Overview of countermeasures by the EU28 to the Kremlin’s subversion operations

How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies?

Jakub Janda
Head of the Kremlin Watch Programme

Veronika Víchová
Kremlin Watch Analyst

Monika Richter
Kremlin Watch Analyst

Ilyas Sharibzhanov
Kremlin Watch Analyst

Jakub Fišer
Kremlin Watch Member

Kremlin Watch is a strategic program of the European Values Think-Tank, which aims to expose and confront instruments of Russian influence and disinformation operations focused against liberal-democratic system.
Overview of countermeasures by the EU28 to the Kremlin’s subversion operations

XII. Greece .................................................................................................................... 62
XIII. Hungary ................................................................................................................. 64
XIV. Ireland ..................................................................................................................... 67
XV. Italy .......................................................................................................................... 69
XVI. Latvia ....................................................................................................................... 72
XVII. Lithuania ................................................................................................................. 75
XVIII. Luxembourg ......................................................................................................... 78
XIX. Malta ....................................................................................................................... 80
XX. The Netherlands ....................................................................................................... 82
XXI. Poland ..................................................................................................................... 85
XXII. Portugal .................................................................................................................. 88
XXIII. Romania ............................................................................................................... 90
XXIV. Slovakia ................................................................................................................ 93
XXV. Slovenia ................................................................................................................ 96
XXVI. Spain ..................................................................................................................... 98
XXVII. Sweden ............................................................................................................... 101
XXVIII. The United Kingdom ......................................................................................... 104
1. Introduction

This Report summarises the attitudes, policies, and strategic responses of the EU28 to Russia’s disinformation campaign and other hostile influence operations. It is now a robustly documented fact that, since the eruption of the Ukrainian conflict in 2013, the Kremlin has pursued increasingly aggressive efforts to destabilise Western alliances, undermine their democratic processes, and sow civil discord. The purpose of this Report is to describe and assess the specific strategies and countermeasures (or lack thereof) adopted across the EU28 in response to the Kremlin’s malign influence operations. The findings of the Report are based on a qualitative analysis of national strategy documents, reports, and official statements from all 28 member states that reveal the priorities of their individual foreign, security, and defence policies. Demand is growing for a coordinated international response to Russian aggression, with many EU heads of state, other European politicians,¹ and security experts² voicing alarm about the threat. As of May 2017, several Western countries have experienced Russian interference in their elections, while the number of cyberattacks across Europe continues to rise.³

Specifically, this Report aims to summarise how individual EU member states are reacting to this growing threat in three separate domains: 1) the government and political establishment, 2) the counterintelligence community,⁴ and 3) the non-governmental (civic) sector. The Report thus provides a comprehensive comparative overview of the current state of play in Europe, identifying common strengths and weaknesses between countries and, most importantly, providing concrete policy recommendations for security and defence enhancement based on specific regional and group trends.

Of course, it is important to keep in mind that typological studies are inherently reductive and thus cannot fully account for the particularities and complexity of individual cases (in this instance, the EU28 country profiles). Nonetheless, the identification of regional and group patterns, common challenges, and proven best practices is a valuable exercise for gaining a deeper understanding of both the threat in question and the most effective palliative policies. The authors hope the Report fulfils these objectives and, furthermore, that it stimulates political will for decisive and internationally-coordinated action against Russian disinformation and other means of subversive influence. Any errors or omissions are our own.

² See <http://www.europeanvalues.net/mogherini/>
³ “EU Suffers Jump in Aggressive Cyberattacks”. Financial Times. 8 January 2017. <https://www.ft.com/content/3a0f0640-d585-11e6-944b-e7eb37a6aa8e>
⁴ The authors understand that, by nature, counterintelligence work cannot be done in the public view. However, we maintain that it is a matter of public duty for national intelligence and counterintelligence agencies to issue public warnings about urgent national security threats, for instance in their annual reports or open statements on leadership.
2. Method

Country profiles detailing the state of play in each EU member state were compiled using policy reviews, media analyses, and independent expert data. We reviewed official strategy documents and summary reports of each member state, together with recent statements made by their political representatives and security/intelligence officials. Our analysis centred on content pertaining to the influence of foreign powers, cyber-security, disinformation campaigns, counterintelligence activities, and media literacy programs. We searched for all available data on policy proposals and countermeasures (both planned and implemented), as well as evidence of their effectiveness, using open-source, online, and academic sources. We also utilised the expertise gained through our cooperation with numerous institutions and organisations in the countries under review, in order to identify the most effective national projects and local response initiatives. If we have missed any relevant initiative, we will gladly update the Report as feedback arrives.

