Transit Center at Manas (4)*, *The 2010 Senkaku crisis (8)*, *Bronze night riots (19)*
- Lack of information sharing and cooperation between civilian and military authorities limits the government's ability to effectively determine and pursue its objectives: *Operation Parakram (24)*
- Preparation for disruptive events, such as cyber attacks, should focus on credible, factual responses consistent across national authorities, stressing civil preparedness: *Electronic warfare during Zapad 2017 (26)*

**Empower and enable all levels.** Responsibility for communication does not only lie with high-level officials and spokespeople: in today's fast-paced and networked media environment, statements by regional officials and even by low-ranking soldiers on the ground can be influential or be exploited by hostile actors to legitimise a specific point of view. Governments should consider training officials to refrain from making statements which undermine the overarching narrative, and to be mindful of the impact their individual actions and statements might have.

- Improving awareness of information-based threats and developing media presentation skills through training across government and at the lowest levels of national authorities will help officials make statements that are not open to misinterpretation: *Disinformation in Sweden (6)*

**Consistency.** Aligning words and deeds is of fundamental importance for coherent government messaging. Inconsistent messaging due to a lack of strategy, poor coordination, or attempts to cater to different audiences, can result in a say-do gap which undermines an actor's overall credibility. Messaging (including actions) across national authorities, while tailored to address specific audiences, should consistently reflect overarching themes.

- When information from different official channels contradicts each other, this fundamentally affects trust in government communication and leaves room for doubt and alternative interpretations: *Civil disorder in Bahrain 2011 (22)*
- Balancing competing demands of domestic and international audiences can result in information fratricide, especially when words are not aligned with actions: *Pakistani involvement in Yemen (23)*
- When two or more countries face similar or identical hybrid threats, efforts to align narratives and coordinate approaches would help present a unified front: *Cyber attacks on ROK & US (29)*

### 3. Understand the strategic logic

In order to understand an adversary's strategic logic, national authorities should grasp the underlying thinking and calculation behind adversarial measures. This entails assessing their potential aims, and the way in which different instruments are integrated and synchronised to achieve these objectives. Such an understanding would allow governments to identify potential vulnerabilities and key target audiences, anticipate future developments through horizon scanning, and adjust their preparation and response.

**Long-term aims of adversary.** Taking a '360 degree' approach will help decision-makers situate an activity within larger systematic efforts and strategies, and shed light on an adversary's underlying motivations and goals. By monitoring activities across the full spectrum of adversarial measures, decision-makers will be able to identify how the adversary's aims and information activities align and gauge their success or failure. Once the overall strategic logic is better understood, decision-makers will be able to better develop their strategy accordingly.

- An adversary's long-term goals may be unclear (they might not even be clear to the adversary). Hybrid activity often operates opportunistically and may not have any specific immediate objective other than generating influence in another country by investing in the potential of actors and networks: *Ruskiy Mir Foundation in the Baltics (20)*

**Modus operandi and toolkit of adversary.** Governments should have a thorough understanding of their adversary's capabilities and methods, to develop knowledge of how potential threats fit within their existing toolkit and serve their long-term aims. This includes looking at historical patterns of behaviour, analysing where an adversary might be testing defences, and identifying actors with aligned interests that the adversary could employ as agents or useful allies.

- Examining whether a specific tool – such as ambiguous cyber operations, or the providing of 'humanitarian' assets – has been used systematically by a state actor in different contexts and against different countries can be of use when trying to determine hostile intent: *2007 cyber attacks on Estonia (3), Humanitarian aid in the Russo-Georgian conflict (9)*
- Hybrid threats are often opportunistic. A typical approach might be to create pressure or intensify social divides, and then take advantage of crises once they emerge. Similarly, a small uncalculated incident might be exploited and deliberately escalated into an international incident for strategic gain: *The 2010 Senkaku crisis (8), Bronze night riots (19)*
- Potentially hostile civil society groups are often modelled on Western cultural institutions and soft power approaches, but might be aimed at undermining the cohesion of the host nation: *Institute of Democracy and Cooperation (15), Ruskiy Mir Foundation in the Baltics (20)*

**Identify potential key target audiences for adversarial activity.** Understanding the strategic logic and aims of adversaries will enable decision-makers to better anticipate the potential target audiences of their activities. It is also important to consider that the primary target audience may be local to the hostile actor, such as domestic public opinion.

- Decision-makers should identify actors with aligned interests who could be used by an adversary as agents, channels or mouthpieces: *Serbian Orthodox Church (17)*

## 4. Determine what you want to protect and identify vulnerabilities

Hybrid threats deliberately target and exploit existing vulnerabilities of the target state, often opportunistically. Domestic issues such as systemic corruption and social divisions can be exploited by malign state actors. Weakness in national security institutions and a lack of public confidence in government may be seen as domestic political issues, but these vulnerabilities enhance the ability of hostile actors to affect critical functions and damage national security interests. Nations should continually assess their vulnerabilities in an honest and transparent manner and articulate this in national security policy.

**Physical vulnerabilities in services and infrastructure.** Hybrid threats target a state's physical weaknesses; these can be deficiencies in areas such as cyber security, transport and communication infrastructure, or essential goods and services to the population.

- A common technique to influence foreign populations is to step in where the government has failed to provide services such as healthcare and education. Development aid programmes are then used to promote a particular political system or ideology, while simultaneously delegitimising the target state government: *The spread of Salafism in Egypt (5)*, *Casas del ALBA in Peru (30)*
- Unresolved territorial disputes and insufficient border security open up opportunities for deliberately ambiguous activities: *The 2010 Senkaku crisis (8)*, *Detention of Eston Kohver (11)*, *Finnish airspace violations (12)*

**Vulnerabilities concerning governance and sovereignty.** Shortcomings in a state's ability to exert control over its territory, guarantee law and order, manage crisis situations, or make independent policy decisions can enable foreign actors to exert malign influence.

- Economic or energy-related dependencies on another state can induce or coerce a government into making decisions that negatively affect national security interests: *US Transit Center at Manas (4)*, *South Stream Pipeline (13)*, *Pakistani involvement in Yemen (23)*, *Zambian elections 2006 (16)*
- Domestic vulnerabilities such as pervasive corruption, lack of financial or political transparency, and inadequate legal frameworks, not only invite hostile influence activities, but also impede the government's ability to investigate and counter these activities: *The spread of Salafism in Egypt (5)*, *South Stream Pipeline (13)*, *Criminal Networks in the Donbas (21)*

**Social vulnerabilities.** A lack of social cohesion can expose fracture lines that can be exploited by hostile actors. Vulnerabilities include disagreements on what constitutes national identity, different interpretations of history, sectarianism, or radicalism and violent extremism.

- Existing polarisation between identity groups which is based on religion, political ideology or ethnicity can be exploited by hostile actors; governments face the additional challenge of calling out foreign influence without exacerbating divisions: *Russian language referendum in Latvia (14)*, *Bronze night riots (19)*, *Serbian Orthodox Church (17)*
- Social grievances, such as certain groups feeling excluded or discriminated against, are easily instrumentalised to incite discord and civil unrest: *Bronze night riots (19)*, *Civil disorder in Bahrain 2011 (22)*
- Hostile actors can capitalise on insufficient trust in government and media organisations, or exploit a general sense of insecurity and uncertainty present in public discourse: *Criminal Networks in the Donbas (21)*, *Russian espionage in Sweden (27)*



## 5. Build resilience

Resilience in the context of this study describes the ability of a state and society to withstand pressure and recover from crises or shocks which may be the result of a hybrid threat. Improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost-benefit calculation. Deterrence through resilience is therefore a key component of reducing a nation's susceptibility to hybrid threats.

**Patch 'holes in the fence'.** Countering every hostile measure itself is not a sustainable solution, as hybrid threats are highly adaptable, and might continue to target vulnerabilities in different ways. Tackling these vulnerabilities head-on is the first and crucial step for governments to build resilience and make it harder for hostile influence to gain a foothold. Effective communications can help raise public awareness, get stakeholders to agree on the nature of the problem, and generate sufficient political will-power to address the vulnerabilities in question.

- Depending on the vulnerabilities identified, addressing these root problems often demands a sustained and focused effort, which requires adequate resourcing. Eliminating systemic corruption or making up for deficiencies in healthcare and education takes time and political will. Governments can take the lead by raising awareness of vulnerabilities, threats, and the need for resilience-building – both within different government departments and amongst the wider public: *Casas del ALBA in Peru (30)*
- Countries that feature social groups with historical, ethnic or cultural ties to potentially hostile state actors should avoid the unnecessary politicisation of contentious issues and instead focus on common values, shared historical experience and an inclusive vision of the future. This will increase the overall sense of national belonging and frustrate hostile efforts to hamper integration or promote separatist ideals: *Chinese public diplomacy in Taiwan (10), Russian language referendum in Latvia (14), Bronze night riots (19)*

**Whole-of-society.** To tackle domestic issues and build resilience, governments should work together with the private sector, media, NGOs and academia. This will enable the public to be better informed and contribute to inclusive policy-making, and develop an awareness of malicious influence intended to harm the nation.

- The issue of hostile influence through political actors is best addressed by civil society and independent media rather than the government, to avoid the impression of a biased, politically-motivated persecution of a particular party or politician: *The spread of Salafism in Egypt (5), Communist Party of Bohemia and Moravia (18)*
- A healthy and diverse media, both state-funded and independent, and fact-checking organisations, will be able to provide multiple open-source verifications or validations of incidents and events: *US Transit Center at Manas (4)*

**Work with partners.** Hybrid threats are an international issue. National resilience and deterrence are strengthened by forging strategic alliances with international partners which share a common interest in identifying and countering potential threats. Governments should encourage and enable information sharing between nations and integrate those mechanisms to identify and respond to threats at the international level in a coordinated and united manner.

- Many countries share similar security concerns. Governments should support each other in the face of hybrid threats, encourage information exchange, and create joint expertise-based institutions to build a unified front: *2007 cyber attacks on Estonia (3)*
- Threats can be deliberately aimed at weakening a state's relations with other countries, or its commitment to international organisations and institutions: *South Stream Pipeline (13)*

## 6. Activity should be based on values, with clear objectives

Governments need to be clear about their strategic aims and ensure that statements and actions are consistent with core values. They should understand that employing measures or taking positions which appear to be deceptive or inauthentic will undermine their credibility. Democracies should also be aware that appearing to deal harshly with a suspicious actor – such as with civil society or media organisations – might provide the justification for autocratic governments to crack down on disagreeable foreign-sponsored NGOs or media outlets in their own country.

**Uphold democratic values.** Democracies – due to their commitment to freedom of speech, their respect for national and international law, and their accountability to the population – often find themselves at a disadvantage when addressing hybrid threats. This might be due to lack of evidence connecting a suspicious organisation to a hostile foreign actor or proving hostile intent. Legal obstacles can constrain a government's freedom of action in shutting down suspicious civil society organisations, and rightly so. Governments must therefore align their actions with core democratic values, and conduct any investigation in a transparent manner, to bolster their credibility and legitimacy.

- Shutting down or outright banning a suspicious media outlet, political party, or civil society organisation is often not an option for a democratic government. Governments should instead focus on involving civil society in the surrounding debate, and let it point out anti-democratic ideas and groups: *Confucius Institutes (2)*, *Disinformation in Sweden (6)*

**Listen to critical voices.** Governments should plan to incorporate critical voices from neutral or friendly actors into their communication strategy. Governments should anticipate likely lines of argument and take them into account when formulating strategy, which will both increase trust in democratic processes and leave less room for hostile foreign influence to alienate groups from the government.

- Domestic criticism and protests are a normal and healthy part of democracy. It will only benefit adversaries when governments do not take them seriously or try to dismiss them as foreign-sponsored agitation: *Civil disorder in Bahrain 2011 (22)*
- There is likely to be criticism at how foreign influence is handled by the government – some will claim that the government has reacted too harshly and unnecessarily disrupted bilateral relations, while others will criticise that the government's stance has been too weak. Governments should anticipate these lines of argument, and be able to explain in clear terms which considerations led them to choose a specific course of action: *The 2010 Senkaku crisis (8)*, *Zambian elections 2006 (16)*

**Have specific and achievable end goals.** Having realistic and clearly defined strategic aims is vital for coherent communication and unity of effort. All activities should then be nested under this common purpose. Governments should ensure that both proactive and responsive strategies aimed at countering hybrid threats are based on clear and achievable goals, which will enable measurement of progress and the evaluation of outcomes.

- Without clearly stated objectives which are time-bound, it is difficult to maximise the use of resources, maintain coherence and credibility, and sustain public support for prolonged periods of time: *Operation Parakram (24)*

## 7. Be proactive

A proactive approach would enable governments to maintain dominance over evolving narratives and frame events in a manner favourable to their interests. Instead of merely responding to threats as they materialise, governments should anticipate events and issues that are likely to be exploited by adversaries. This can reduce risk by not merely 'countering' an adversary's activities, but pre-emptively steering public discourse in a preferred direction and building resilience, thus reducing the likelihood of unintentionally reinforcing an adversary's preferred narrative of events.

**Prepare through scenario-based training.** Likely scenarios can be mapped out and possible courses of action evaluated with up-to-date target audience analysis, to get an understanding of the possible information effects and outcomes of different decisions. Scenario-based training should be grounded in a comprehensive analysis of the information environment to identify the most appropriate channels of communication and prepare responses for negative themes that are likely to arise.

- In the event of negative themes such as divisive arguments or disinformation arising, responses with key facts and nuances of the situation explained can be quickly presented to media and disseminated in order to mitigate effects of disinformation: *Hamas' use of human shields in Gaza (7), Electronic warfare during Zapad 2017 (26)*

**Expect the unexpected.** By their very nature, hybrid threats can be complex and adaptive. Therefore, governments need to have the institutional capacity to deal with such evolving security challenges, with systems and processes in place that are agile enough to adapt to different actors and changing tactics. The right mindset – both an understanding of hybrid scenarios, and a Strategic Communications approach – would enable governments to quickly detect threats and act in an adequate and efficient manner.

- Based on existing vulnerabilities and tensions with other states – e.g. unresolved border disputes, or stationing of unwelcome foreign troops in the vicinity – governments should anticipate likely scenarios and themes in order to have response mechanisms and communication strategies in place: *The 2010 Senkaku crisis (8)*

**Beware of reinforcing adversary narratives.** Governments should consider how a proposed action or message might serve an adversary's narratives. Attempting to directly 'counter' hostile narratives can reinforce the particular framing of a situation in a way that lets an adversary set the agenda and supports their objectives. Similarly, debunking disinformation can sometimes be counterproductive, as it will give the narrative in question greater prominence. It is therefore important for governments to consider the appropriate frame, medium and messenger. For instance, whether an action or response is taken by a high-level political actor or by subject-matter experts can have a crucial informational effect.

- By analysing a territorial violation on a purely safety-related and technical level rather than on a political level, governments can try to de-escalate tensions and alter the perception of an incident: *Finnish airspace violations (12), Electronic warfare during Zapad 2017 (26)*
- Governments should consider if their proposed actions and messages could be used to reinforce and amplify an adversary's narrative – for example, of 'Russophobia', 'Islamophobia', or 'East-West status conflict': *Detention of Eston Kohver (11), Russian espionage in Sweden (27), Religious extremism in the Netherlands (28)*
- If a hostile measure is repeatedly used against a state, governments should consider if it is productive to defensively counter and respond to every single incident. It might be more constructive to develop long-term strategies on a different level altogether, and take proactive approaches that promote a government's own narrative: *Humanitarian aid in the Russo-Georgian Conflict (9)*

## 8. Understand the information environment

The ultimate purpose of any hybrid threat is to affect the political decision-making of the target nation by influencing key target audiences. Adversarial activity may be undertaken to make a political statement, alter perceptions and attitudes of the general public, degrade levels of trust and confidence in government, or create confusion and a sense of insecurity. This is why consistent, coherent and factual government communications tailored to different key audiences is crucial to maintain trust and cohesion.

**High-visibility measures.** Some hostile measures are specifically designed to be high profile and generate maximum impact. Such threats might be intended to influence decision-making or public opinion on a specific issue, undermine trust in government by creating uncertainty and confusion, or to provoke a particular response. Government strategic communications should demonstrate – through both words and actions – that it has control over the situation; authorities must also have mechanisms in place to ensure that factual information is distributed to the population to mitigate the spread of rumours and disinformation.

- Disruptive events, such as cyber attacks or electronic warfare activities which target civilian systems, are often not intended to cause severe damage – which is part of the strategy of staying below the threshold of any kind of serious reprisal. Rather, these activities might be aimed at sending a political message, achieving certain psychological effects, or making a statement of capability: *2007 cyber attacks on Estonia (3)*, *Electronic warfare during Zapad 2017 (26)*, *Cyber attacks on ROK & US (29)*

**Reputation and legitimacy.** Public debates on the ethics of ‘right’ and ‘wrong’ are often heavily emotional, which an adversary can exploit by strategically framing a political issue in legal terms. Legal arguments can serve both as a source of legitimacy and as a tool to delegitimise an adversary. For instance, in cases of unclear attribution, an adversary might insist on the principle of ‘innocent until proven guilty’. Similarly, an adversary might seek to repudiate accusations of meddling in the internal affairs of other countries by employing ‘whataboutism’ and calling out hypocritical behaviour. One way of preventing these lines of argument from having damaging effects on a government’s legitimacy and reputation, is to display the importance of legal advisors in decision-making by referencing their counsel in public statements.