The chief methodological contribution is the development of a rating system based on three qualitative measures: 1) political acknowledgment of the threat by state representatives, 2) government strategy and applied countermeasures, and 3) counterintelligence responses. The tables below define and operationalise the scale for each of the three measures. Based on each country’s total score (the sum of all three measures), we generated an overall symbolic ranking and grouped the EU28 into six categories based on their recognition of and response to the Russian threat. This categorisation is the basis of the Report’s conclusions and also structures our final recommendations based on individual states’ experience and capabilities. These recommendations follow the experiences and best practices of the EU countries that are most advanced in countering disinformation and hostile influence.
## Analytical framework: Operationalisation of the rating scale

### Political acknowledgment of the threat

<table>
<thead>
<tr>
<th>RATING</th>
<th>DESCRIPTION</th>
<th>SYMPTOM(S)</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>COLLABORATION WITH HOSTILE FOREIGN INFLUENCE</td>
<td>Governing politicians are receptive to Russian influence and cooperate with the Kremlin</td>
<td>Evidence of cooperation between governing politicians and hostile foreign agents; prevention of any state response to the threat</td>
</tr>
<tr>
<td>1</td>
<td>THREAT DENIAL</td>
<td>A critical majority of governing politicians deny or systematically downplay existence of the threat</td>
<td>Government prevention of any state response to the threat</td>
</tr>
<tr>
<td>2</td>
<td>THREAT PARTIALLY ADMITTED</td>
<td>While individual governing politicians admit existence of the threat, the majority are reluctant to do so</td>
<td>Government permits low scale ad hoc initiatives by individual state experts, but does not proactively pursue any substantive policy</td>
</tr>
<tr>
<td>3</td>
<td>GOVERNMENT ADMITS THE THREAT</td>
<td>The majority of governing politicians admit existence of the threat and enable individual government bodies to begin pursuing initial responses under-the-radar</td>
<td>Individual government ministers pursue the development of policy responses; specific countermeasures are either in planning or have already been practically implemented; there is agreement on political direction within the government</td>
</tr>
<tr>
<td>4</td>
<td>GOVERNMENT PURSUES POLICY COUNTER-MEASURES</td>
<td>The governing establishment openly admits existence of the threat and pursues development of a national defence system to counter hostile foreign influence operations</td>
<td>The government takes a proactive approach to defence and explicitly tasks its security institutions with developing a comprehensive policy to counter the threat</td>
</tr>
<tr>
<td>5</td>
<td>ALL-GOVERNMENT POLICY COUNTER-MEASURES IN PLACE</td>
<td>There is unanimous agreement within the governing establishment about the existence and severity of the threat; policy development and implementation is coordinated among all levels of government</td>
<td>Complex and extensive defence initiatives have already been effectively implemented at different state levels without any significant political setbacks</td>
</tr>
</tbody>
</table>
## Government counter-activities

<table>
<thead>
<tr>
<th>RATING</th>
<th>DESCRIPTION</th>
<th>SYMPTOM(S)</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>COLLABORATION</td>
<td>The government abets the spread of Russian disinformation and hostile influence, either from conviction or for opportunistic reasons</td>
<td>The government adopts measures that limit state resilience against Russian influence and/or enable the fulfilment of the Kremlin's goals (e.g., limiting press freedom, collaborating with extremist parties, etc.)</td>
</tr>
<tr>
<td>1</td>
<td>IGNORANCE</td>
<td>The government is not concerned with disinformation and influence operations; it does not consider them a threat and takes no steps to counter them</td>
<td>The government makes no indication that it recognises Russian disinformation and other hostile foreign influence operations to be a threat</td>
</tr>
<tr>
<td>2</td>
<td>PARTIAL INITIATIVES IN SOME AREAS</td>
<td>The government adopts a few limited initiatives to counter disinformation and hostile foreign influence operations, though the effectiveness of these measures is questionable</td>
<td>One or a few departments of the state administration indicate concern about disinformation or other influence operations and take steps to counter them, though their focus is typically limited to a particular problem or domain (e.g., cyber-security, media literacy, etc.); a lack of resources or political support prevents these initiatives from being fully efficient. The state has a representative in at least one international body dedicated to countering disinformation operations, though it does not have a sophisticated or coordinated policy in place domestically.</td>
</tr>
<tr>
<td>3</td>
<td>SOPHISTICATED INITIATIVES IN SOME AREAS</td>
<td>The government adopts a few more ambitious initiatives to counter disinformation and hostile foreign influence operations; these are widely supported and show efficiency</td>
<td>One or a few departments of the state administration indicate concern about disinformation or other influence operations and take steps to counter them, though their focus is typically limited to a particular problem or domain (e.g., cyber-security, media literacy, etc.); sufficient resources and political support deliver positive results. The state has a representative in at least one international body dedicated to countering disinformation operations</td>
</tr>
</tbody>
</table>
### 4 Initiatives Launched in All Areas

The government adopts initiatives at various levels of state and in all relevant departments, though a lack of coordination and efficiency remains problematic.

All relevant departments of the state administration have adopted programs for strategic communication, comprehensively targeting the crucial impact areas of hostile interference and subversion; however, these programs are not fully efficient due resource shortage or poor coordination. The state actively supports (financially and/or logistically) at least one international body dedicated to countering disinformation operations.

### 5 Sophisticated Initiatives in All Areas

The government has adopted and refined initiatives across all levels of state and in all relevant departments, with highly positive results.

All relevant departments of the state administration have adopted sophisticated programs for strategic communication, comprehensively targeting the crucial impact areas of hostile interference and subversion; these programs are efficient, well-funded, and highly coordinated, delivering impressive results. The state actively supports (financially and/or logistically) at least one international body dedicated to countering disinformation operations.
### Counter-intelligence activities

<table>
<thead>
<tr>
<th>RATING</th>
<th>DESCRIPTION</th>
<th>SYMPTOM(S)</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>COLLABORATION</td>
<td>The intelligence services take steps limiting the country’s ability to counter hostile influence and subversion operations</td>
<td>Cases of unlawful investigation, attacks on domestic journalists, threats against the local population, and other similar incidents evince uninhibited Russian clandestine activity in the country</td>
</tr>
<tr>
<td>1</td>
<td>IGNORANCE</td>
<td>The intelligence services are wholly unconcerned with hostile influence and subversion operations</td>
<td>The intelligence services do not express concern about hostile influence and subversion; they do not name disinformation or other influence operations as national security threats in public reports or statements</td>
</tr>
<tr>
<td>2</td>
<td>ACKNOWLEDGEMENT OF THE THREAT</td>
<td>The intelligence services recognise that the threat exists but do not consider it a priority</td>
<td>The intelligence services briefly acknowledge the threat of hostile influence and subversion operations in their public reports and/or statements; they do not describe or analyse the issue in any meaningful way</td>
</tr>
<tr>
<td>3</td>
<td>UNDERSTANDING THE THREAT</td>
<td>The intelligence services recognise the threat of hostile foreign influence and have a reasonable grasp of how disinformation and subversion operations are conducted in the country</td>
<td>The intelligence services address in detail the threat of hostile influence and subversion operations in their public reports and/or statements, analysing the issue and identifying channels, perpetrators, and motives</td>
</tr>
<tr>
<td>4</td>
<td>OCCASIONAL INTERFERENCE</td>
<td>The intelligence services recognise and understand the threat; in one or a few cases, they have taken direct action to counter disinformation and/or hostile influence operations</td>
<td>Beyond a detailed description and analysis of hostile influence operations in public reports and/or statements, the intelligence services occasionally pursue specific security-related incidents (e.g., uncovering Russian spies, investigating disinformation project, etc.)</td>
</tr>
<tr>
<td>5</td>
<td>ACTIVE COUNTERING</td>
<td>The intelligence services recognise and comprehensively understand the threat; they act systematically to counter disinformation and/or hostile influence operations</td>
<td>The intelligence services consider hostile influence and subversion operations to be a national security priority and undertake systematic countermeasures, including regular investigations of Russian connections in the country, training programs for public officials and/or cyber defence strategies.</td>
</tr>
</tbody>
</table>
3. Summary and Conclusions