- Images and emotions are extremely effective means to influence public opinion and frame the narrative. First impressions – even when not accurate – usually frame the narrative, which can allow an adversary to achieve a public relations victory based on a semblance of legitimacy: *Hamas’ use of human shields in Gaza (7)*, *Humanitarian aid in the Russo-Georgian Conflict (9)*

**Measured response.** In responding to hostile measures, governments need to find a way of taking a public stance vis-à-vis the source nation, while not reinforcing the adversary’s desired information effect. A public response should not only be aimed at the adversary but should be tailored to the adversary’s target audience. Government messaging should not just discuss issues that worry the authorities but should address the concerns of the population.

- Media reporting on suspected espionage activities can quickly cause alarm and public concern, which is complicated by the fact that governments face severe constraints when releasing information on intelligence-related matters. Nations should be careful to avoid cultivating paranoia and make a distinction between general threat assessments and responses to single events: *Russian espionage in Sweden (27)*
- Governments often face the challenge of communicating and acting in a way that addresses a threat without reinforcing in-group vs. out-group perceptions: *Religious extremism in the Netherlands (28)*

## 9. Learn to operate in shades of grey

Hybrid threats can be complex, adaptive and inflict damage on national security before they are detected. Ambiguity surrounding intent and attribution impairs decision-making and complicates effective responses. Compelling and credible evidence may not be publicly available, and so the role of government communication becomes particularly important. Official statements should be specific and coherent, capture the nuances of the situation and give enough factual, credible information to inspire public confidence in the government. Governments should not spend too much time on trying to decipher deliberately ambiguous messages and actions, but instead frame events in a manner favourable to their aims.

Ambiguity can hinder effective responses. Ambiguity surrounding hybrid threats – the difficulty in identifying intent and attributing responsibility – can considerably slow down decision-making. It can also limit the response measures available to any affected government if public support is needed. Authorities may also not be able to release all of the information they have, which inevitably leaves room for doubt and alternative narratives that contest the government's position.

- Attributing a hybrid threat to a state actor can pose significant challenges and it may take time to establish compelling and credible evidence. State involvement is rarely black-and-white; the spectrum can range from state-tolerated to state-encouraged, state-orchestrated, or state-executed activity.<sup>10</sup> For example regarding cyber attacks or civil unrest, the degree of state responsibility can be extremely difficult to assess: *2007 cyber attacks on Estonia (3)*, *The 2010 Senkaku crisis (8)*, *Civil disorder in Bahrain 2011 (22)*, *Cyber attacks on ROK & US (29)*
- Connecting actors and groups to hostile foreign governments can be challenging, especially when financial or political links are not substantial, but interests and goals clearly align: *The spread of Salafism in Egypt (5)*, *Institute of Democracy and Cooperation (15)*, *Communist Party of Bohemia and Moravia (18)*
- Assessing hostility can be as difficult as determining attribution. For instance, snap exercises, which could be interpreted as threatening by neighbouring countries, provide a high degree of plausible deniability: *Russian snap exercises in the High North (1)*, *Snap exercises and Crimea (25)*, *Electronic warfare during Zapad (26)*

**Attribution impacts the perception of hostility.** An activity might not in itself be perceived as hostile or harmful, and only be seen as threatening when it is carried out by a certain actor. Foreign funding of an NGO by a friendly democratic state actor will inevitably be treated differently than foreign funding by an autocratic state actor that has been hostile on past occasions. In the absence of credible and compelling evidence, assessments of hostility and attribution ultimately become a political endeavour.

- Strategic context, history, bilateral relations, and common values with the source nation all impact whether an activity is interpreted as hostile: *The spread of Salafism in Egypt (5)*, *Humanitarian aid in the Russo-Georgian Conflict (9)*, *Casas del ALBA in Peru (30)*

**Counter the threat on your own terms.** When adversaries intentionally only give vague or contradictory information in order to confuse and slow down responses, governments can lose valuable time trying to disentangle and interpret the situation. Governments should not let the adversary dictate the rules of the game, but instead counter the threat on their own terms.

- Constantly being in the defensive, demanding clarity from the state actor in question, and scrambling to piece together different bits of information will let the adversary set the agenda. It will also let the adversary seem more powerful and calculating than they actually might be. Instead, governments should present closed ranks and unity of purpose, and stress resilience and international support: *The 2010 Senkaku crisis (8)*, *Bronze night riots (19)*

<sup>10</sup> Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, 22 February 2012.

## 10. Not every activity is a threat

Defining an activity as a threat and attributing it to a state actor is ultimately a political endeavour, and governments should be mindful not to inflate the threat level for political ends, either deliberately or inadvertently. As hybrid threats target a nation's weaknesses, it is a challenge to distinguish hostile influence from legitimate social grievances or failings of the government. Policy-makers should resist the temptation to blame external actors as a convenient way of shifting blame for domestic failings. Inflating or misattributing hybrid threats can affect the government's credibility in the long run and risks unnecessary escalation.

**Context affects meaning.** Historical context and coinciding events affect how words and actions are interpreted by audiences. An action which is perceived as routine or unremarkable at one moment, can be seen as hostile under different circumstances.

- A change in strategic context, such as the deterioration of relations between the Russian Federation and the West, fundamentally affects how events such as territorial violations and military exercises are interpreted: *Finnish airspace violations (12)*, *Electronic warfare during Zapad 2017 (26)*
- The level of analysis can also affect interpretation: an event can be seen as normal activity from a bilateral perspective, and only be interpreted as threatening when placed in a larger historical and strategic context: *Russian snap exercises in the High North (1)*

**Threat assessment.** Governments need to be able to identify why a particular activity is a threat. Regardless of actual hostile intent behind the activity, governments need to be able to assess if the activity in question has any harmful effect on national security interests, and measure this on a continuous basis.

- As the impact of foreign influence frequently depends on internal factors, governments must be careful not to overemphasise the role of foreign hostile activity. In cases relating to social grievances and civil unrest, too much focus on foreign influence might be perceived as an attempt to deflect from political failings: *Civil disorder in Bahrain 2011 (22)*
- Public diplomacy, i.e. the direct interaction of a government with foreign populations, is a fundamental element of international relations. Governments must therefore be able to articulate precisely how a certain kind of public diplomacy is detrimental to national security interests, and take appropriate measures that are consistent with democratic values and international norms: *Confucius Institutes (2)*, *Chinese public diplomacy in Taiwan (10)*

**Avoid unnecessary escalation.** While hybrid threats can sometimes be designed as precursors to the use of conventional military force, they are usually calculated as an asymmetric method of influencing another state without entering into a costly open conflict. A government's response should find a balance between countering hybrid threats and over-reacting in a way that could escalate the situation.

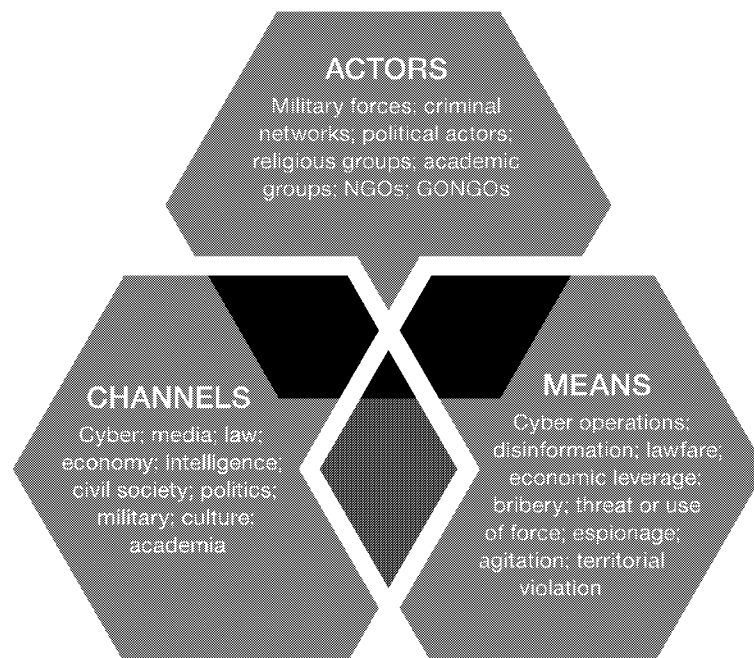
- Particularly when a threat exploits ethnic, cultural or religious divisions in a society, inadequate government responses might easily exacerbate these fractures: *Russkiy Mir Foundation in the Baltics (20)*, *Religious extremism in the Netherlands (28)*
- Factual and nuanced government communication is especially important to avoid threat inflation due to alarmism and a tendency to ascribe every negative occurrence to a hostile foreign actor: *Zambian elections 2006 (16)*, *Electronic warfare during Zapad 2017 (26)*, *Russian espionage in Sweden (27)*
- An apparently hostile activity might be aimed primarily at the perpetrator's domestic audience, for instance to distract from domestic problems, or to reinforce a certain narrative. Overreaction would then either only play into the hands of the source nation, or lead to an escalation that benefits neither party: *Finnish airspace violations (12)*

# Analysis of thematic areas

For the purpose of this project, sixteen thematic areas of threat were identified to group case studies together for analysis. The thematic areas are designed as a typology to help understand the wide range of means and ways that hybrid activity can manifest itself – military and non-military, conventional and unconventional, overt and covert, state and non-state. The thematic areas often overlap, as hostile influence usually involves more than one thematic area.

Grouping the case studies into thematic areas also enables policy-makers and Strategic Communications practitioners to identify case studies relevant to their current problem set. Findings and recommendations from this research that are specific to a thematic area will be covered in this chapter, with an emphasis on the role of Strategic Communications in understanding and responding to hybrid threats.

The thematic areas cover actors, channels and means.<sup>11</sup> In terms of this research – which has limited itself to looking at hybrid threats originating from states – an **actor** might be an institution, political organisation or religious group that is set up, supported, sponsored or somehow inspired by a state. A **channel** is the system or environment that the actor uses – for example, media, cyber, or law – which prescribes certain conditions, principles, and rules of behaviour; every channel has its own dynamics, particularities, strengths and vulnerabilities. The **means** describe the specific measures employed by an actor through a specific channel: this could for instance be disinformation, cyber-attacks or lawfare. Although this might seem like a linear process – an actor employing a channel by using a specific means – it is not always this clear-cut. For example, an actor such as a religious organisation might function as a channel to reach certain audiences in another country.



ACTORS, CHANNELS AND MEANS OF HYBRID THREATS (SOURCE: OWN ELABORATION).

<sup>11</sup> This decomposition into actors, channels and means is based on the diagram of hybrid influencing elaborated by the Hybrid CoE, cf. Atte Harjanne, Eetu Muilu, Jekaterina Pääkkönen and Hanna Smith, "Helsinki in the Era of Hybrid Threats – Hybrid Influencing and the City," (Helsinki 2018: Hybrid CoE), 6.

## THEMATIC AREAS OF THREAT

<p><b>Territorial violation</b></p>	<p><b>Non-Government Organisations (NGOs)</b></p>	<p><b>Government Organised Non-Government Organisations (GONGOs)</b></p>	<p><b>Espionage and infiltration</b></p>
<p>Violation of the internationally enshrined legal principle of territorial integrity which extends across the terrains of land, sea and air. Any such violation is considered an act of aggression by the target nation if carried out without previous consent or knowledge of the target nation.</p>	<p>A not-for-profit organisation that is officially independent from national and international governmental organisations, but is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>A non-governmental organisation which is openly funded, organised and/or directed by a government and may be acting against the national security interests of another nation.</p>	<p>Infiltrating organisations or institutions in order to gain intelligence. Infiltrating organisations or institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to the source nation.</p>
<p><b>Exploitation of ethnic or cultural identities</b></p>	<p><b>Media</b></p>	<p><b>Lawfare</b></p>	<p><b>Agitation and civil unrest</b></p>
<p>Exacerbating existing societal divisions in order to influence identity groups to act in the interests of a hostile state actor against the interests of the target nation.</p>	<p>The deliberate use of media either directly or via an intermediate actor in order to influence audiences and achieve attitudinal or behavioural change which is beneficial to an adversary.</p>	<p>Lawfare describes the hostile use of the legal system against an actor by damaging or delegitimising them, tying up their time, or winning a public relations victory. Lawfare is broadly understood as any exploitation of real, perceived or even manipulated instances of international law violations in order to undermine the target nation.<sup>29</sup></p>	<p>Encouragement of the citizens of a target nation to incite or participate in mass demonstrations and protests with the aim of undermining the government.</p>
<p><b>Cyber operations</b></p>	<p><b>Religious groups</b></p>	<p><b>Academic groups</b></p>	<p><b>Coercion through threat or use of force</b></p>
<p>Organised activity that involves the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."<sup>30</sup> The cyber domain describes an "electronic information (data) processing domain comprising one or several information technology infrastructures."<sup>31</sup></p>	<p>An actor identified as being aligned with a religious institution, movement or group that promotes a religious doctrine or ideology. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>An actor identified as being aligned with an academic institution, think tank or educational interest group. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>The threat or use of force to compel the target nation to act in a particular way or restrict freedom of action.</p>
<p><b>Energy dependency</b></p>	<p><b>Political actors</b></p>	<p><b>Economic leverage</b></p>	<p><b>Bribery and corruption</b></p>
<p>Considered to be a threat when the dependency lies on a source which is considered to be hostile. The target nation is dependent upon a source to the extent that withdrawal would have an immediate and serious effect on the energy infrastructure of the target nation. The dependency can thus be used to economically weaken the target nation or coerce the target nation into acting against its own national interests.</p>	<p>Activity which involves a political figure, party or organisation which is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.</p>	<p>The use of economic measures to exert an influence which coerces the target country to act in a way which it otherwise would not. This can be acting to the detriment of the latter's national security or in violation of international law.</p>	<p>The receiving or offering of any undue reward by or to an actor within the target nation in order to influence their behaviour, in particular to induce them to act contrary to their professional obligations and against the national security interests of their own nation.</p>

<sup>12</sup> See: Charles J. Dunlap, Jr., "Lawfare Today: A Perspective," *Yale Journal of International Affairs* 3, no.1 (2008): 146; "Is Lawfare Worth Defining?" *Case Western Reserve Journal of International Law* 43, no.1 (11 September 2010).

<sup>13</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>14</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).



## Territorial violation.

**Violation of the internationally enshrined legal principle of territorial integrity which extends across the terrains of land, sea and air. Any such violation is considered an act of aggression by the target nation if carried out without previous consent or knowledge of the target nation.**

**Characteristics.** A territorial violation can be a violation of soil, airspace or territorial waters of a nation. It can range from a limited and temporary violation to a large-scale seizure of territory. While on a technical level, a territorial violation can be clearly identified and defined, there can nevertheless be significant ambiguity surrounding a violation, hampering any assessment on whether or not it was a deliberately hostile act. A territorial violation by a single aircraft, or by a private entity like a fishing trawler, gives the related state actor the ability to plausibly deny any hostile intent or involvement. Unresolved territorial disputes and insufficient border security open up additional opportunities for deliberately ambiguous activities. A territorial violation might be aimed at provoking a certain government response, influencing public debate, testing defences, or actually changing borders.

**Considerations.** In dealing with territorial violations, governments should ensure that the violation is not perceived as a sign of weakness and lack of control, but avoid any unnecessary escalation. Government communication should appreciate that the amount of detail provided, the speed of response and the terminology used to describe an incident can significantly alter how an incident is framed by media coverage and perceived by the wider public. For instance, by analysing a territorial violation on a purely safety-related and technical level rather than on a political level, a government might be able to de-escalate tensions. In determining underlying motivations and the degree of hostility, governments should consider the scale of the violation, the overarching strategic context, historical patterns of behaviour, and the response (or non-response) of the opposite government.

*Detention of Eston Kohver (11), Finnish airspace violations (12), Electronic Warfare during Zapad 2017 (26)*

## Non-governmental organisations (NGOs).

**A not-for-profit organisation that is officially independent from national and international governmental organisations, but is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** NGOs are independent and non-profit civil society organisations, which can be active in areas such as education, healthcare, development work, public policy, religion, environment, or culture. They can perform a variety of charitable or social functions, such as acting as an advocacy group, providing a forum of interaction and debate, or supplying social goods and services that the government is unable or unwilling to deliver. Despite their name, NGOs can receive direct or indirect funding and donations from governments, although funding usually comes from the public, private businesses and other organisations that support their cause. The social work of an NGO is not only a powerful source of legitimacy, but also provides the basis for continuous face-to-face interaction with the public, a vital condition for building trust and influencing public opinion.<sup>15</sup> An NGO can be perceived as threatening by a government if it is deemed to be working in support of a state actor to push an ideology which undermines the ruling authority, promoting antidemocratic values, or challenging national unity by increasing social divisions.

**Considerations.** A vibrant civil society and respect for freedom of speech and cultural exchange are fundamental for a well-functioning democratic society. The ambiguity surrounding links of NGOs to hostile state actors makes it difficult for governments to counter potentially harmful activities. Almost every NGO is reliant upon operational and/or financial support, and governments face the challenge of defining the threshold of hostile interference. Governments should be careful to interfere directly in an NGO's work, as this would likely harm the government's credibility and undermine the very democratic values it aims to protect. In cases where an NGO provides critical services in healthcare or education that the government has failed to deliver, governments should focus on addressing these vulnerabilities and improving their policy performance, rather than closing down NGOs. Before implementing any potential legal regulations of NGOs, such as enhancing financial transparency, governments should carefully consider the second and third order effects that their proposed action could have on the treatment of NGOs in other countries; for instance, countries such as China, India or Russia have recently implemented laws to monitor NGO work perceived to be an instrument of hostile interference.

*Institute of Democracy and Cooperation (15), Casas del ALBA in Peru (30)*

<sup>15</sup> Reza Hasmath, Timothy Hildebrandt, and Jennifer Hsu, "Conceptualizing Government-Organized Non-Governmental Organizations." Paper Presented at Association for Research on Nonprofit Organizations and Voluntary Action Annual Conference (Washington D.C., USA), 17-19 November 2016.