### Overall Ranking of the EU28

<table>
<thead>
<tr>
<th>GROUP “F” “Kremlin collaborators”</th>
<th>EU28</th>
<th>Political acknowledgement of the threat</th>
<th>Government counter-activities</th>
<th>Counter-intelligence activities&lt;sup&gt;5&lt;/sup&gt;</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyprus</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Greece</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GROUP “E” “The ignorant”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Austria</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Croatia</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Malta</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Portugal</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Slovakia</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Slovenia</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>GROUP “D” “The hesitant”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Italy</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>GROUP “C”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

<sup>5</sup> The authors understand that, by nature, counterintelligence work cannot be done in public visibility. However, we maintain that it is a matter of public duty for national intelligence and counterintelligence agencies to issue public warnings about urgent national security threats, for instance in their annual reports or open statements on leadership.
Overview of countermeasures by the EU28 to the Kremlin's subversion operations

<table>
<thead>
<tr>
<th>“The mildly concerned”</th>
<th>France</th>
<th>Spain</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP “B”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“The cognizant”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Romania</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP “A”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“The full-scale defenders”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lithuania</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>15</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
I. General Conclusions

1) The Kremlin’s use of aggressive hostile influence tactics like disinformation, together with its support for European extremists and radical leaders, has strongly alienated at least 12 countries out of the EU28 (Groups A & B)

2) We identify two outright “Kremlin collaborators” within the EU28 – Greece and Cyprus (Group F) – who have shown no meaningful resistance to Russia’s subversive activities

3) We identify a group of 8 EU states which largely continue to ignore or deny the existence of Russian disinformation and hostile influence operations - Hungary, Austria, Croatia, Luxembourg, Malta, Portugal, Slovakia, Slovenia (Group E)

4) Three states half-acknowledge existence of the threat (Group D); their hesitation is attributable either to geographic distance and historical neutrality (Ireland) or to the presence of pro-Kremlin forces in the political domain that suppress any efforts to place the threat on the agenda (Italy, Bulgaria)

5) Three states acknowledge the threat of disinformation and hostile influence operations but do not demonstrate adequate understanding of that threat; often, they are not geographically proximate to the Russian Federation (Group C):

   - Belgium recognises the threat of Russian disinformation abroad, particularly in the Eastern neighbourhood, but does not consider this to be a problem for its internal security, and therefore does not consider it a national priority. Its security institutions predominantly focus on the threat of Islamist terrorism.

   - Spain and France consider Islamist propaganda to be the more serious issue and mostly attribute disinformation campaigns to terrorist recruitment. In France, incoming President Macron seems poised to make a shift in this position, but it remains an open question given France’s historically sympathetic attitude to Russia.

6) We identify a large group of member states that not only acknowledge the existence of the threat but also seek to understand and analyse its particularities, as well as develop relevant and effective countermeasures (Groups A & B):

   - Eight of these states experienced a strategic shift or “awakening” after the annexation of Crimea and are now nearing the helm of the fight against Russian hostile influence operations. However, their practical strategies for countering Russian subversion are still under development, and some have weak spots that require redress (Denmark, the Netherlands, Romania, Finland, Czech Republic, Germany, the United Kingdom, Poland). There are noticeable differences in the depth and complexity of their national strategies (Group B).

   - Four states show the highest levels of activity, resilience, and readiness with respect to the threat, given their historical experiences with Russia: Sweden, Estonia, Latvia, Lithuania (Group A)
II. Trends and setbacks

7) For many of the EU28, a wide gap remains between mere acknowledgment of the threat and the development of concrete and viable counter-measures. The implementation of an effective strategy at the state level requires at least partial political consensus, civic support, and strong democratic institutions. Strong rhetoric and condemnation of Russian interference comes at virtually no political cost, but developing a pan-government approach necessitates the dedication of all major political parties and government bodies, as well as their active resistance against local obstacles and Kremlin-linked counter-pressures.

8) The Scandinavian EU countries (Denmark, Sweden, and Finland) have implemented strategies enhancing the overall resilience of their societies to any manner of contingencies, disinformation campaigns, or other subversive operations. Their programs are focused on prevention and crisis management, and their governments, intelligence agencies and non-governmental sectors are all engaged in these efforts.

9) The Baltic States (Latvia, Lithuania, and Estonia) stand at the forefront of the fight against hostile Russian influence, in large part due to their geographic proximity to Russia, historical experience, and sizeable Russian minorities. These countries have adopted strong countermeasures against Russian influence, often restricting Russian pseudo-media. They also actively engage their Russian-speaking minorities, to greater or lesser success. The Baltic experience with Kremlin-linked subversion tactics is the most developed within the EU28 and serves for major lessons learnt.

10) Apart from these two regions, there is a significant lack of cooperation between governments (G-G) and civil society (G-NGO) in the other EU28. In many countries, the approaches of the state administration and non-governmental sector differ significantly.

• In some cases, like Slovakia, civil society leads the fight against Russian influence, but fails to persuade the government of the importance of this task and the danger of the threat due to internal political limitations (e.g., government ignorance, a lack of political will, etc.).

• In other countries, like Hungary, small pockets of civil society strive to expose the threat but yield little to any influence on government policy due to internal political struggles.

• In countries like France and Germany, civil society is largely inactive on this front; there is no coordinated or robust civic response at the national level. Public knowledge is typically limited to a handful of individuals at think-tanks, universities, and select media outlets.

11) There is a strong negative correlation between the degree of Russian subversive influence on the one hand and the state of media literacy and press freedom on the other. In countries with deteriorating press freedom, for instance due to measures that limit serious investigative journalism, submission to Russian influence has increased in recent months (e.g., Hungary and Croatia). Meanwhile, countries with a strong tradition of independent journalism, along with newer efforts to boost
media literacy, boast greater resilience against Russian malign influence and disinformation campaigns (e.g., the Scandinavian countries and the UK).

12) In Western Europe, it is notable that traditionally powerful European states only begin to display interest in countering Russian disinformation during, immediately before, or even after major domestic elections, when they have experienced or anticipate Russian interference:

- **France** widely ignored the threat until its recent presidential elections. Newly elected President Emmanuel Macron experienced Russian meddling during his campaign and his official foreign policy adviser recently stated, "We will have a doctrine of retaliation when it comes to Russian cyber-attacks or any other kind of attacks."\(^6\)

- The government of the **Netherlands** barely reacted when Russian disinformation circulated during the 2016 referendum on the Association Agreement with Ukraine. During the 2017 parliamentary elections, it decided not to use electronic voting in order to avoid possible Russian meddling. The Dutch intelligence agency AIVD has since concluded that Russia tried to influence the 2017 elections by spreading fake news.\(^7\)

- The **United Kingdom** has been supporting many strategic-communications projects in the Eastern Partnership region, but the debate on Kremlin subversion in the UK was very limited before the Brexit referendum in 2016. The UK’s close ties to Kremlin-linked money has also not featured on the agenda until recently. The current British government has announced major programs to counter Russian influence in Central and Eastern Europe. For example, Foreign Secretary Boris Johnson has decided to launch the Empowerment Fund, which aims to countering Russian influence in post-Soviet countries by boosting their defences against propaganda and cyber warfare.\(^8\)