## **Government organised non-governmental organisations (GONGOs).**

**A non-governmental organisation which is openly funded, organised and/or directed by a government and may be acting against the national security interests of another nation.**

**Characteristics.** A GONGO can function as a tool of public diplomacy that enables a government to directly engage with foreign publics and decision-makers. GONGOs can further a government's interests abroad, for example by promoting language and culture, interacting with diasporic communities and expatriates, or promoting certain humanitarian, economic, or political goals. A GONGO's director and management board are often directly selected or approved by the government. Although a GONGO is initiated, directed and/or funded by a government, its institutional set-up mirrors an NGO, meaning that it can often circumvent certain laws of transparency and accountability.<sup>16</sup> Although a GONGO is clearly connected to a state actor, its set-up can provide a degree of plausible deniability for the government, which can take credit for well-received GONGO activities, but still keep the organisation at arm's length when its work faces criticism.<sup>17</sup> A government can perceive a foreign GONGO as problematic, for example if this GONGO promotes antidemocratic thoughts and values, undermines the ruling authority, or discourages the integration process of minority groups with historical or cultural ties to the opposite government.

**Considerations.** Not all public diplomacy is hostile. GONGOs are an essential part of the relationship between states; they promote intercultural dialogue and enrich the civil society landscape at home. GONGOs are officially connected to a foreign state actor, which has an impact on how their activities are perceived by the wider public – they do not have the same amount of authenticity and credibility that organic civil society organisations and independent NGOs have. Governments face the challenge of assessing if a GONGO is damaging the democratic legal order by influencing public opinion or government in a way that undermines the ruling authority. In dealing with GONGOs, transparency and monitoring processes are vital: governments should scrutinise their funding channels, institutional set-up and mandate to assess whether a GONGO is propagating political ideas at odds with democratic values or engaging in other subversive activities.

*Confucius Institutes (2), Russkiy Mir Foundation in the Baltics (20)*

## **Espionage and infiltration.**

**Infiltrating organisations or institutions in order to gain intelligence. Infiltrating organisations or institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to the source nation.**

**Characteristics.** Espionage and infiltration are clandestine acts that usually aim to collect valuable information about the target nation, or infiltrating institutions which are considered to be legitimate and exploiting this legitimacy to promote a narrative favourable to a hostile state actor. Intelligence work relies on covert actions, and its exposure often has significant consequences for the degree of trust between states as well as between governments and publics. Adversaries can also try to expose intelligence work of the target nations or their partners, such as surveillance operations on citizens and organisations, to decrease public trust in government and intelligence services.

**Considerations.** In dealing with intelligence work, governments face the challenge of balancing the need for transparency with operational security. It is often not possible to report on sensitive information without compromising operational security and disclosing methods of intelligence collection. Governments should therefore work on building public trust in intelligence services. This includes admitting and openly discussing intelligence failures and providing as much information as possible. Speculation beyond the known facts should be avoided as this can affect government credibility, and provoke sensational media reporting, thereby risking unnecessary threat inflation. Moreover, a distinction needs to be made between overall threat warnings and evidence that supports attribution on a case by case basis.

*Detention of Eston Kohver (11), Russian espionage in Sweden (27)*

<sup>16</sup> Stephen W. Kleinschmit and Vickie Edwards, "Examining the Ethics of Government-Organized Nongovernmental Organizations (GONGOs)," *Public Integrity* 19, 2017: 529-46.

<sup>17</sup> Reza Hasmath, Timothy Hildebrandt, and Jennifer Hsu, "Conceptualizing Government-Organized Non-Governmental Organizations," Paper Presented at Association for Research on Nonprofit Organizations and Voluntary Action Annual Conference (Washington D.C., USA), 17 – 19 November 2016.

## **Exploitation of ethnic or cultural identities.**

**Exacerbating existing societal divisions in order to influence identity groups to act in the interests of a hostile state actor against the interests of the target nation.**

**Characteristics.** Hostile foreign actors can target pre-existing divisions in the population of another state. These divisions might be differences in religion, culture, ethnicity, or language. Methods can range from disseminating divisive narratives (either directly, e.g. through public statements, or indirectly, e.g. through media channels, institutions or proxy organisations), to giving material, ideological or organisational support to extremist groups or even separatist movements in another country.

**Considerations.** A key challenge for governments facing foreign exploitation of ethnic or cultural identities is that the core problem – that of social divides or minority grievances – is primarily an internal one. Hostile foreign influence will simply aggravate these problems by targeting vulnerable audiences and framing divisions in a way that is harmful to national unity. A government needs to be very precise in its communications when calling out hostile influence regarding social divisions, as excessive attention to foreign influence might be seen as an attempt to dismiss or discredit legitimate grievances of an ethnic or cultural group. Inconsiderate messaging can also reinforce in-group/out-group perceptions. The messenger used, and the frame selected, can have a considerable effect on how the message is perceived by different audiences. Countries that feature social groups with historical, ethnic or cultural ties to potentially hostile state actors should avoid the unnecessary politicisation of contentious issues, either by accident or for political gain. Instead, they should focus on common values, shared historical experience and an inclusive vision of the future. This will increase the overall sense of national belonging and frustrate malign efforts to hamper integration or promote separatist ideals.

*Chinese public diplomacy in Taiwan (10), Russian language referendum in Latvia (14), Bronze night riots (19)*

## **Media.**

**The deliberate use of media either directly or via an intermediate actor in order to influence audiences and achieve attitudinal or behavioural change which is beneficial to an adversary.**

**Characteristics.** Media is a key channel through which the public is provided with an account of world events, and the means by which most people develop an understanding of an official position. It functions as an array of different institutions, often independent from government, that scrutinise official government positions. Today, traditional media, such as print and television, are increasingly supplanted by new forms of social media, including platforms like Twitter and Facebook, and direct messaging applications, such as WhatsApp. In this networked media environment, journalists have lost their former position as gatekeepers necessary to transmitting political messages to the public. Instead, politicians are now able to directly engage with publics. Adding to this, connectivity allows for instant messaging with a high degree of reach and audience engagement. This has consequences for public diplomacy practices. It facilitates the direct engagement with foreign publics, increases reach and impact and makes it difficult to identify the origin of a message and attribute responsibility. Adversaries can manipulate the media environment through different tactics, such as disinformation, agenda-setting, or information laundering, with the aim to polarise a discussion or confuse the audience. They can also try to buy or set up media outlets to exert influence on a foreign media landscape.

**Considerations.** In a globally-connected networked media environment, government responses are significantly restricted by their bureaucratic systems and democratic decision-making rules and processes which hamper their ability to issue timely, consistent and coherent messages. Statements by regional officials and even by low-ranking soldiers on the ground can be influential or be exploited by hostile actors to legitimise a specific point of view. Governments should consider training officials to refrain from making statements which undermine the overarching narrative, and to be mindful of the impact their individual actions and statements might have. While accepting that from time to time mistakes will be made, improving an awareness of risks in the information environment and developing media skills down to the lowest levels of governments will help officials make statements that are not open to misinterpretation.

*Disinformation in Sweden (6), The 2010 Senkaku crisis (8), Civil disorder in Bahrain 2011 (22)*

## Lawfare.

**Lawfare describes the hostile use of the legal system against an actor by damaging or delegitimising them, tying up their time, or winning a public relations victory. Lawfare is broadly understood as any exploitation of real, perceived or even manipulated instances of international law violations in order to undermine the target nation.<sup>18</sup>**

**Characteristics.** Legal arguments are strongly intertwined with notions of legitimacy and ethics. Adversaries can strategically use these characteristics to legitimise their actions or delegitimise their opponents by framing an action in legal and ethical terms as just or unjust behaviour that requires or impedes a certain course of action, such as an intervention. At the same time, legal conformity does not necessarily lead to the perception of an action as legitimate or just. Media coverage, particularly images or video footage, that portray shocking or compelling scenes such as human suffering, starvation or police violence, often have a strong emotional resonance and can either support or undermine legal arguments. Adding to this, hostile actors can use legal arguments to confuse foreign audiences or simply tie up their time by initiating lengthy legal disputes and processes.

**Considerations.** The legality of an action is often not straightforward, but dependent on a certain interpretation of the applicability of a legal rule to a certain situation. Moreover, legal arguments are often accompanied by emotional messages that can support or undermine claims of legality. Governments should appreciate the functioning of the legal system in defining appropriate behaviour and act in accordance with legal norms, as non-compliance with international law will inevitably undermine their credibility. In dealing with the misuse of legal arguments by adversaries, governments should recognise the ambiguity of law and develop the ability to anticipate different interpretations and possible challenges to their own position. Governments should therefore conceptualise law as a domain to counter the use of legal instruments when employed in a hostile manner. It is important to employ legal advisors and communication experts to address lawfare issues and use their guidance to underpin a line of argument when addressing the public.

*Hamas' use of human shields in Gaza (7), Humanitarian aid in the Russo-Georgian Conflict (9)*

## Agitation and civil unrest.

**Encouragement of the citizens of a target nation to incite or participate in mass demonstrations and protests with the aim of undermining the government.**

**Characteristics.** Civil unrest, in the form of mass protests, strikes or riots, can be caused by political, economic or social grievances. Foreign agitators can incite or aggravate civil unrest in a number of ways, in order to undermine the government. For example, they can use proxies and surrogates, infiltrate disaffected groups, give material or organisational support to allied organisations, or encourage protesters by making public statements that serve to legitimise their cause. They can also use social media to agitate groups and induce protesters into violent behaviour, which is particularly difficult to trace back to foreign governments. Often, the goal of fostering civil unrest is to provoke the government into overreacting and responding in a heavy-handed way, to create a narrative of government repression.<sup>19</sup>

**Considerations.** While peaceful protests are a fundamental part of a healthy democracy, they can affect public order and safety if they escalate and turn violent. Foreign instigators can exploit the concerns and grievances of citizens, especially of vulnerable groups or minorities, and encourage them to channel these in a violent rather than political manner. Governments suspecting a foreign government of having incited or escalated civil unrest should beware of scapegoating a foreign government, while not taking legitimate grievances seriously. Governments should promote political inclusion, and show they are responsive to domestic criticism and address vulnerabilities, such as economic inequality. They should provide channels and means for disaffected groups to voice their concerns in legitimate and constructive ways. Governments should also consider training their security forces to be aware of the information effect of their actions, especially of the effect that images and videos of inordinate use of force can have when distributed quickly over social media.

*Bronze night riots (19), Civil disorder in Bahrain (22)*

<sup>18</sup> See: Charles J. Dunlap, Jr., "Lawfare Today: A Perspective," *Yale Journal of International Affairs* 3, no.1 (2008): 146; "Is Lawfare Worth Defining?" *Case Western Reserve Journal of International Law* 43, no.1 (11 September 2010).

<sup>19</sup> John A. Wickham, Jr., and Mildred E. Hedberg, "Field Manual No. 19-15: Civil Disturbances," *US Armed Forces*, 25 November 1985.

## Cyber operations.

**Organised activity that involves the “employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.”<sup>20</sup> The cyber domain describes an “electronic information (data) processing domain comprising one or several information technology infrastructures.”<sup>21</sup>**

**Characteristics.** As public and private physical infrastructure become more networked and reliant on information technology, they become increasingly vulnerable to cyber attacks. Adversaries can employ cyber operations to target critical infrastructures, such as banking or healthcare systems. Such disruptive attacks are often designed to be overt and aimed at high public visibility, for which they do not need to be particularly sophisticated – such as denial-of-service attacks, computer viruses or website defacements. Covert cyber operations aimed at espionage, by contrast, often remain undetected for a long time.

**Considerations.** The difficulty of attributing a cyber attack hampers a government’s ability to respond in an effective and timely manner. In dealing with the increasing threat of cyber operations, governments should both prepare effective communication strategies for immediate crisis response, as well as enhance their capabilities and methods to investigate and communicate attribution findings.<sup>22</sup> Communication strategies need to be included in civil contingency plans to calm the population and distribute essential information immediately to mitigate the spread of rumours and disinformation. Governments should increase cyber literacy amongst government officials, spokespeople and among the media, to ensure factual, coherent and credible communications.

*2007 cyber attacks on Estonia (3), Cyber attacks on ROK & US (29)*

## Religious groups.

**An actor identified as being aligned with a religious institution, movement or group that promotes a religious doctrine or ideology. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** Religion can be instrumentalised by a state actor in various ways. It might set up, direct and/or give financial or operational support directly to religious institutions, or to civil society groups, political actors, media outlets or other institutions that promote a particular religious ideology. A government might also subsidise or otherwise facilitate the education and training of clerics and religion teachers abroad, or provide foreign audiences with educational materials such as books on the religious ideology it is aiming to promote. Underlying motives of a government could be to further a transnational religious movement out of ideological conviction, or to promote a certain world view that bolsters the government’s legitimacy at home and abroad.<sup>23</sup> A government might also use religious language as a channel to reach and influence certain foreign audiences for political purposes. Religious activity can become a security concern when it threatens the democratic legal order by promoting antidemocratic aims or means, such as the rejection of state authority.

**Considerations.** Freedom of religion constitutes one of the core principles of a pluralist democratic society. Governments face the challenge of balancing the right to freely practice religion with a potential risk to national security interests. A hostile state can use religious groups to undermine the ruling authority. Religious activity is usually built on a strong unifying narrative that promotes a distinct worldview, implicating certain values, beliefs and practices. Messages based on a sense of community and belonging facilitate emotional resonance and positive identification, which adversaries can exploit to exacerbate social differences. In dealing with a potential hybrid threat involving a religious actor, governments should ensure a careful message design that avoids reinforcing social cleavages. It is important that governments de-link religion from the specific threat to avoid the perception that an entire religious group is targeted; they should also try to trace funding flows or an alignment of interests between a religious group and a foreign government.

*The spread of Salafism in Egypt (5), Serbian Orthodox Church (17), Religious extremism in the Netherlands (28)*

<sup>20</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>21</sup> Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge UP, 2013).

<sup>22</sup> John S. Davis II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica, CA: RAND, 2017).

<sup>23</sup> Peter Mandaville and Shadi Hamid, *Islam as Statecraft: How Governments Use Religion in Foreign Policy* (Washington, D.C: Brookings, November 2018).

## Academic groups.

**An actor identified as being aligned with an academic institution, think tank or educational interest group. This includes the infiltration of existing groups or the creation of new groups which are funded by sources hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** State actors can aim to influence academic groups, such as university lecturers or think tanks, within the target nation to co-opt the brand of independent scientific or educational institutions. By setting up or supporting such groups, adversaries can try to influence audiences through the guise of objective and neutral centres of expertise. This provides their messages with a high degree of authority and makes it more likely that domestic publics or policy-makers accept their point of view based on perceived impartiality. Academic groups that are aligned to the source nation can also be used as a channel to exert influence on diaspora student communities that study at foreign universities.

**Considerations.** Independent academic research plays a crucial role in every democratic society by evaluating government policies and providing advice and expertise. International academic exchange is a source of success for high-ranking universities around the world. Many academics receive scholarships or funding from governments, which makes it difficult to assess the threshold of malign interference. It is a challenge to protect higher educational institutions against such influence while safeguarding their independent status and ensuring their role as free centres of advice and expertise. Democratic governments should encourage educational and cultural exchange, while protecting the integrity of their higher educational systems. In cases where an academic group has frequently engaged in promoting opinions at odds with fundamental democratic values, governments should seek dialogue with university leadership or unions. These should encourage that academic groups disclose any partnerships or sources of funding to guarantee transparency. This ensures that their research can be discussed against the background of any potential bias. While the decision of closing down academic institutions should lie with the respective universities, governments can raise awareness and warn against foreign academic groups becoming an integral part of domestic educational institutions, and ask universities to critically engage with their programmes and academic methods.

*Confucius Institutes (2), Institute of Democracy and Cooperation (15)*

## Coercion through threat or use of force.

**The threat or use of force to compel the target nation to act in a particular way or restrict freedom of action.**

**Characteristics.** Military force posture and presence, such as the build-up of troops at an international border, ordering large snap exercises, or the development of certain capabilities such as nuclear weapons, is usually planned with certain information effects in mind to send a message of intimidation, deterrence or reassurance. The threat of force can also be implicit in political statements and can have a significant impact on another country's domestic public debates and decisions related to security and defence.

**Considerations.** Governments face the ambiguity as to whether military measures are aggressive or defensive in nature, and so need the ability to synthesise traditional military intelligence with analysis of the information environment. Snap exercises provide adversary governments with a high degree of plausibility, and an excuse to circumvent the OSCE Vienna Convention's stipulations on transparency and troop numbers. When trying to understand the desired information effect, governments should take into account that timing and context can significantly influence how military activity is perceived. For instance, a snap exercise might be perceived as normal on a bilateral level but be part of a worrying trend on a wider strategic level. An airspace violation can be treated as a purely technical and safety-related matter in one year, and as a clear threat in another, depending on the state of bilateral relations at the time. Government communication – i.e. the frame, the wording, and level of urgency – has a considerable impact on how military posture or threatening comments are received by the wider public, and whether or how they impact security-related debates and decisions, such as NATO membership.

*Russian snap exercises in the High North (1), Operation Parakram (24), Snap exercises in Crimea (25)*

## Energy dependency.

**Considered to be a threat when the dependency lies on a source which is considered to be hostile. The target nation is dependent upon a source to the extent that withdrawal would have an immediate and serious effect on the energy infrastructure of the target nation. The dependency can thus be used to economically weaken the target nation or coerce the target nation into acting against its own national interests.**

**Characteristics.** Energy-related dependencies on another state can be dangerous if this induces or coerces the government into making decisions that negatively affect national security interests. A hostile actor can withdraw the supply of critical energy resources, such as oil or gas, with the aim of coercing the target nation into taking a desired course of action. Moreover, the awareness of a dependency or a credible threat by an adversary can already have an indirect influence on decision-making. Overreliance on a single energy source and a failure to ensure supply diversification can exacerbate energy dependency. Poor governance performance and state capture in energy policies hampers the development of a coherent strategy on energy security.<sup>24</sup> Furthermore, energy dependency is often not just a bilateral issue, as the decisions of single countries can affect the energy security of an entire region. What may not be considered as a threat to an individual state's national security can affect the resilience of broader global governance structures.

**Considerations.** Democratic governments must balance value, reliability, and security in the provision of its energy. Decision-makers should be attentive to the possible vulnerabilities of energy policies and monitor lobbying in this area to make sure that the protection of national security is taken into account when taking decisions on energy supply. Governments face the additional challenge that most critical energy infrastructure is in private hands, which makes it more difficult to regulate and protect energy infrastructure.<sup>25</sup> One way of addressing this issue is the establishment of Public-Private Partnerships (PPPs), which are "long-term contracts between a public agency or public sector authority and a private sector entity."<sup>26</sup> This is not always an easy endeavour, since business and national security interests often diverge, and both public and private entities are reluctant to share information and know-how. In these cases, effective communication can help raise public awareness, get stakeholders to agree on the nature of the problem, and generate sufficient political will-power to develop a joint approach to energy security that balances both business and security interests.

*South Stream Pipeline (13)*

## Political actors.

**Activity which involves a political figure, party or organisation which is suspected to be funded, organised or directed by a source hostile to the target nation or influenced by an ideology which undermines that of the target nation.**

**Characteristics.** Adversaries can support ideologically aligned political groups, such as parties, their youth organisations, or individual politicians to influence democratic processes and decision-making. Tactics can range from open support, such as through public statements or high-level visits, to covert actions, such as secret funding, infiltration or bribery.

**Considerations.** In the absence of a clear link between a political actor and an adversary, the line between legitimate democratic debate and subversive activity which damages the national interest may be unclear. It is often difficult to distinguish whether a political actor's alignment of interest or ideology with a hostile state actor is the result of foreign influencing such as funding, or simply stems from independent pragmatic calculations or convictions. Political actors suspected of working against the national interest are often best addressed by civil society and media organisations rather than the government, to avoid the impression of a biased, politically-motivated persecution of a particular party or politician. Governments should avoid directly attacking a political opponent and rather focus on strengthening the legal frameworks around elections to ensure a fair campaign and political debate.

*The spread of Salafism in Egypt (5), Zambian elections 2006 (16), Communist Party of Bohemia and Moravia (18)*

<sup>24</sup> "EU and NATO's Role in Tackling Energy Security," Policy Brief No. 47, *Center for the Study of Democracy*, February 2015.

<sup>25</sup> Tiziana Melchiorre, "Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security," *NATO Energy Security Centre of Excellence (Vilnius 2018)*, 5.

<sup>26</sup> *Ibid.*, 6.

## Economic leverage.

**The use of economic measures to exert an influence which coerces the target country to act in a way which it otherwise would not. This can be acting to the detriment of the latter's national security or in violation of international law.**

**Characteristics.** Economic dependencies on another state can become a threat if this induces or coerces the government into making decisions that negatively affect national security interests of the target nation. Economic leverage can be exerted on the target nation through economic sanctions, such as import and export embargoes or tariffs, or withdrawing the supply of critical goods, but also through incentives, such as trade preferences, development aid, or export of energy resources, high tech products or military equipment.<sup>27</sup> Economic sanctions can also be employed as a tool of 'signalling and deterrence' to communicate discord with the target nation's policies or issue a general statement of capability that is intended to grant credibility to future threats of coercive measures.<sup>28</sup>

**Considerations.** Governments face the challenge of balancing values, business interests and security concerns in their foreign relations. Adversaries that hold economic leverage over another state can affect a change in behaviour even without having to resort to explicit threats, as the sheer awareness of potential sanctions or other hostile measures can suffice to change government's decision-making. Hostile economic measures can often be implemented with a high degree of plausible deniability, as measures such as the imposition of tariffs can be framed as a purely economic decision detached from the political matter at hand. Governments should develop long-term strategies to assess economic and political dependencies, resist 'easy cash' and build strategic alliances with partner nations to reduce the risk of the exploitation of economic leverage by hostile actors.

*US Transit Center at Manas (4), The 2010 Senkaku crisis (8), Pakistani involvement in Yemen (23), Zambian elections 2006 (16)*

## Bribery and corruption.

**The receiving or offering of any undue reward by or to an actor within the target nation in order to influence their behaviour, in particular to induce them to act contrary to their professional obligations and against the national security interests of their own nation.**

**Characteristics.** Pervasive and systemic corruption in a state poses a significant vulnerability to hostile foreign influence. An adversary might attempt to destabilise or weaken another country by systematically promoting corrupt behaviour and criminal networks, thus making the country harder to govern and decreasing trust in the government. Corruption can also function as an enabling factor for other hostile measures: a kleptocratic government is more likely to make decisions that undermine the country's national security interests for the personal gain of a few politicians, for example on matters related to energy security.

**Considerations.** Corruption is first and foremost a domestic problem, which is often merely exploited by foreign actors. As corruption is fundamentally intertwined with a lack of transparency and poor governance, it can be difficult to trace these types of hostile foreign influence. The fact that the very institutions designed to counter these types of hostile foreign influence – including security forces, the judiciary and elected politicians – may themselves benefit from the corrupt system or otherwise be under the influence of criminal networks, hinders the effective countering of such threats. Systemic corruption decreases public trust in democratic institutions in the long run, as it causes frustration with the lack of accountability and transparency, and disillusionment with political processes. A key issue for a government is to muster enough political will to fight corruption in earnest, and tackle this domestic vulnerability to foreign influence. Governments also need to credibly display this political resolve to the public, for example by using show cases of high-level punitive action for their information effect, to regain credibility and trust among the population. This should be accompanied by sincere efforts to increase transparency and create a robust legal framework. Government should also consider allocating higher salaries to judges and conducting amnesty programmes for lower-level corrupt business-people.

*Criminal networks in the Donbas (21)*

<sup>27</sup> Richard N. Cooper, "Is 'Economic Power' a Useful and Operational Concept?," *Weatherhead Center for International Affairs*, Working paper series no. 04-02, 2004, 7.

<sup>28</sup> Chen-Yuan Tung, "Cross-Strait Economic Relations: China's Leverage and Taiwan's Vulnerability," *Issues & Studies* 39, no. 3, (September 2003): 137-175, 136-7.



# CASE STUDY SUMMARIES

This section contains summaries of 30 case studies analysed using a standardised framework. Cases were selected because they were assessed as featuring behaviour which could be considered as having the characteristics of hybrid threats.

# RUSSIAN SNAP EXERCISES IN THE HIGH NORTH

## SUMMARY

On 16 March 2015 the Russian Federation began a *combat readiness test* ('snap exercise') of its Northern Fleet and force elements located in its Western Military District. The scale of the exercise was much larger than originally announced, and coincided with the Norwegian exercise Joint Viking in Finnmark (the northernmost part of Norway) and the US exercise Drogone Ride. Since both of these exercises were announced well ahead of time, it is reasonable to assume that the Russian snap exercise was timed as a defensive move or as a response to these exercises.

There remains considerable debate as to whether the readiness exercise violated the Vienna Document, a confidence and security-building measure agreed upon with the OSCE. Norway stated at the time that it was monitoring the situation, and did not submit a complaint to the OSCE. However, the consistent use of such snap exercises to circumvent requirements for notification runs counter to the spirit of the agreement and undermines its provisions.

Readiness tests are often assessed as being a threat to national security, since they have precluded a number of past conflicts, most notably in Ukraine.<sup>1</sup> In this case it is assessed that the exercises did not pose a threat to Norwegian security interests, but rather they were part of conventional geopolitics in the High North. While there seems to be a discrepancy between Norway and NATO's position on the exercises, this ostensible discrepancy is itself part of the conventional balance of power in the region.

## KEY POINTS

- The case study highlights the importance of strategic context: whether one considers the exercises in the context of NATO activities and the conflict in Ukraine or just as a bilateral issue has an impact on how different audiences understand events.
- From Norway's perspective, a high level of military activity, including the conduct of such exercises in the High North, was considered to be routine. Norway treated this series of events as part of accepted normality and did not identify the combat readiness tests as an exceptional or significant threat.
- NATO, by contrast, regarded the increase in Russian snap exercises as a breach of the spirit of the Vienna Document. This highlights the need to consider the differences between NATO narratives and national strategic interests, which in turn reinforces the importance of messaging which is coherent and mutually supportive at the international level.
- An effect does not necessarily have to be a change in behaviour, but could also be the maintenance of the status quo, i.e. considering a high level of military activity to be 'normal'.

## CONTEXT

■ **The High North.** The 'High North' is of significant geostrategic value to Russia; home to the Northern Fleets' strategic nuclear submarines and supporting base infrastructure. Beyond its immediate geostrategic importance, the High North is rich in mineral, energy, and marine living resources. In any conflict, it would be expected that Russia would defend this region by deploying forces into northern parts of Norway, the Barents Sea, and the Norwegian Sea.

■ **Increase in exercises.** Russian snap exercises, also referred to as readiness exercises, have increased in number since 2013, as part of Russia's military reform and modernisation plans, as well as the turn to (and reintroduction of) power politics and great power competition. Russia has previously used such exercises as a deception tool prior to the use of offensive military operations.<sup>2</sup>

■ **Cooperation.** The Vienna Document<sup>3</sup> is a Confidence and Security-Building Measure (CSBM) agreed upon with the OSCE in 1990, which requires participating states to notify each other ahead of time about major military activities such as exercises. According to a strict application of the text, exercises carried out without prior notifications to the troops involved are an exception to this rule.



Baltic Fleet repels simulated missile attack near Kaliningrad on 18 March 2015. IMAGE – Ministry of Defense of the Russian Federation.

## KEY ACTORS

Russian Ministry of Defence  
Norwegian Ministry of Defence  
Norwegian Parliamentary Foreign Relations and Defence Committee  
Norwegian Intelligence Service  
Norwegian Joint Headquarters

General Sergey Shoygu Russian Minister of Defence (since 2012)  
Alexey Meshkov Russian Deputy Foreign Minister (2012 – 2017)  
Colonel-General Vladimir Shamanov Commander Russian Airborne Troops (2009 – 2016)  
Ine Eriksen Søreide Norwegian Defence Minister (2013 – 2017)  
Jens Stoltenberg NATO Secretary General (since 2014)

# NARRATIVES

## Russian government

- New challenges demand exercises, particularly of Russian strategic formations in the north.
- The purpose of this exercise is to test the Northern Fleet's readiness and capability to protect Russian interests in the Arctic region.
- Russia is concerned about the number of NATO exercises, particularly in the north-eastern region of Europe, which increase tensions and destabilise the region.<sup>4</sup>

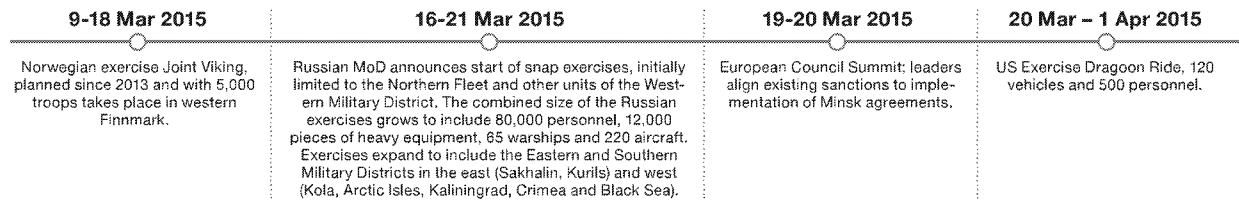
## Norwegian government

- All nations periodically conduct military exercises, including readiness exercises.
- This exercise, although large, was within the scope of what is considered normal, and thus not considered a threat.
- Norway will register any deviation from what is considered to be normal, although it does not seem as though Russia should have provided advance notification for this exercise.<sup>5</sup>

## NATO

- These Russian snap exercises run counter to the spirit of the Vienna Document, and are a serious concern (exercises are discussed in context with Russian aggression in Ukraine).<sup>6</sup>

# KEY EVENTS



# STRATEGIC LOGIC

It is reasonable to assume that Russia factors the timing of Norwegian and NATO exercises into their planning process ahead of snap exercises. Hence, this exercise in particular can be understood as a response to exercises Joint Viking and Dragoon Ride – all of which are part of the continual ‘dialogue’ of exercises between actors. In addition to the obvious and immediate benefits of improving military capability, this particular readiness exercise might have had other underlying strategic logics, such as also being a domestic show of force to boost national pride, a part of Russia’s strategic deterrence against what it sees as NATO aggression, or as a reminder to neighbouring states not to stray too far from Russian interests. Exercises can also be part of an effort to normalise military activity at this scale. At a time of discord between Russia and the West, the underlying core logic could arguably be to demonstrate Russia’s determination not to alter their course under Western pressure.

# MEASURES

- DIPLOMATIC.** Strategic deterrence of NATO; typical power politics (High North).
- INFORMATION.** Frequent updates about exercises after commencement; portrayal of exercise as a natural response to NATO behaviour.
- MILITARY.** Conducting a snap exercise to test readiness levels without prior notification and expanding the scope of the exercise. Conducting exercises for which the would-be adversary can only be NATO and/or the US.
- INTELLIGENCE.** None, but it is reasonable to assume that they were attentive to NATO nation responses during the exercises.
- LEGAL.** Taking advantage of the flexibility and room for interpretation in the terms of the OSCE’s Vienna Document.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- High North as Norway’s most important strategic area of responsibility.<sup>7</sup>
- Maintenance of the international rule of law, institutions, regulations and norms that regulate behaviour (e.g. Vienna Document).
- Predictability and consistency of relations with Russia, as well as further cooperation with Russia based on common interests.

## VULNERABILITIES

- Asymmetry of Russian-Norwegian relations in terms of military capability, which is why Norway aims to make the High North an area of multilateral cooperation.
- Unresolved border disputes in the High North, especially regarding the delimitation of littoral states’ Exclusive Economic Zones (EEZs) and the definition of extension of their continental shelves beyond the EEZs. Norway and Russia, however, reached an agreement on a maritime boundary in the Barents Sea in 2010.

## THREATS

- This snap exercise can be interpreted as a demonstration of Russia’s ability to achieve dominance in the Kola Peninsula and environs, particularly against the type of force concentration demonstrated in exercise Joint Viking.
- Exercises might be perceived as threatening, because Russia has previously used exercises to shape the operational environment for offensive operations against neighbouring states.
- Norway’s official position at the time was that the exercises posed no direct threat to Norway.

## EFFECTS

- This snap exercise did not force Norwegian authorities to deviate from ‘business as normal.’
- An effect does not necessarily have to be a *change* in behaviour, but also the maintenance of the status quo. Russian intent might simply have been to *normalise* these kinds of snap exercises in the High North.
- Discrepancy between Norwegian reactions (exercises do not pose a threat to national security) and NATO reactions (snap exercises as serious concern and at odds with the spirit of the OSCE Vienna Document), as NATO considers not only bilateral relations but overall regional trends.

# CONFUCIUS INSTITUTES

## SUMMARY

The Confucius Institutes (CIs) are non-profit educational institutions funded by the Chinese government, with the stated purpose of promoting Chinese language and culture. They were brought forward as a means to tell China's story to the world, but also to demonstrate to the domestic population how China is welcomed and respected globally. Since the launch of the Confucius Institutes programme in 2004, the large-scale initiative has been described as a Chinese 'soft power' success. The Confucius Institutes have secured a number of partnerships with universities in 146 countries around the world, including in NATO member states. In 2017, there were 525 Confucius Institutes at colleges and universities, as well as 1,113 Confucius classrooms at primary and secondary schools.

The CI initiative resembles other cultural institutes like the United Kingdom's British Council or the German Goethe Institut in the ways it provides language training and promotes culture (e.g. through cooking courses or calligraphy classes, and celebrating Chinese holidays). Unlike these other cultural associations, however, the CIs are set up as

a structural unit within a host university, and employ a system of double directorship.

However, the motives behind this large-scale initiative and the procedures of installation in host countries have attracted criticism, in particular the lack of transparency concerning the university contracts, hiring policies and financial aspects. Moreover, reports of self-censorship on sensitive political and historical topics (such as Tibet, Taiwan, or the Tiananmen Square protests of 1989) by both Chinese teachers and local university professors have raised concerns about intellectual freedom. Several scandals in 2014 involving instances of censorship cast light on the hard-line approach applied by the previous Director General, and the tight control exerted by the CI's governing body Hanban and the Chinese Ministry of Education. The controversy resulted in the non-renewal of CI contracts in several universities in the US and Europe and greatly contributed to the perception of CIs as an instrument of Chinese influence.

## KEY POINTS

- Institutions such as the CI should not be seen as inherently hostile – public diplomacy remains a key component of increasing understanding and cooperation between nations. Concurrently, attention should be paid to instances where national security interests might be affected – such as audiences being exposed to a world view at odds with democratic values. The Confucius Institutes should be viewed as acting in accordance with the official Chinese position and in line with larger Chinese strategies of soft power.

- The domestic goals of the Confucius Institutes are as important as the effects desired through the use of public diplomacy to influence foreign audiences. China's government is trying to spin the 'World Welcomes China' narrative in order to legitimise its rule through the image of acceptance and sympathy abroad.

- Such organisations must be treated solely as sources for language and cultural exchange; the lack of academic freedom precludes any claims to wider expertise. A stricter administrative and financial division within the host universities should be applied in order to ensure academic freedom. Sources of funding, as well as underlying political objectives, should be made transparent to the public, media and academia.