- In **Italy**, initial concerns about disinformation and hostile influence operations emerged during the constitutional referendum in December 2016, when the rising anti-establishment Five Star Movement proliferated disinformation and pro-Kremlin propaganda.\(^9\) Nonetheless, the government is still not taking any action to counter these efforts. Italy is also a Kremlin ally when it comes to halting new EU sanctions related to Kremlin-sponsored atrocities in Ukraine and Syria.\(^10\)

---


13) Recognition of these information threats typically results in certain efforts to manage the crisis. In the fight against fake news, governments often seek the help of corporations like Google and Facebook in order to protect their elections, but these companies have very limited assistance options. Eventually, most measures undertaken at the last minute turn out to be “too little, too late” and lack necessary coordination. Importantly, policies against hostile foreign influence must be designed and implemented long in advance.

14) Germany's position could be the game-changer: with federal elections in September 2017, Germany is currently preoccupied with developing resistance against Russian meddling. Over the last few months, Germany has begun taking the threat posed by Russia much more seriously than ever before. Germany actively tries to boost its cyber defence and also promotes cyber security internationally, even creating a new Bundeswehr command. If the next German government tackles this threat with true German precision and intensity, it will spill over to EU policy and prompt substantive democratic counter-pressure. Until now, the concerns of mostly smaller EU members on the Eastern flank have been insufficient to instigate a shift in EU policy.

---

III. Sectoral trends

Political acknowledgment

1) The number of states with very low levels of acknowledgment is high, but the reasons for this differ. Some commonalities exist, but few apply in all cases. The most notable of these are as follows:

- Some governments look to Russia for policy inspiration, financial injections, or political support, either in the international or domestic arena (e.g., Cyprus seeks support for the island’s integrity, while the Hungarian government derives inspiration from some of the Kremlin’s authoritarian policies)
- Strong national presence of relevant pro-Kremlin political parties (e.g., Syriza in Greece, FPÖ in Austria)
- Decreasing freedom of the press, bad conditions for journalists, state control over a large portion of the media (e.g., Hungary, Croatia)
- Strategic documents focus on economic and energy issues where the country is dependent on Russia (e.g., Croatia)

2) At the other end of the spectrum, countries with the highest levels of political acknowledgment (i.e., Group A) have very high standards and strong traditions regarding press freedom. Most of these countries have been worried about the Kremlin’s subversive influence for a long time and have been preparing for it.

3) Some states that are currently aware and active were somewhat caught off guard by the surge in hostile Russian activity. They did not anticipate the expansion of Russia’s disinformation campaign and other subversion tactics, and their reaction was triggered by a bad experience related to false reports, cyberattacks or electoral interference (e.g., Germany, the Netherlands, the Czech Republic). Now, these are “awakening” to the threat.

Government counter-measures

4) Many countries are striving to keep up with new technologies and allocate substantial resources to their cyber capabilities. They are not only upgrading their technology, but also establishing coordination units and investing manpower.

- The Bundeswehr plans to employ 13,500 German soldiers and civilian contractors to manage cyber defence under the National Cyber Security Council.\(^{12}\)
- The National Computer Security Incident Response Team in Latvia cooperates with more than 600 IT specialists from government institutions and local authorities. Latvia also has a Cyber

\(^{12}\) Werkhäuser (2017).
Defence Unit consisting of IT specialists and students from the public and private sector, trained to help the national armed forces in case of need. 

- Even states with little to no political acknowledgment of malign Russian influence (e.g., France, Croatia, Malta) are enhancing their cyber capabilities to prevent interference in their government communication.

5) There is a noticeable effort to cooperate with or regulate social networking sites and internet browsers.

- Germany proposed a bill according to which social networks have to pay fines of up to 50 million euros if they fail to give users the option to complain about hate speech and fake news, or refuse to remove illegal content.

- Facebook and Google cooperated with French news organisations before the presidential elections in order to launch new fact-checking tools.

6) Best results are often attained by those countries that are cooperate effectively with civil society.

- The Baltic region represents the best example of this cooperation, with governments actively engaged with reservists, volunteers, and non-profit organisations.