## CONTEXT

- **Worldwide presence.** The first Confucius Institute was established in 2004 in Seoul, South Korea,<sup>2</sup> although the first pilot project was launched earlier that year in Tashkent, Uzbekistan.<sup>3</sup> In the following 13 years, the number of CIs globally reached 525 Confucius Institutes at colleges and universities, as well as 1,113 Confucius classrooms at primary and secondary schools in 146 countries (2017). 173 of the Institutes are located in Europe and 110 in the United States of America.<sup>4</sup>

- **Calls for closure.** Both the Canadian Association of University Teachers and the American Association of University Professors (AAUP) called for the closure of all Confucius Institutes, with the AAUP stating in 2013 that the CIs "function as an arm of the Chinese state" and "advance a state agenda in the recruitment and control of academic staff, the choice of curriculum, and in the restriction of debate."<sup>5</sup> In a 187-page report analysing

the work of the CIs in the US, the National Association of Scholars also recommended an immediate closure of all Confucius Institutes in 2017.<sup>6</sup>

- **China and Soft Power.** 'Soft Power', as defined by American political scholar Joseph Nye in the late 1980s, "occurs when one country gets other countries to want what it wants [...] in contrast with the hard or command power of ordering others to do what it wants."<sup>7</sup> President Xi Jinping said in 2014 that "we should increase China's soft power, give a good Chinese narrative, and better communicate China's message to the world," although it is unclear whether they refer to Nye's concept of soft power or have their own definition. China's soft power tools include infrastructure and aid programmes, but also more traditional tools like educational exchanges and international media outlets, as well as the Confucius Institutes.<sup>8</sup>

## KEY ACTORS

**Confucius Institute Headquarters (Hanban)** a corporate body affiliated to the Chinese Ministry of Education

**Xu Lin** former Director General of Hanban, left in 2014 after censorship scandal

**Ma Jianfei** Secretary of the Party Committee of Hanban (Director General level); the Director General position has been empty since the censorship scandal)

# NARRATIVES

## Chinese government

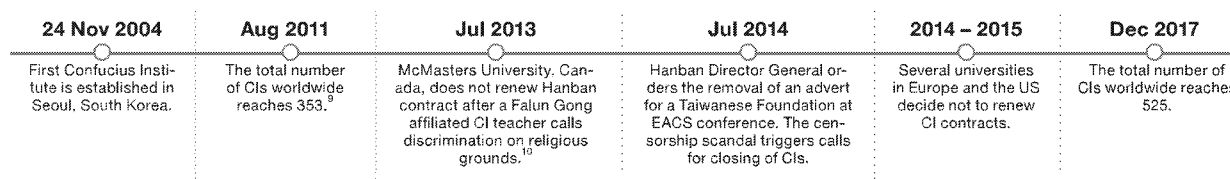
- 'The world welcomes China': Confucius Institutes are much welcomed across the globe.
- Host institutions are the primary initiators in setting up the CIs.
- The CI initiative is the biggest international legacy of President Hu's rule.

## Critics of the Confucius Institutes

From various Western NGOs, think tanks, government officials and academics:

- Suspicion of CIs, 'better-safe-than-sorry' approach.
- Academic institutions can become too dependent on Hanban money, which can lead to (self-)censorship on sensitive political issues, and thus limit freedom of expression.
- By decreasing the outreach of competing narratives (e.g. from Taiwan, Tibet), the CIs have the potential to influence public opinion in the long run.

# KEY EVENTS



# STRATEGIC LOGIC

In order to establish a Confucius Institute, Hanban requires the host institution to establish a partnership with an educational institution in China, making it appear more as a local initiative than an organisation established by an outside actor. Once the partner institution is approved by Hanban, both organisations appoint a director of the soon-to-be established Confucius Institute, thus abiding by the principle of double directorship stipulated by China. It is likely that the Chinese side initially viewed the cooperation

between the universities and the principle of double directorship as a means of reassuring the partners abroad.<sup>11</sup> Ironically, this policy resulted in almost instant suspicion from the Western partners. Drawing on the image of universities as the beacons of freedom of expression and academic thought, the partner institutions may risk becoming a point of entry for Chinese political agenda in the West.

# MEASURES

**DIPLOMATIC.** The work of CIs is intertwined with that of the diplomatic corps, especially the Cultural Affairs Office. Almost every event organised by CIs (festivals, concerts, language competitions) is attended by representatives from the Chinese Embassy at the Ambassador or Consul General level. The establishment of a CI requires an official application from the host institution: when the host institution is reluctant, the initiative of the establishment is unofficially expressed by the Chinese side, lobbying for the institution to apply for CI status. In more strategic cases, the Ministry makes use of diplomatic channels to convey the message that an application for establishment coming from a local entity would be highly appreciated.<sup>12</sup>

**INFORMATION.** Teaching and opportunity marketing (e.g. scholarships) contribute to the CI's successful informational impact. The space for China-related discussion is very narrow, as no meaningful exchange on China's interior or international problematic issues is allowed.

**FINANCIAL.** CIs typically receive a minimum of USD 100,000 in annual support for programming.<sup>13</sup> The CIs are obliged to report their annual projects and accounts to Hanban for approval. The CIs are jointly financed by the Chinese Ministry of Education and the host university. Most of the CIs are not self-sustainable.

**INTELLIGENCE.** Speculation over industrial espionage have been made in the US, and universities with cutting-edge technology were encouraged to exercise caution when cooperating with CIs. Hanban has strongly denied this.

**LEGAL.** The degree of integration of the Confucius Institutes into the everyday academic work of the universities is determined by contracts signed between the involved institutions. In some cases, the legal framework gives the Institutes influence over academic goal-setting, potentially endangering academic freedom.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Sovereignty of foreign policy and internal mechanisms making the foreign policy decisions.
- Integrity and consistency of internal public opinion of external actors (countries).
- Integrity and consistency of academic thinking related to research on China.

## VULNERABILITIES

- Academic institutions often face severe financial constraints. They will therefore often welcome the generous funding from Hanban to provide educational training they would otherwise not be able to offer.
- The policy of establishing a CI within an existing university and injecting the funds and the management into the host university make the university more vulnerable towards a Chinese political agenda.

## THREATS

- The boundaries of what CIs should and should not promote in terms of Chinese culture abroad are rigorously predetermined in operational guidelines, and are politically non-neutral. The agenda of Hanban, if not analysed critically, has the potential to influence the host country's public opinion on China's sensitive political issues.

- The asymmetry of resources invested by the CIs in the popularisation of China's official world view decreases the outreach of competing narratives (e.g. those of Taiwan).
- Potential self-censorship on the side of the host university (e.g. in 2013, Sydney University cancelled a lecture by the Dalai Lama, reportedly to avoid damaging its ties with China, including funding for its CI).<sup>14</sup>

## EFFECTS

- General aim of the popularisation of Chinese culture and especially Chinese language has been achieved, as CI courses reach hundreds of thousands of people worldwide.
- Increased visibility of China in host countries.
- Minimisation of the cultural impact of opposing organisations by monopolising the narrative on Chinese culture.
- Hanban is facing massive public relations challenges following suspicious attitudes towards CIs that have dominated both the Western media as well as academia since the 2014 scandals.

# 2007 CYBER ATTACKS ON ESTONIA

## SUMMARY

In April and May 2007, Estonia was the target of a coordinated cyber attack. Over a three-week period, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by a Distributed Denial of Service (DDoS). The cyber attack coincided with the Estonian government's decision to relocate the Soviet-era 'Bronze Soldier Memorial' in Tallinn, which led to significant civil disturbance in both Estonia and Russia.

Much of the malicious network traffic showed signs of political motivation and Russian-language origin. The Russian government denied any involvement, blaming 'patriotic' pro-Russian groups and individuals. However, the cyber attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and a refusal

to cooperate with the Estonian investigation in the aftermath of the attacks, which likely encouraged the perpetrators.

The attacks caused some disruption and economic cost to Estonia. Perhaps more importantly, though, they exposed Estonia's vulnerabilities, and demonstrated the *potential* of cyber attacks to cause far more lasting damage if intended. However, the incident also demonstrated Estonia's capabilities and resilience in countering the cyber attacks. Ultimately, the shock caused by the cyber attack led to a significant strengthening of cyber defence capabilities, institutions and legislation in Estonia, the European Union, and NATO.

## KEY POINTS

- Ambiguity was a key feature of this cyber attack. As the attacks were apparently carried out independently by individuals using their own resources, any state sponsor responsible for orchestrating the attack was able to disguise themselves and deny involvement. This underscores the requirement for governments to achieve political consensus on attribution in a timely manner based on the available evidence and be able to communicate this in a clear and understandable way to the general public.

- In addition to the physical effect on infrastructure, cyber attacks have a significant psychological dimension. In this case, attackers could have inflicted significantly more damage within the cyber domain if desired, but it was highly likely that a key objective was to test the responses of

the Estonian government and EU and NATO allies, as well as to damage the reputation of the Estonian government in the eyes of Estonia's Russian-speaking population and global public opinion. The cyber attacks almost certainly targeted the government's ability to provide effective and calming strategic communication to domestic and foreign audiences during the crisis.

- In this case, as well as in similar cyber attacks on Lithuania (June 2008), Georgia (July/August 2008), and Kyrgyzstan (January 2009),<sup>1</sup> cyber activity was integrated and synchronised with a wide spectrum of other measures, such as economic or diplomatic pressure, with the result of increasing strategic effects.

## CONTEXT

- **Distributed Denial of Service (DDoS).** DDoS attacks are one of the most common forms of cyber attacks. The attacker will spread malicious software to vulnerable computers, e.g. through infected emails and attachments, and so create a network of infected machines (called a botnet). The attacker can then command the botnet to bombard a certain website or online service with traffic, until the site crashes under the sheer load of requests.<sup>2</sup> DDoS attacks, by their nature, do not usually cause extensive or even irrecoverable damage, but can cause considerable disruption.

- **The Bronze Soldier Memorial.** The Bronze Soldier is a controversial Soviet-era war memorial built at the site of a number of war graves. For many Estonians, the memorial symbolises a time of occupation, deportation and grief. The government stated that moving the statue and the remains from the centre of Tallinn to a cemetery was more suitable and would help societal unity.

## KEY ACTORS

**Ministry of Defence of Estonia**  
**CERT-EE** Estonia's Computer Emergency Response Team  
**NATO**

**Toomas Hendrik Ilves** President of Estonia (2006 – 2016)  
**Urmat Paet** Minister of Foreign Affairs of Estonia (2005 – 2014)  
**Andrus Ansip** Prime Minister of Estonia (2005 – 2014)  
**Vladimir Putin** President of the Russian Federation (2000 – 2008, 2012 – present)  
**Sergei Ivanov** First Deputy Prime Minister of the Russian Federation (2007 – 2008)  
**Sergey Lavrov** Foreign Minister Russian Federation (since 2004)  
**Jaap de Hoop Scheffer** NATO Secretary General (2004 – 2009)

## NARRATIVES

### Estonian government

- The Bronze Soldier memorial is divisive due to different interpretations of history; its relocation to a cemetery will help national unity.
- The cyber attacks are a blatant attack not only on Estonia's sovereignty, but also on the entire EU and NATO.<sup>3</sup>
- The Russian government is at least indirectly responsible for these cyber attacks.<sup>4,5,6</sup>
- Estonia countered the attack very effectively.
- There is an urgent need to adapt and expand national and international law to address new threats such as cyber attacks.

### NATO

- Cyber attacks are a serious security issue.<sup>7</sup>
- NATO is providing technical assistance and political solidarity for Estonia.<sup>8</sup>

### Russian government

- The Estonian government's decision to move the Bronze Soldier memorial is disrespectful and sacrilegious, and will have serious consequences for bilateral relations.<sup>9,10</sup>
- Claims that the Russian government orchestrated the cyber attacks are false.<sup>11</sup> Independent 'patriotic' Russian groups and individuals were involved in the cyber attacks.

# KEY EVENTS

10 Jan 2007	26 – 27 Apr	27 Apr	28 Apr	4 May	9 May	19 May	Jan 2008
Government announces plan to relocate Bronze Soldier Memorial.	Excavation works begin around the Bronze Soldier Memorial. Peaceful protests soon turn into violent riots.	First wave of uncoordinated cyber attacks on high-profile websites begins (targeting major political websites and media outlets).	Coordinated fight-back effort of MoD together with CERT-EE begins, supported by other CERTs around Europe.	Second, more sophisticated and coordinated wave of cyber attacks, this time also targeting banks (esp. Hansabank and SEB Eesti Uhisbank). <sup>12</sup>	Attacks peak on Russian 'Victory Day.'	Cyber attacks abruptly and simultaneously cease.	Estonia indicts one of the responsible hackers.

## STRATEGIC LOGIC

The attacks appeared to be spontaneous and self-organised, with 'patriotic' non-state actors claiming involvement. If the attack was indeed orchestrated by a state actor, the difficulty of attributing responsibility for cyber attacks made it easy for a state actor to credibly deny involvement. However, the synchronisation of the cyber operations with other strategically ambiguous measures, hostile statements by Russian officials, and the

Russian government's lack of support for Estonia's efforts to resolve the attacks indicate that this was very likely a coordinated act of hostility, and that the cyber attacks – if not directed by the state – were at the very least not discouraged. It is reasonable to assume that there was a strong focus on how Estonia (and its partners) sought to manage a response to the attack.

## MEASURES

**DIPLOMATIC.** Public statements by President Putin and other officials harshly criticised Estonia's plans to relocate a Soviet-era war memorial. Protesters besieged Estonia's Embassy in Moscow for a number of days.

**INFORMATION.** By targeting media and many other websites, the cyber attack aimed to prevent Estonian citizens from obtaining information (i.e. news, updates from the government, bank balance) in the way they were accustomed. By interrupting, or making less reliable and instant, the access to information, the attack targeted Estonia's reputation as a digital-advanced state.

**MILITARY.** There were no accompanying military exercises, movement of forces, or provocative actions. Falling short of the threshold for invoking Article V was likely a strategic imperative.

**ECONOMIC.** Increased friction at the Russian-Estonian border included lengthening of border checks, the severing of rail links due to unscheduled 'repairs' and the cancellation of orders from Russian businesses. The Russian First Deputy Prime Minister called on Russians to boycott Estonian goods and services in response to the relocation of the monument.<sup>13</sup>

**FINANCIAL.** Targeting banks and other financial institutions indicated that attackers were aware of the vulnerability of e-services to DDoS disruption. The web-interfaces for internet-based services of the two biggest banks in Estonia were offline for up to 90 minutes, and foreign money transfers were temporarily unavailable.<sup>14</sup>

**INTELLIGENCE.** It is reasonable to assume that intelligence gathering on vulnerabilities and specific target identification occurred, as the attacks were disciplined in nature, and effects were restricted inasmuch as they did not cause existential or irrevocable damage. Given the likely involvement of organised criminal networks, the identification and clearance of these individuals, as well as monitoring and payment would have required reliable intelligence activity.

**LEGAL.** Ambiguity was a key characteristic of this attack. Although it was clearly illegal under national and international law, the aftermath of such an attack is almost impossible to prosecute given the difficulty of identifying responsible individuals living in Russia – even if such evidence were gathered, it would likely be inadmissible because of the way it was obtained, and would reveal intelligence collection capability.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

■ Actual and perceived political stability, good governance, and security. Public confidence in the government, military and security structures.

■ Liberal democratic systems such as Estonia depend upon the free flow of information.

■ Estonia was, and is, one of the world's most digitally connected societies,<sup>15</sup> and is critically dependent on the internet and related services.

■ It is critical to national security to minimise the vulnerability of information systems, and ensure the security of national databases and registries.<sup>16</sup>

■ Estonia's reputation as a business-friendly state, where inner- and inter-state movement of funds is safe and reliable, is an important resource for the country.

■ National unity, minimisation of friction between different societal groups, especially regarding the significant Russian-speaking community.

### VULNERABILITIES

■ Estonia's highly developed information infrastructure simultaneously made the country vulnerable to disruption from cyber attacks.

■ DDoS attacks, the predominant form of attack used here (although other attack types were employed as well), exploit the vulnerability of unprotected websites and web-enabled resources to succumb to the direction of massive amounts of internet traffic. Automated and reactive measures could have been put in place to prevent this vulnerability.

■ Around 330,000 of Estonia's 1.3 million inhabitants are ethnic Russians,<sup>17</sup> many more have Russian as their first language. The Russian Federation has a history of manipulating this community to strategic benefit by promoting instability.

### THREATS

■ Exploitation of identity politics, different understandings of history, a largely symbolic act to cause civic unrest.

■ Use of hijacked resources, and criminal networks with smart command and control. In the 2007 cyber attack, a combination of professional attackers and entry-level users of DDoS and other tools created a smokescreen.

■ Disrupted information flow, which threatened to have a psychological effect on citizens and the confidence of businesses and investors.

### EFFECTS

■ Although the direct effects of the cyber attacks were contained, the incident demonstrated the ability of hostile state actors to inflict asymmetric damage and disruption without needing to draw on conventional and escalatory forms of force. The attack was first and foremost an act of communication.

■ Polls showed that public confidence in the government actually increased after the Bronze Soldier riots,<sup>18</sup> although trust of Russian-speakers in the government decreased and social divisions increased.

■ Increased resilience, capability and capacity of Estonia (as well as other states and international organisations such as NATO). Increased international cooperation over cyber defence.

■ Implementation of a national cyber security strategy 2008-2013. Establishment of a 'Cyber Defense League' and the NATO Cooperative Cyber Defence Centre of Excellence (both initiatives had been planned before the attack, but gained new importance in the aftermath).<sup>19</sup>

# US TRANSIT CENTER AT MANAS

## SUMMARY

In 2001, the US established an air base<sup>1</sup> at Manas International Airport in Kyrgyzstan as an air mobility hub to support Operation Enduring Freedom – Afghanistan (OEF-A). This base was of strategic importance to the US and its allies, with responsibility for the aerial refuelling of coalition aircraft, airlift of supplies and equipment, movement of coalition personnel and building partnerships with the Kyrgyz population.<sup>2</sup> Although the facility was costly, it provided much safer and more reliable access to Afghanistan than the routes available through Pakistan.

Kyrgyzstan received significant remuneration for the lease, securing USD 318 million in direct investment,<sup>3</sup> as well as indirect financial and non-financial benefits. Russia, however, increasingly pressured Kyrgyzstan to close to the Transit Center at Manas (TCM), wary of a long-term US military presence in the region. Russian offers of financial and economic assistance were intertwined with verbal threats to restrict US-Kyrgyz relations, especially concerning economic cooperation.

Russia also attempted to shift Kyrgyz public opinion against the US facility, in particular through Russian media channels, which focused extensively on accidents related to the base and frequently fabricated or exaggerated negative aspects of the Transit Center.

Kyrgyzstan was thus caught in an apparent dilemma between US and Russian assistance. For over a decade, the Kyrgyz government balanced these opposing pressures with some success. Successive Kyrgyz Presidents used the increasing Russian pressure and growing anti-American public opinion in Kyrgyzstan as bargaining chips in their efforts to increase US payments. However, mostly as a result of rampant corruption prevalent in the national government, Kyrgyzstan failed to use this cash injection to minimise its economic vulnerabilities. Despite intense efforts by the US to keep the Transit Center open, including a wide range of outreach efforts towards the Kyrgyz population, a parliamentary vote in 2013 ended the lease with the US government and the facility was closed in 2014.

## KEY POINTS

- While the Russian Federation used primarily economic instruments as leverage, this was integrated with diplomatic and informational measures. Identifying and countering any potential threat requires the ability to assess adversarial activity across the full spectrum of military and non-military means.
- Economically vulnerable states should pursue long-term strategies that minimise their economic vulnerabilities or be prepared to accept risk concerning their national security interests. Earning “easy cash” without further positive implications can escalate into further economic and political dependence on external powers.
- It is likely that public opinion was a significant factor in the political decision to close the base. If a country is assessed to be vulnerable to outside influence, every effort should be made to identify and understand those key target audiences which hold the balance on domestic consent for government policy.



Photo by Staff Sgt. Travis Edwards, U.S. Air Force/Released

## CONTEXT

■ **Kyrgyzstan.** Like all former Soviet territories, Kyrgyzstan was subject to Soviet policies of collectivisation, Russification, and economic integration with the wider USSR. These policies left a legacy of Russian language and by extension, consumption of Russian-language mass media, as well as close political and economic links with Russia. Kyrgyzstan is one of the poorest countries in the region. The state has been heavily dependent on Russia, although Chinese economic influence has been growing in recent years.

■ **The Transit Center at Manas.** The Transit Center was located at the Manas International Airport, a civilian installation situated 20km north of the capital, Bishkek. The US base shared the airport's 4,200-metre runway. On average, 1,200 to 3,500 coalition troops passed through Manas every day, and between 6 and 13 million pounds of cargo passed through the base every single month.<sup>4</sup>

■ **Financial Aspects.** The Kyrgyz government negotiated with the US to increase payments from the agreed figure of USD 2 million to USD 17.4 million in 2006, rising to USD 60 million annually from 2009.<sup>5</sup> The airport also collected a fee of USD 7,000 for every take-off and landing, and all of the fuel was purchased locally. The US provided assistance to Kyrgyzstan, such as infrastructure improvements, economic development, and counter-terrorism initiatives.<sup>6</sup> Overall, the Transit Center at Manas contributed about USD 40 million per year to the Kyrgyz economy from its first year, and employed around 500 Kyrgyz nationals.<sup>7</sup>

■ **Corruption surrounding the TCM.** Most of the US payments were syphoned off by the regime, flowing to private companies with close links to the Kyrgyz government, and never reached the Kyrgyz population. Technically, these contracts did not violate any US laws or procedures,<sup>8</sup> but the lack of transparency in these financial transactions had a significant impact on domestic political discourse.

## KEY ACTORS

Russian Ministry of Foreign Affairs  
US Department of Defense  
US Department of State

Askar Akayev *President of Kyrgyzstan (1991 – 2005)*  
Kurmanbek Bakiyev *President of Kyrgyzstan (2005 – 2010)*  
Almazbek Atambayev *President of Kyrgyzstan (2011 – 2017)*  
Vladimir Putin *President of Russian Federation (2000-2008, 2012-present), Prime Minister (1999 – 2000, 2008 – 2012)*  
Dmitry Medvedev *President of Russian Federation (2008 – 2012), Prime Minister (since 2012)*



# NARRATIVES

## Kyrgyz government

- Kyrgyzstan receives substantive economic advantages from allowing the US to use the Manas facilities (since 2001).
- The US needs to provide more economic incentives if it wants to continue using the Manas facility (since 2006).
- Kyrgyzstan needs Russia politically and economically; therefore Russia's interests have to be respected (since 2011).
- There is no requirement for US troops to be at a civilian airport just outside the capital (since 2011).

## Russian government

- The base at Manas is destabilising regional security.
- Kyrgyzstan needs to choose between the US and Russia. Economic cooperation with Russia will far outperform closer cooperation with the US.
- The US has hidden and hostile intentions with the facility.

## US government

- The TCM is crucial for the US and its mission in Afghanistan.
- The TCM has no negative impact on Kyrgyzstan, but actually contributes to regional stability.
- Kyrgyzstan receives meaningful economic aid in exchange for allowing the use of the Manas facilities.

# KEY EVENTS



# STRATEGIC LOGIC

Russia used a number of measures to pressure Kyrgyzstan to close the US base at Manas. It employed both carrots and sticks – financial and economic assistance combined with hostile rhetoric – to further its interests,

especially concerning economic cooperation. Russia also attempted to influence Kyrgyz public opinion against the US base through Russian-language media.

# MEASURES

**DIPLOMATIC.** Kyrgyzstan announced significant decisions regarding the TCM preceding or following visits of Russian officials or during visits to Russia. Russian officials publicly criticised Kyrgyz decisions that contradicted Russian positions.

**INFORMATION.** Russian state and private media are widespread in Kyrgyzstan. The closure of the TCM was a popular topic amongst Russian-language media, much more so than in the Kyrgyz media.<sup>12</sup> Russian and Russian-language media often fabricated or exaggerated negative aspects of the US Manas facility, emphasising accidents, the negative impact on the environment, and focused on rumours surrounding fuel dumping, US espionage, and drug-trafficking from Afghanistan via Manas.<sup>13</sup> One incident, in particular, was widely reported by Russian media: in 2006, a local truck driver was fatally shot at an entry control point by a US serviceman, which caused outrage among the population. In 2009, there were also

reports of possible Russian cyber attacks against Kyrgyzstan,<sup>14</sup> but linkage to the TCM is not proven.

**MILITARY.** In 2003, Russia established its own air base (Kant) in Kyrgyzstan, likely as a symbolic counterbalance to the US base.

**ECONOMIC/FINANCIAL.** Economic and financial instruments were primary elements of Russian influence. Kyrgyz decisions relating to a possible closure of the TCM were preceded or succeeded by announcements of Russian assistance (in 2009, Russia agreed to provide a USD 2 billion credit and financial aid worth USD 150 million,<sup>15</sup> and in 2012 Russia agreed to write off Kyrgyzstan's debt of USD 489 million<sup>16</sup>). Russia also pressured Kyrgyzstan to join the Eurasian Economic Union (EEU), which would compensate for the loss of US financial aid and further integrate Kyrgyzstan into a Russian-centred economic space.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Consolidation of democracy and the values associated with it.
- Peace and security in the country and the surrounding region.
- Economic sovereignty, economic sustainability and development.
- Sovereignty of the information space.

## VULNERABILITIES

- Corruption of political elites, which also affected the money flows surrounding the TCM.
- Regional instability, terrorist activity in the wider region.
- Weak national economy, economic dependence on Russia (close links in trade, investment, ownership of assets, and workplaces for Kyrgyz expats).
- Poor journalistic standards; strong presence of Russian-language mass media in Kyrgyzstan, which might decrease the reach of alternative points of view.

## THREATS

- Risk of democratic backsliding.
- Closure of the Russian market to Kyrgyz companies and individuals; reduction or halting of economic and financial assistance from Russia; further dependence on Russia.
- Influencing of public opinion through misinformation (either deliberate or due to lack of journalistic standards).

## EFFECTS

- Democratic backsliding: Kyrgyzstan's participation in the War on Terror provided international legitimacy, and the international community noticeably muted human rights concerns.<sup>17</sup>
- Despite extensive outreach efforts to the local population by the Mission Support Group at Manas, Kyrgyz public opinion gradually tilted against the TCM over the years (likely resulting from dissatisfaction over corruption, negative reporting on the TCM, and the context of deteriorating US-Russian relations).
- Increased bargaining power of Kyrgyz government vis-à-vis the US due to pressure from Russia and domestic public.
- Cooling of US-Kyrgyz relations after the closure of the TCM; Kyrgyzstan has since re-approached Russia, which partly compensated Kyrgyzstan for the loss of US payments.

# THE SPREAD OF SALAFISM IN EGYPT

## SUMMARY

The Kingdom of Saudi Arabia (KSA) has supported Salafī charities, websites and media channels as well as the Salafī Nour Party in Egypt. This support has taken various forms, ranging from ideological guidance to material assistance. Money is believed to come mainly from members of the Saudi royal family, businesspeople, or religious leaders via Muslim charities, rather than through official state channels.<sup>1,2</sup> The KSA likely pursues two main goals in promoting a sympathetic religious ideology in its neighbouring country – firstly, countering the Muslim Brotherhood, which it perceives to be a domestic and regional threat, and secondly, influencing Egypt's internal debates and political processes. This dynamic should be seen in the broader context of Egypt-KSA relations, as well as the interconnectedness of political power struggles and religious movements in the region.

In the years before the revolution in 2011, the spread of Salafism in Egyptian society was greatly facilitated by a number of Salafī TV

channels, reaching people more easily than local mosques and organisations, and the work of Salafī charities, which reached millions of poor Egyptians by providing them with essential services such as food, healthcare and literacy classes. Although KSA support of these media outlets and charities was not originally perceived as a national security threat by authorities, the Egyptian government started to take measures to control foreign funding from 2008 onwards.

After the revolution, the previously apolitical Salafī movement developed a political arm, the Nour Party, which was surprisingly successful in the country's first democratic elections, coming second after the Muslim Brotherhood's party. Accusations of covert funding from the KSA have been frequent (although not yet backed by hard evidence), and the Nour Party has openly supported or pushed for policies favourable to the KSA (e.g. handover of two Egyptian Red Sea Islands to the KSA; position on Syria).

## KEY POINTS

■ Existing divisions in society are a vulnerability which can be readily exploited by malign influence. In the case of Egypt, widespread poverty and youth unemployment have provided a key target audience for KSA-sponsored Salafī ideologues. Their vulnerability to Salafī jihadism also provides a national security threat to Egypt.

■ Tracking money flows presents a significant challenge since donations often come from private individuals, and Egypt suffers from a severe lack of transparency and widespread corruption.

■ Foreign funding is not always perceived as a threat. Foreign funding debates in Egypt usually revolve around western funding, rather than funding from the Gulf.

## CONTEXT

■ **Egypt-KSA relations.** For much of the latter half of the 20th century, Egypt and the KSA have had a close relationship; this was mainly due to the fact that Egypt relied on the KSA for security, political and economic support, while the KSA have counted on Egypt as a strong and experienced military force to counter what they perceive to be an expansionist Iran.<sup>3</sup> The KSA supported President Mubarak until he was deposed in 2011. Bilateral relations took a downturn after the Muslim Brotherhood came to power in Egypt, and the Saudi government allegedly gave General Sisi USD 1 billion to overthrow the Morsi government.<sup>4</sup>

■ **Salafism in Egypt.** Contemporary Salafism originated in Egypt in the late 19th century as an intellectual movement aiming to rediscover a purer and more literalist interpretation of Islam which adherents believe the early Muslims practised.<sup>5</sup> Salafism has many similarities to Saudi Arabian Wahhabism. Salafism in Egypt draws its support mainly from the poor.<sup>6</sup> Some estimates indicate that Salafis control around 4,000 mosques in Egypt (3.5 per cent of all mosques) and have over three million followers (3.2 per cent of Egypt's population).<sup>7</sup> Salafis are often described as an apolitical, "quietist" movement<sup>8</sup> – unlike the Muslim Brotherhood, which has strong political aspirations – which may be a key reason why the Egyptian government tolerated Salafism for a long time to counter the influence of the Muslim Brotherhood.<sup>9</sup>

## KEY ACTORS

**Salafī Call** *Egypt's largest Salafī society*

**Nour Party** *the 'Party of Light'; political party founded by Salafī Call after the 2011 revolution*

**Muslim Brotherhood** *transnational Sunni Islamist organisation*

**Egyptian Ministry of Awqaf** *in charge of religious endowments, has administrative control of Egyptian mosques and regulates religious discourse through state-approved imams and sermons*

**Hosni Mubarak** *President of Egypt (1981-2011)*

**Mohamed Morsi** *President of Egypt (2012-2013)*

**President Abdel Fattah al-Sisi** *President of Egypt (since 2014)*

**Abdullah bin Abdulaziz Al Saud** *King of Saudi Arabia (2005-2015)*

## NARRATIVES

### Major Egyptian Salafī groups

- Promotion of ultra-conservative positions, but renouncement of violence.
- Denying receiving financial support from Gulf states.
- Call for non-participation in the 2011 protests during the 'Arab Spring'.

### Salafī Nour Party

- Frequent support of KSA-friendly policies (even when these contradict Egyptian policies).
- More recently, maintaining that Sisi's government is conducting a hostile media campaign against the Nour Party.

### Egyptian government

- Foreign funding of political parties is illegal and undermines national security.
- The KSA is hardly mentioned in the context of foreign funding; discussions usually revolve around western funding.
- Promotion of moderate Islam, especially the teachings of Al Azhar University.
- Wariness of ultraconservative Salafī teachings.

### KSA government

- Support for the coup that removed Mohamed Morsi from power; antipathy towards Muslim Brotherhood.
- Denial of government funding for Egyptian Salafis.

## KEY EVENTS

2005	2006	25 Jan 2011	11 Feb 2011	5 Jun 2011	Nov 2011 – Jan 2012	3 Jul 2013	Sep – Nov 2013	Oct – Dec 2015
Muslim Brotherhood (MB) wins 20 per cent in parliamentary elections.	Government grants licenses to air to Salafi TV channels, likely to counter MB influence. <sup>10</sup>	Egyptian Uprising begins; 'Salafi Call' society discourages its followers from taking part in protests.	Mubarak steps down. Many new media companies and satellite channels (many of them Salafi) are founded in the following months.	Salafi Nour Party is officially licensed.	Parliamentary elections, MB's party wins 47.2 per cent, Nour Party wins 24.3 per cent. Both enter into an uneasy 'marriage of convenience'.	The MB's Morsi is deposed in a coup led by General Sisi; the Nour Party supports the coup.	The Nour Party unsuccessfully tries to preserve Islamic references in the Egyptian constitution.	Parliamentary elections, Nour Party wins only 11 seats and accuses government of arresting its members and conducting a hostile media campaign

## STRATEGIC LOGIC

The KSA's likely aim of promoting Salafi ideology in Egypt and other countries is "to consolidate their political and ideological influence by establishing a network of supporters capable of defending the kingdom's strategic and economic interests."<sup>11</sup> Another motivating factor for promoting Salafism might also be the KSA government's fear of the growing strength of the Muslim Brotherhood, which it perceives as both a domestic and regional threat and which is supported by Qatar, as well as regional rivalry with Iran. Egypt's Salafis have taken up many of the tactics of the Muslim

Brotherhood to spread their ideology, by building public trust and support through providing basic services such as food and education to the poor. The rural poor have been the main constituency of the Salafi Nour Party, which promotes many KSA-friendly policies. Money rarely flows via official government channels, but mostly comes from Salafi charities and private individuals residing in the KSA, usually in the form of "zakat" (alms to the poor, one of the five pillars of Islam).

## MEASURES

**INFORMATION.** Egyptian Salafi groups benefit from a combination of educational, scholarly, and ideological support from the KSA. A large amount of free Wahhabi literature is distributed in mosques and other public institutions.<sup>12</sup> Adnan al Khtiry, a well-known KSA cleric, gave a speech in Egypt in 2011 in which he urged Egyptian voters to support the Nour Party and other Islamist candidates.<sup>13</sup> Satellite channels have become very popular and effective in spreading Salafism, featuring prominent preachers that often reach a celebrity-like status. Many of these Salafi-themed TV channels are believed to receive private funding from Gulf states, or are owned by Saudi investors.<sup>14,15</sup>

**MILITARY/INTELLIGENCE.** Some Salafi Jihadist groups re-emerging in the Sinai Peninsular since 2011 have been accused of receiving financial support from the KSA's intelligence service and certain Wahhabi charities.<sup>16</sup>

**ECONOMIC/FINANCIAL.** 'Salafi Call', the Nour Party's parent organisation, is believed to be the biggest Egyptian recipient of funds from the KSA, and it is estimated that 30 per cent of these funds were/are transferred to the Nour Party to win political votes.<sup>17,18</sup> While direct financial ties have not been proven, there are many recorded instances of unusually high spending by the Nour Party (in particular during election campaigns) which have given rise to that suspicion. Many Egyptian Salafi NGOs and charities, which provide essential social services and education to the population, receive funding from Gulf countries, especially the KSA.