- The United Kingdom established the 77th Brigade, combining the Regular Army and Army Reserves, cooperating on tackling the challenges of modern warfare.

- In the Czech Republic, the government actively engaged the non-governmental sector while conducting the National Security Audit, an assessment of vulnerabilities against the influence of foreign powers. There are various activities linking NGO experts with the national security establishment, even though it is still under revision.

- Many other states accept volunteers when dealing with the issue of cyberwarfare, for example in a ‘reservist’ model called ‘cyberleague’.

---


15 See <http://www.army.mod.uk/structure/39492.aspx>

15) **13 EU countries are highly concerned with the Russian disinformation threat**, and are therefore participating in at least one of three allied projects (EEAS East STRATCOM, NATO STRATCOM COE, Finnish COE on Countering Hybrid Threats).

<table>
<thead>
<tr>
<th>EU28</th>
<th>EEAS East STRATCOM Team (Brussels)</th>
<th>NATO STRATCOM COE (Latvia)</th>
<th>Finnish COE on Countering Hybrid Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonia</td>
<td>Has sent seconded-national expert</td>
<td>Sponsoring nation</td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>Has sent seconded-national expert</td>
<td>Founding and hosting nation</td>
<td>Participating</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Has sent seconded-national expert</td>
<td>Sponsoring nation</td>
<td>Participating</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Has sent seconded-national expert</td>
<td>Sponsoring nation</td>
<td>Participating</td>
</tr>
<tr>
<td>Sweden</td>
<td>Has sent seconded-national expert</td>
<td>Partner country</td>
<td>Participating</td>
</tr>
<tr>
<td>Finland</td>
<td></td>
<td>Partner country</td>
<td>Host of the COE</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Has sent seconded-national expert</td>
<td>Had sent national expert</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td></td>
<td>Sponsoring nation</td>
<td>Participating</td>
</tr>
<tr>
<td>Poland</td>
<td></td>
<td>Sponsoring nation</td>
<td>Participating</td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
<td>Sponsoring nation</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td></td>
<td>Joining nation</td>
<td>Participating</td>
</tr>
<tr>
<td>Italy</td>
<td></td>
<td>Sponsoring nation</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>Has sent seconded-national expert</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Most of “the cognizant” countries (Group B) and “the full-scale defenders” (Group A) are actively participating in these institutions.

- The Czech Republic and Estonia have not yet engaged with the Finnish COE.
- Finland, Germany, and Poland do not have experts in the EEAS unit.
- Denmark and the Netherlands each only participate in one of the institutions and Romania has not engaged with any of them so far.

Counterintelligence activities (publicly known)

16) From 2015-2017, many European intelligence agencies issued very vocal warnings about Russian behaviour, mainly with respect to hostile interference in their domestic affairs (e.g., France, Germany, the Netherlands, the United Kingdom, the Czech Republic). Overall, the agencies indicate the Kremlin’s behaviour is on a downwards trajectory – domestically in Russia, in the Eastern neighbourhood, and also against EU states. Several European intelligence chiefs (namely from British MI5,17 German BFV,18 and BND19) have made public statements warning about these threats, which is often unusual in the local context, where public on-record engagement is a rarity.

17) Overall, cybersecurity has become a major concern across Europe, but rarely with respect to Russia as a specific actor. However, many countries are attempting to enhance their cybersecurity capabilities.

18) A high concentration of clandestine Russian operations is notable even in countries with limited to no political acknowledgment of Russian subversive influence.

- There have been several cases of Russian spy activity20 in Austria, but they were not publicly promoted so as not spoil relations with the Kremlin, especially regarding energy ties.
- Bulgaria is also a key target for Russian intelligence operations,21 which is not reflected in the activities of the Bulgarian intelligence services.

19) However, in some countries, the intelligence services have started to actively counter these clandestine operations.