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Political self-determination, independent political processes free from foreign interference.
- Domestic security, especially since one of President Sisi's main sources of legitimacy lies on his pledge to eradicate terrorism.
- Economic development and stability, which President Sisi is attempting to achieve through some reforms.
- Economic independence and energy security.
- Cohesion and unity between different societal groups.

### VULNERABILITIES

- High unemployment rate and lack of opportunities, especially for young people. Over a quarter of Egyptians live under USD 2 per day.<sup>19</sup> Poverty and unemployment are fertile ground for religious extremism.
- Crippled economy since the Arab Spring, which makes Egypt more vulnerable to outside influence, and KSA offers of support become more attractive.
- Shortage of foreign exchange (not least due to loss of tourism income due to instability).
- High levels of corruption and a lack of political will to fight it (many Egyptians believe that Salafi political parties would be less corrupt).
- Rapid population growth (but decrease of resources and arable land).

### THREATS

- Growth of Salafi and other militant jihadi groups (terrorist attacks have steadily grown in numbers and have become more sophisticated).
- Regional instability, especially in neighbouring Libya and Sudan. Arms smuggling across the Libyan border.
- Growing sectarianism: extremist Salafi ideology contributes to growing divisions in society and encourages anti-Shia and anti-Coptic sentiments.
- Foreign sponsoring of a political party is a threat to any country's independent decision-making process.

- Over-reliance on Gulf money. Easy cash allows the government to put off highly necessary but painful reforms. Economic dependency has also been used as leverage by the KSA on several recent occasions (e.g. territorial bargaining in 2017: planned handover of two Egyptian Red Sea Islands to the KSA in exchange for aid and investment).<sup>20</sup>

### EFFECTS

- Growing popularity of Salafism in Egypt, presumably achieved in part thanks to the work of Salafi charities, and the wide reach of Salafi TV channels and websites.
- Development of political Salafism after the 2011 revolution. The astounding success of the newly formed Nour Party in the first free elections is likely due to hidden sources of funding which allowed it to compete in almost every district with significant resources. The Nour Party's declining influence since then can be attributed to internal fighting and splits within the party, and President Sisi's efforts to keep the party at arm's length.
- Gradual and visible increase in religious conservatism over the last twenty years in Egypt, as well as increased sectarian violence.<sup>21</sup>
- Growing awareness of the Egyptian government of the threat posed by Salafi extremism. Counter-efforts include the promotion of more moderate alternatives, closure of some Salafi TV channels, investigations of NGOs over foreign funding, and removal of certain Salafi books from Egyptian mosques.



# NARRATIVES

## Swedish government

- Russia is a potential threat to Sweden, but should not be exaggerated.
- NATO membership is a multifaceted issue.
- Swedish defence of Gotland is important for regional security in the Baltic Sea.

## CEPA

- US involvement is vital for regional security in the Baltic Sea.
- Russian military activity in the Baltic Sea is a security threat.
- Allied defence of Gotland is vital for regional security in the Baltic Sea.

## Russian government

- There is an irrational fear of Russia in Sweden; key communicators in Sweden are aggressive and warmongering.
- The US is demonising Russia to encourage Swedish NATO membership.
- Sweden's increased defence spending is destabilising the Baltic Sea.

# KEY EVENTS

16 Jun 2015	24 Jun 2015	28 Jun 2015	30 Jun 2015	15 Jul 2015	16 Jul 2015	17 Jul 2015
Swedish Parliament approves total defence measures policy.	CEPA publishes report on Baltic security, claiming that Russian military exercises had included scenarios for the seizure of Gotland. This report stimulates public debate in Sweden.	Governor of Gotland is quoted in <i>Expressen</i> : "It's very necessary to have a permanent defence here. We need people on the ground prepared for a possible invasion."	Governor of Gotland speaks on a panel at Almedalen: "We usually say that we are an aircraft carrier. You can launch a war [on mainland Sweden] from Gotland."	<i>Sverige Radio</i> quotes Governor of Gotland (articles in Russian and German): Gotland "could be used as an aircraft carrier in the middle of the Baltic Sea, which could be used by Russia during a possible invasion of the Baltics." Summary of article appears in Russian news agency <i>Regnum</i> .	<i>Sputnik</i> (in French): "Swedish Official: The Island of Gotland is Well-Placed to Bomb Russia."  <i>Sputnik</i> (in English): "Sweden Getting Ready to Fire Missiles at Russian Troops from Gotland Island."	Governor of Gotland issues clarification of her comments.

# STRATEGIC LOGIC

The technique used in this case study of disinformation is the *laundering of information*. This describes a process similar to money laundering – the process of legitimising dirty money by obscuring its illegal origins – adapted to the information environment. In this case, the process is reversed, by taking information and laundering it through intermediaries to deliberately distort the original meaning. These intermediaries cite authentic sources but do so with minor changes to the text and by

removing the original context and meaning. *Sputnik* then refers to these intermediaries as its sources for the falsified quote. The result is a "dirty" quote that has been "laundered" via intermediaries to appear legitimate. Fake news and disinformation sources may also be legitimised through this process and the *Sputnik* article should be seen as part of a broad range of disinformation techniques.

# MEASURES

**DIPLOMATIC.** Russian politicians and diplomats frequently intervene in Swedish domestic affairs regarding NATO and Baltic Sea security.<sup>4</sup> The Russian President and Foreign Minister have openly warned Sweden against NATO membership.<sup>5</sup>

**INFORMATION.** *Sputnik* is one example of how disinformation is used with the aim of undermining Swedish society and weakening confidence in public and private sector institutions.<sup>6</sup>

**MILITARY.** Russia has a long history of violating Swedish airspace and waters. This has contributed to an increased sense of threat to national security that places public concerns about Russia at only a marginally lower level than the threat from international terrorism.<sup>7</sup>

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

■ Public debates surrounding political decision-making on defence matters. In this case, the debates concern the level of threat from Russia, Sweden's relationship with NATO, the level of funding of the Swedish military, and the relationship between Gotland and the Swedish mainland.

■ Effective Swedish defence, outlined the government's proposition 2014/15:19, which emphasises the concept of "total defence" to stress the necessity of collaboration between military and civilian defence, with a particular focus on the roles of government agencies and local government.

## VULNERABILITIES

■ Open and democratic debate can also turn into a weakness when actors deliberately seek to leverage pre-existing ideological divisions (e.g. sentiments regarding immigration or NATO) to suit other ends. Polarised domestic debates are fertile ground for foreign influence.

■ The territorial vulnerability of Gotland and the debate about remilitarising the island is exploited in the *Sputnik* article discussed here.

## THREATS

■ Hostile influence on domestic political debates by spreading disinformation (here: through mistranslation and removing statements from their original context) by news sources like *Sputnik*. This is especially concerning when debates surround issues of national security.

■ Skewing of debates also threatens to lead to stronger social divisions regarding polarised topics.

## EFFECTS

■ Increased government and public awareness of the threat posed to national security by Russian information warfare. Many initiatives related to countering disinformation and fake news, bursting filter bubbles, and source criticism have been launched in Sweden or have been supported by Swedish actors.

■ This specific *Sputnik* article discussed here does not seem to have had any effect in influencing debates or decisions (except for potentially reinforcing certain minority opinions). CEPA's report was far more effective in setting the agenda for Swedish discussions on NATO membership by increasing public awareness. *Sputnik* lifted a narrative that may fit with conspiracy theories about Swedish aggression against Russia and re-militarisation.

# HAMAS' USE OF HUMAN SHIELDS IN GAZA

## SUMMARY

Hamas, an Islamist militant group and the de facto governing authority of the Gaza Strip, has been using 'human shields' both defensively and offensively in conflicts with Israel since 2007. According to the Statute of the International Criminal Court (ICC), the war crime of using human shields encompasses "utilizing the presence of a civilian or other protected person to render certain points, areas, or military forces immune from military operations."<sup>1</sup> Hamas has launched rockets, positioned military-related infrastructure-hubs and routes, and engaged the Israeli Defense Forces (IDF) from, or in proximity to, residential and commercial areas.

The strategic logic of human shields is based on an awareness of Israel's desire to minimise collateral damage, and of Western public opinion's sensitivity towards civilian casualties. If the IDF uses lethal force and causes an increase in civilian casualties, Hamas can utilise that as a legal instrument, accusing Israel of committing war crimes, which could result in the imposition of a wide array of sanctions. Alternatively, if the IDF limits its use of military force in Gaza to avoid collateral damage, Hamas will be less vulnerable to Israeli attacks. Moreover, despite the Israeli public's high level of support for the Israeli political and military leadership during operations, civilian casualties are one of the friction points between Israeli left-wing and right-wing supporters.

Israel's efforts to avoid civilian casualties have been multifaceted: the IDF imposed restrictions on the use of force in the vicinity of civilians and focussed on precision airpower to reduce the risk of collateral damage. Moreover, the IDF has taken to warning residents to evacuate prior to an impending air strike (by dropping leaflets, phoning residents, or firing missiles without explosive warheads onto the roof), although in doing so they lose the element of surprise, and Hamas frequently used the warning to encourage civilians to gather at the targeted site. As part of a wide range of legal safeguards within the IDF's operational chain of command, the IDF's international law unit (the "Dabla") has to approve each target to ensure compliance with international law.<sup>2</sup> Moreover, the IDF has taken pains to explain their targeted strikes to both internal and external audiences, in particular via social media.<sup>3</sup> Nevertheless, Israel has not managed to dominate the narrative, with many international organisations and foreign governments accusing Israel of using disproportionate force.

## KEY POINTS

- The use of human shields can be considered an example of 'lawfare' – i.e. the use of the legal system against an enemy by damaging or delegitimising them, tying up their time or winning a public relations victory.<sup>4</sup>
- Even if a targeted strike may be justifiable from a legal perspective, first impressions frame the narrative. Public opinion tends to be influenced more by images depicting the suffering of innocent civilians than by well-thought-out legal arguments.
- National governments should be able to justify their position publicly and reveal their adversary's use of civilians in combat. This can only be accomplished by thoroughly documenting incidents, preparing supportive messages, and working across multiple channels to convey those messages.
- Priority should be given to information activities aimed at the very civilians who are used as human shields, in order to undermine the adversary and convince civilians to actively or passively refuse to serve as human shields. Such activities need to be coherent and consistent and coordinated.



## CONTEXT

■ **Use of human shields.** Hamas is not the only militant organisation using human shields – it was in fact inspired by Hezbollah's strategy in Lebanon.<sup>5</sup> Other Palestinian organisations such as the Islamic Jihad Movement in Palestine, the Popular Resistance Committees (PRC), or the Humanitarian Relief Foundation (IHH) have also resorted to human shields. Even the IDF have used human shields in the past; however this practice

was declared unlawful by the Israeli Supreme Court, and several officers were court-martialled for applying the technique.<sup>6</sup> Typical uses of human shields include launching attacks from densely populated civilian areas, locating military infrastructures in civilian areas, or protecting terrorists' houses and military facilities.

## KEY ACTORS

**Hamas** *Palestinian fundamentalist Sunni organisation that has been designated by the US, the EU and other countries as a terrorist group*  
**Israeli Defense Forces (IDF)**  
**Israel Security Agency (Shabak / Shin Bet)** *monitors terrorist activity in the Gaza Strip and the West Bank*  
**Israel Ministry of Foreign Affairs**

**Ismail Haniyeh** *former Prime Minister of the Palestinian National Authority, current head of Hamas Political Bureau in Gaza, has frequently encouraged Palestinians to act as human shields (e.g. to climb to the roofs of houses targeted by the IDF)*  
**Khaled Mashal** *head of Hamas Political Bureau (1996 – 2017)*

# NARRATIVES

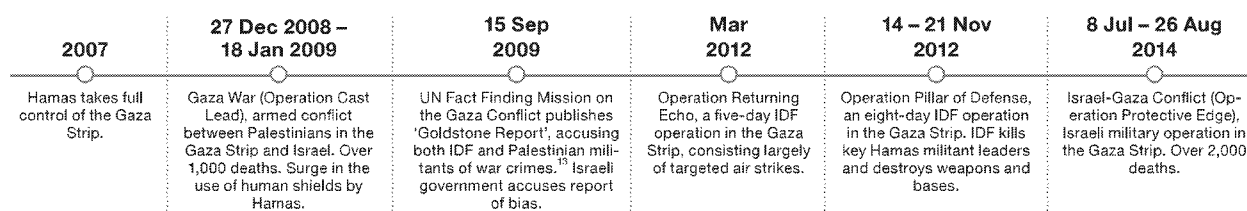
## Hamas

- Israel commits war crimes and is indiscriminately killing Palestinian civilians.
- The Palestinian people support Hamas unconditionally, even if that means risking their lives.<sup>7</sup>
- It is the Palestinian people's religious and national duty to serve as human shields, in order to serve the resistance and support its cause.<sup>8</sup>
- Israel's early warning messages before an airstrike are psychological warfare.<sup>9</sup>

## Israeli government

- Israel uses military force to protect its citizens in light of Hamas' aggression. It only targets Hamas' military facilities and militants.<sup>10</sup>
- Civilian casualties are caused by Hamas' use of human shields to protect its assets. Israel actively engages in all possible efforts to avoid harming civilians, including alerting them before strikes.<sup>11</sup> The IDF often cancels planned strikes when there is a risk to civilians.
- The Palestinian population in the Gaza Strip is subjected to Hamas' terror and does not support the movement's use of human shields.<sup>12</sup>

# KEY EVENTS



# STRATEGIC LOGIC

The dense, heavily populated Gaza Strip provides the ideal setting for a terrorist and paramilitary organisation. The region consists of a variety of populated areas both organised and unorganised, temporary and permanent, aboveground and under the surface. Those areas, comprising of cities and refugee camps (which are even more densely populated), enhance the defender's advantage. Hamas' defensive and offensive strategies are based

on leveraging these advantages in combat with the IDF, inspired by Hezbollah's strategy in Lebanon.<sup>14</sup> The objective of this strategy is to maximise the IDF's casualties while protecting Hamas' forces and infrastructure from the IDF's military supremacy. This strategy accepts the possibility of civilian casualties, and even leverages these for internal and external propaganda.

# MEASURES

**DIPLOMATIC.** Incidents of civilian casualties are recorded by Hamas, and the (frequently manipulated) footage disseminated across a wide array of media channels (esp. social media, satellite TV channels).<sup>15</sup> During the fighting itself, Hamas' aims its communications efforts mainly at the local Palestinian population to build resilience; post-conflict communications are aimed primarily at the international community to cause reputational damage to Israel and limit its strategic choices by controlling the narrative. The use of human shields is aimed at earning points in the global arena, by delegitimising Israel's use of force, creating continuous pressure through international institutions (e.g. UN and EU) and NGOs, and promoting sanctions and prosecution by international tribunals. Since the international community does not recognise Hamas as the political representative of the Palestinian people, its diplomatic activities are usually carried out by third-party states and pro-Palestinian organisations (e.g. presenting 'proof' of alleged war crimes).

**MILITARY.** Use of primary military force from within densely populated areas (e.g. launching of rockets and mortar shells), from which Hamas conducts operations while blending in with the local population (e.g. wearing civilian clothing). Hamas thus responds to the IDF's military and technological supremacy by creating an asymmetric equation, leveraging terrain advantages and using civilian populations to protect their military assets.

**ECONOMIC.** Hamas uses the damage caused to civilians and civilian infrastructure as a justification to raise funds from its donor nations (e.g. Qatar, Turkey) and other allies. Hamas also uses (and pays) civilians to dig tunnels, which are a primary source of revenue, commodities, arms and fighters for Hamas, and conceals their entry points beneath civilian buildings.<sup>16</sup>

**LEGAL.** Hamas aspires to exploit Israel's commitment to normative and explicitly defined international law. Using human shields provides Hamas with a win-win scenario: if the IDF uses kinetic force and the number of civilian casualties surges, Hamas can accuse the IDF of committing war crimes; if the IDF limits its use of force to avoid collateral damage, Hamas will be less susceptible to Israeli attacks. Hamas operates effective mechanisms to gather any potentially incriminating information that could prove that the IDF committed war crimes in Gaza. Once evidence is gathered, Palestinian supporters (usually lawyers) will file complaints against Israel in courts of European nations. Hamas skilfully manages to prolong reputational losses for Israel through the time it takes to have cases heard and adjudicated to their advantage.

# NATIONAL SECURITY INTERESTS

## CRITICAL FUNCTIONS

- Effective defence of Israeli territory and the lives of its citizens.
- International reputation as a country that abides by international law.
- Good relationships with Israel's allies.
- Unity within Israeli society during and after military operations.

## VULNERABILITIES

- From a purely military perspective, Israel's commitment to international law limits its ability to freely terminate the threats posed by Hamas.
- Civilian casualties are one of the friction points within Israeli society: although the Israeli public generally supports its political and military leadership during operations, left-wing groups will usually question the outcomes of the operations.
- Dependency on international support as a cornerstone of Israel's foreign policy.

## THREATS

- Human shields limit the IDF's ability to effectively combat Hamas with their technological and military supremacy. The launching of attacks from heavily populated areas also makes critical Israeli infrastructure more vulnerable to rockets and mortar shells.
- Increased divisions within Israeli society over civilian casualties.
- Increased tension between Israel and its allies over excessive force.

## EFFECTS

- Over the years, Israel's public image has suffered tremendously due to reports and images of civilian casualties. Hamas efforts in controlling the narrative have been successful. Almost every large-scale conflict in the Gaza Strip resulted in an international investigation committee, usually led by the UN, to examine whether IDF operations were lawful. Even Israel's closest allies (e.g. UK, Germany, France) have widely criticised Israel's actions.
- The IDF put certain limitations on the use of force<sup>17</sup> and developed more accurate means to strike individuals and infrastructure. It has also taken to warn civilians residing in the proximity that an attack is approaching, thus allowing civilians to evacuate, but limiting the effect of a surprise attack.<sup>18</sup>

# THE 2010 SENKAKU CRISIS

## SUMMARY

The Senkaku Islands are a group of five uninhabited islands and three islets located in the East China Sea. They are under the administrative control of Japan, but are also claimed by China and Taiwan. The Senkaku Islands are of great economic value due to rich fishing grounds and significant oil and gas deposits in the surrounding exclusive economic zone (EEZ). The islands are also of great geostrategic value, facilitating control over the East China Sea.

In September 2010, a Chinese fishing trawler refused Japanese Coast Guard (JCG) requests to leave Senkaku territorial waters. After a stand-off, the trawler rammed two JCG vessels and after a 40 minute chase, the JCG boarded the Chinese trawler and arrested the 15 man crew and captain. The captain was later tried under Japanese domestic law. In response, China drastically curbed its rare earth elements (REE) exports to Japan, whose high-tech oriented economy is very dependent on Chinese REE imports. These hostile economic measures were accompanied by a number of other escalatory measures, including

rhetorical threats, the encouragement of popular protests across China, and the arrest of four Japanese nationals in China for allegedly photographing military targets. All these measures were implemented with various degrees of ambiguity. Short-term, China wanted to force Japan to release the detained trawler captain; long-term, China wanted to demonstrate its ability to use a potent economic instrument as deterrent and as coercive measure or for punishment.

The Japanese government came under strong domestic criticism for the way it dealt with the crisis, in particular for releasing the Chinese captain after several weeks without indicting him. Citizens took to the street to protest both China's behaviour and the "weakness" of the Japanese government. Video footage proving the deliberate nature of the boat ramming was not released to the wider public, likely out of fear of further diplomatic clashes with Beijing.<sup>1</sup> The footage was eventually leaked online and led to increased criticism of the Japanese government for keeping details of the incident from the public.

## KEY POINTS

- This was an example of a small incident which escalated into an international diplomatic crisis. While it is highly unlikely that the Chinese fishing trawler was acting under direct command of Beijing, the incident was still readily exploited for strategic gain.
- Adversarial measures relied heavily on ambiguity. The two key aspects included the informal nature of the embargo on REE and the involvement of a non-state actor (civilian fishing vessel) as catalyst for the conflict.

- In response to such flexible and adaptive StratCom approaches, nations should focus on the consistency and coherence of government messaging, rather than trying to decipher deliberately ambiguous statements and actions.

- Analysing the 2010 Senkaku crisis from the perspective of 2017, it very much resembles an initial engagement used to test the opponent's defences and potential international reaction. The political tensions between China and Japan resurged in 2012 and remain elevated, with the islands as one focal point of the confrontation.

## CONTEXT

- **The role of the US in the dispute.** The US-Japan Treaty of Mutual Cooperation and Security (TMCS) provides a legal framework for stationing of US military bases in Japan, and commits both parties to assist each other in case either of them is attacked on Japanese territory. However, the Senkaku Islands are only covered implicitly in treaty, and the US does not formally take sides in the Senkaku dispute. In August, just before the crisis, Japanese media reported unverified sources claiming that the Obama administration was unwilling to include the Senkaku Islands under the protection of the TMCS, which prompted speculation in Japan about the strength of US security guarantees.<sup>2</sup>

- **EEZ violations.** Japan treated past territorial violations by illegal fishing in the exclusive economic zone of the islands as a criminal matter rather than a political issue. Occasional stunts by anti-Japan activists to

reach the islands by sea have sometimes reignited bilateral tensions; Tokyo committed to a "deport-not-detain" policy. In the months prior to the September 2010 crisis, violations by illegal fishing increased considerably.

- **Rare Earth Elements (REE).** REEs, a set of 17 chemical elements, are a critical component in the production of a wide range of technologically advanced civilian and military products. Since the early 2000s, production has been dominated by China: in 2009, Japan depended on China for around 90 per cent of its REE needs.<sup>3</sup> From the mid-2000s, China began to impose production and export quotas on the domestic REE industry, citing environmental concerns. In July 2010, the amount of planned REE exports for H2 2010 was slashed by 72 per cent compared to the same period in the previous year.

## KEY ACTORS

### Ministry of Foreign Affairs of China

**Baodiao Movement** A social movement in China, Hong Kong and Taiwan that defends Chinese sovereignty over the Diaoyu/Senkaku islands

### Ministry of Foreign Affairs of Japan

### Japanese Coast Guard (JCG)

### Ministry of Foreign Affairs of Taiwan

### US Department of State

**Wen Jiabao** Premier of China (2003 – 2013)

**Naoto Kan** Prime Minister of Japan (2010 – 2011)

**Seiji Maehara** Foreign Minister of Japan (2010 – 2011)

**Wu Den-yih** Premier of Taiwan (2009 – 2012)

**Barack Obama** President of the United States (2009 – 2017)

**Hillary Clinton** Secretary of State of the United States (2009 – 2013)

**Robert M. Gates** Defense Secretary of the United States (2006 – 2011)

## NARRATIVES

### Chinese politicians and state-controlled media (unified front)

- Japan's actions are illegal and unreasonable.
- The Senkaku Islands are rightfully China's.
- China has not imposed any REE embargo.
- Both parties should be careful not to escalate this situation; Japan and China need each other and should work together to compromise.

### Japanese political elite (divided, criticised each other)

- Reaffirmation of Japan's right to the Senkaku Islands; fervent anti-Chinese rhetoric.
- Underlining the necessity to prevent escalation and find a solution.
- Criticism of Naoto Kan's handling of the crisis, "national humiliation."

### Taiwanese government

- Criticism of Japan's actions in the Senkaku/Diaoyu area; calling for de-escalation and calm approach.
- Assertion of Taiwan's claims to the islands as part of greater Chinese territory, while also distancing Taiwan's diplomatic position from that of China.

### US government

- Proposing US as potential mediator; bilateral talks to solve the dispute.
- No public confirmation of US obligation to defend the Senkakus under TMCS, but reaffirmation of general support for Japan.



## KEY EVENTS

7 Sep 2010	7-14 Sep	8-18 Sep	11 Sep	19 Sep	20 Sep	21 Sep	24 Sep	2 Oct	29 Nov
Chinese fishing trawler rams two Japanese Coast Guard vessels. JCG detains captain and crew.	Japanese Ambassador is summoned 6 times to meet high-level Chinese officials.	Anti-Japanese protests across China (Beijing, Shanghai, Hong Kong).	China suspends talks with Japan on joint exploration of gas and oil resources in East China Sea.	China suspends ministerial and provincial-level contacts with Japan.	4 Japanese nationals are arrested in China for allegedly trespassing military zone and taking photos.	China unofficially restricts shipments of unprocessed REE exports to Japan (e.g. salts, oxides, metals).	Japan releases Captain Zhan Qixiong.	Large protests across Japan against the gov's handling of crisis and China's behaviour.	REE shipments to Japan are fully restored.

## STRATEGIC LOGIC

China's behaviour was characterised by a significant degree of escalation both *vertically* (the severity of measures) and *horizontally* (the number and diversity of measures).

China's actions were highly ambiguous. As the captain of the civilian fishing trawler was reportedly drunk<sup>1</sup> at the time of the incident, the Japanese were unable to attribute political responsibility to China for the incident, nor prove that the action was a result of a planned hostile political action conducted

by a proxy. The detention of four Japanese individuals was arranged so that there was no direct evidence of a connection with the detention of the Chinese captain. The disruption of REE shipments to Japan was also highly ambiguous, as it was (a) officially denied by Beijing, (b) a manipulation of the work pattern of the customs officials, (c) introduced in circumstances conducive to supply disruption (i.e. post drastic reduction of REE export quotas).

## MEASURES

**DIPLOMATIC.** Frequent summoning of the Japanese Ambassador by the Chinese MFA. Suspension of bilateral contacts on ministerial and provincial level. Tolerance of anti/Japanese protests across China.

**INFORMATION.** Coordinated anti-Japan campaign by Chinese state-controlled media.

**MILITARY.** No use of conventional military capabilities, but use of paramilitary units (vessels belonging to the Fisheries Law Enforcement Command) to challenge Japanese control over Senkakus. Vessels reached contiguous zone, but did not violate territorial waters.

**ECONOMIC.** Restriction of REE export quotas (2 months before the crisis, Beijing announced a massive reduction of REE export quotas for H2 2010 by 72 per cent compared to H2 2009, which created a fragile situation for Japanese importers). Disruption of REE shipments to Japan from 21 September<sup>2</sup> (Chinese customs officials refused to process new orders and prevented dockers from loading shipments which were already processed; Chinese authorities repeatedly denied having imposed any additional re-

strictive measures). Variety of threats to Japanese economic interests (including calls for boycotts of Japanese products and for the disruption of Japanese business operations in China through blockades or even vandalism of Japanese-owned assets).<sup>6</sup> Suspension of several bilateral economic initiatives (including joint exploration of natural resources in East China Sea). Transport of equipment to offshore platforms located in disputed part of the EEZ in the East China Sea.<sup>7</sup>

**INTELLIGENCE.** Given the extensive links between the China state security apparatus and various Chinese nationalist groups, it is likely that Beijing played an instrumental role in supporting and organising anti-Japanese protests in Hong Kong and Taiwan, in particular the Baodiao movement.<sup>8</sup>

**LEGAL.** Detention of four Japanese nationals on 20 September for allegedly trespassing into a military zone (the dubious nature of the charges and the coincidence with Japan's 19 September decision to extend the arrest of the Chinese captain indicate that this was a component of Beijing's countermeasures).

## NATIONAL SECURITY INTERESTS

### CRITICAL FUNCTIONS

- Coverage of Senkaku Islands by the Japan-US security treaty (TMCS).
- Enforcement of effective control around the Senkaku Islands, demonstrating Tokyo's de facto ownership. Ensuring desired geostrategic position of Japan in the East China Sea.
- Stability of the high-tech manufacturing sector.
- Maintenance of public order and cohesion of Japanese society.
- Maintaining credibility of the official narrative regarding the Senkaku Islands ("Senkakus are legally part of Japanese territory," "no territorial disputes exist," "Japan is capable of effectively enforcing control over area").

### VULNERABILITIES

- Weakened domestic position of PM Kan and the ruling DPJ party (barely survived leadership challenge in August). Presence of militant pacifist and nationalist factions in Japanese society, both groups could be exploited by a potential adversary to impose political cost on the Japanese government.
- Trilateral and asymmetric nature of the territorial claims (Japan's claims are contested by both China and Taiwan; anti-Japanese sentiment could bring China and Taiwan closer together).
- Deterioration of US-Japanese relations following the DPJ's victory in the 2009 elections: DPJ had demanded more equal relations with US. Ambiguity surrounding US commitment to defend Senkaku Islands.
- Anti-Japanese sentiment in the region due to Japan's WWII history. Significant constraints on use of military force (i.e. Article 9 of Japanese Constitution). Lack of permanent military or administrative infrastructure on the islands. Private ownership of three out of five Senkaku Islands, which may prevent Tokyo from exercising optimal level of control.
- Significant economic reliance on China.<sup>9</sup> High and quasi-structural dependence on Chinese supply of REE.

### THREATS

- The Japanese government was put in a delicate position where potential (real or perceived) under- or over-reaction would likely provoke a domestic political crisis. Social unrest due to perceived weakness of government.

- Demonstration of Tokyo's lack of effective control over the area by increased number of incursions and maritime confrontations. Tolerance of Chinese incursions might result in Beijing establishing a quasi-permanent presence of para-military units of fishermen militias and coast guard.
- Formation of a unified anti-Japanese front between China and Taiwan over Senkaku Islands.
- Disruption of Japan's high-tech manufacturing sector.
- Drainage of gas reserves from the disputed EEZ in the East China Sea.
- Mishandling of the crisis might create a political precedent, negatively affecting Japan's position in its other territorial disputes.

### EFFECTS

- Transformation of the Senkaku issue into a domestic political problem that severely weakened the government (PM Naoto Kan eventually resigned in 2011). The Senkaku Islands became an emotionally-loaded issue for the Japanese public. The 2010 crisis set a chain of events in motion which led to the 2012 Senkaku crisis (which was much more severe than the 2010 crisis).
- Significant deterioration of China-Japanese relations. Strengthening of nationalist anti-Chinese sentiment in Japanese society.<sup>10</sup>
- Short-term disruption of the Japanese manufacturing sector due to REE shortage. Massive short-term global REE price increase, followed by a medium-term decrease. Implementation of a variety of REE supply diversification strategies (e.g. increased REE recycling, seeking alternative sources of supply and substitutes, developing further strategic reserves). However, China managed to maintain its position as dominant REE supplier to Japan. Relocation of REE processing operations of several large Japanese companies to China, to limit the risk of supply disruptions.
- Domestic and international press coverage of the Japanese government during crisis was more negative than positive. The vague rationale of releasing the Chinese captain was perceived as sign of political inconsistency or even diplomatic incompetence.

# HUMANITARIAN AID IN THE RUSSO-GEORGIAN CONFLICT

## SUMMARY

During the Russo-Georgian conflict of 2008, the Russian Federation used 'humanitarian' assets in support of the separatist populations of Abkhazia and South Ossetia, two regions of Georgia which both declared independence in the early 1990s. The Russian government provided "significant quantities of food, water, medications, water purification facilities, diesel power plants, tents and other material resources,"<sup>1</sup> and set up refugee camps. On 11 and 12 August 2008, two large convoys were sent to South Ossetia's capital, transporting, amongst other things, "two mobile field hospitals [...], 58 tons of food supplies, 31 power generating stations, potable water and more than 200 rescue workers."<sup>2</sup>

The Russian government used what it termed 'humanitarian assistance' as an instrument to pursue broader policy goals that were not humanitarian in nature. Moscow relied on relief efforts and the language of humanitarianism to present itself as a neutral and impartial actor and to justify its continued support for the residents and de facto authorities of Abkhazia and South Ossetia, despite Georgian protests against its continued involvement. Russia thus exploited the tensions

between the laws surrounding territorial sovereignty and the imperative to provide effective relief to civilians.

In the larger context of the Russo-Georgian conflict, Russia's provision of humanitarian assistance played merely a secondary or indirect role, since other measures adopted by Russia (e.g. 'passportisation', economic assistance, arms supplies and eventually full military intervention) presented a direct and far more severe challenge to Georgia's national security. However, humanitarian assistance was of great diplomatic and information value, as it enabled Russia to portray itself as a neutral actor motivated by considerations of civilian protection. The humanitarian activities were also used to strengthen the political and social ties between Russia and the Abkhaz and South Ossetian populations and to weaken their allegiance to the Georgian state. Russia's 'humanitarian' activities demonstrated Georgia's incapability to prevent Russian intervention in its domestic affairs and physical territory, as well as its inability to assert its authority over Abkhazia and South Ossetia.

## KEY POINTS

- The instrumental use of law is not limited to armed conflict but also occurs in peacetime. The term 'lawfare' may be too narrow, if applied to describe the (mis)use of law as a substitute for conventional military means, to capture the instrumental use of legal arguments outside of armed conflict and the military context.
- There is a close link between legality and legitimacy, and between legal justifications and broader strategic narratives. Legal arguments can serve both as a source of legitimacy and as a tool to delegitimise an adversary. In the Georgian scenario, Russia used the law in an instrumental manner as part of a broader narrative, and its arguments were

designed to promote a narrative of legality and legitimacy, rather than to make a compelling legal case.

- Western nations and institutions should conceptualise law as a domain to counter the use of legal instruments when used in a hostile manner. This would also foster a more dynamic approach to the use of law and legal argument to counter hybrid threats.

## CONTEXT

■ **Secessionist regions in Georgia.** Georgia gained independence from the USSR in 1991, although it immediately faced armed secessionist movements in the regions of South Ossetia and Abkhazia, which were actively supported by Russia. Particularly since the so-called Rose Revolution in November 2003 led to a pro-Western political environment in Georgia, Russian support of the secessionist regions is widely understood to be motivated by geopolitical considerations aimed at countering Western influence. The Russian Federation has a long history of providing humanitarian aid and assistance to the separatist regions, stretching back to the conflicts of the early 1990s.

■ **The 2008 conflict.** From 2004 to 2008, relations between Georgia and the two separatist regions deteriorated sharply, as did Russo-Georgian relations. Violence intensified in the first half of 2008, followed by mutual accusations of preparations for war. Large-scale hostilities broke out between the Georgian and South Ossetian sides on 7 August, leading to

Russian intervention on 8 August and to active hostilities in the Abkhaz zone from 9 August. Armed conflict between Georgia and Russia lasted until 12 August. Approximately 850 people were killed and up to 3,000 wounded;<sup>3</sup> around 138,000 people were internally displaced.

■ **International legal framework of humanitarian assistance.** The international community has not developed a single overarching legal regime to regulate the provision of humanitarian aid and assistance in a comprehensive manner. Different legal rules and considerations apply in times of peace and under the law of armed conflict. In the absence of armed conflict, the legal regulation of humanitarian assistance is caught between two competing imperatives: respect for the sovereignty of the affected state and the need to provide effective relief to the civilian population. A key question is whether or not humanitarian assistance falls foul of the principle of non-intervention in the absence of the territorial state's prior consent.

## KEY ACTORS

**United Nations Security Council**  
**EMERCOM** *Russia's Ministry for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters*

**Dmitry Medvedev** *President Russian Federation (2008 – 2012)*  
**Sergey Lavrov** *Foreign Minister Russian Federation (since 2004)*  
**Vyacheslav Kovalenko** *Russian Ambassador to Georgia (2006 – 2008)*  
**Vitaly Churkin** *Russian Permanent Representative to the UN (2006 – 2017)*  
**Mikheil Saakashvili** *President of Georgia (2008 – 2013)*  
**Irakli Alasania** *Ambassador of Georgia to the UN (2006 – 2008)*