---


20 Ibid.

The Czech Republic has expelled several Russian spies under diplomatic cover.22

Several Russian diplomats have also been expelled from Poland, including former Russian military attaché Eduard Shishmakov who is currently accused of participating in the plot in Montenegro.23

The Estonian Secret Police (KAPO) identifies and apprehends Russian spies regularly. For example, two dual citizens of Russia and Estonia were apprehended and sentenced to jail for spying in 2016.24

In 2014, Lithuania also expelled three Russian intelligence officers operating under diplomatic cover and several diplomats had to leave office before their accreditation expired.25

Non-governmental sector

Even in countries where the government is in denial about Russia or where the state is trying to prevent the topic of Russian hostile influence from reaching the public agenda, civil society is often still fighting against the odds.

In Cyprus, the media breached a long-time taboo and recently began speculating about Russia’s true motivations and ambitions.26

In Hungary, where there is a significant governmental pushback against civil society, Political Capital is fighting back by analysing and countering disinformation operations within the country.

Civil society in Slovakia is extraordinarily active, with numerous successful initiatives like Konspiratori.sk and the Forum Against Propaganda.

In several countries, the organisations dedicated to myth-busting and countering disinformation are also trying to tackle the threats of extremism and far-right radicalism (e.g., Austria, Slovakia).

Even though enhancing media literacy is not the main priority of the EU28, small initiatives and projects exist in almost every state. Only a few countries (e.g., the Scandinavian states) have effective long-term strategies.


I. On country practices:

- **Recommendation 1:** Follow and learn from the experience of the **Scandinavian countries** in media literacy and overall resilience growth.

- **Recommendation 2:** Follow and learn from the experience of the **Baltic countries with Russian interference methods** and crisis management scenarios.

- **Recommendation 3:** Follow and learn from the experience of **Finland in strategic communications coordination** between governmental ministries and agencies.

- **Recommendation 4:** Follow and learn from the experience of the **Czech Republic (CTHT) and Sweden (MSB)** in dedicating multi-level expertise teams to countering hostile foreign influence and electoral protection.

- **Recommendation 5:** Follow and learn from the **Czech experience with conducting an in-depth National Security Audit**\(^{27}\) to identify weak spots in national security infrastructure.\(^{28}\)

- **Recommendation 6:** Follow and learn from the experience of the **Baltic intelligence agencies in their methods of raising public awareness** by publicising some of their cases. Only 6 out of the EU28 have done so.

On EU policy:

- **Recommendation 7:** **Use and support the EEAS East STRATCOM Team** for its weekly trend analysis of disinformation campaigns (“Disinformation Review”). Concerned EU states should send their experts to join the team.

- **Recommendation 8:** At least **13 out of the EU28 are highly concerned** about the Russian threat. Despite this number, **almost nothing has been accomplished policy-wise at the EU level.** The EU HRVP Federica Mogherini continues to ignore and downplay the threat.\(^{29}\) As a consequence, the specialised EEAS East STRATCOM Team, founded under Mogherini’s jurisdiction, comprises only a handful of EU state experts, while the EEAS does almost nothing, despite repetitive calls for action from other member states and the European Parliament. In light

\(^{27}\) The National Security Audit was conducted by the Czech Republic in 2016. One chapter is exclusively devoted to the question of hostile foreign influence. It includes a SWOT analysis summarising the strengths and weaknesses of Czech defence against the threat, and presents specific recommendations for enhancing resilience. It is a critical step for the development and implementation of a sophisticated and effective strategy.


\(^{29}\) See <http://www.europeanvalues.net/mogherini/>
of this situation, the 13 concerned countries should form a coalition to demand real policy measures to be adopted at the EU level – precisely what the EU is for. So far, very little coalition building has been pursued.

II. On policy development:

- **Recommendation 9**: Start sharing experience on hostile interference in national elections and on what can be done to mitigate the threat. Use the framework guide on how to make elections part of the national critical infrastructure.\(^3^0\)

- **Recommendation 10**: Protecting elections is not enough. A long-term strategy for mitigating hostile foreign influence must be developed and tailored for the local environment. See this 50-measure strategy.\(^3^1\)

III. Towards the game-changer:

- **Recommendation 11**: Concerned EU countries should assist Germany in adopting a politically assertive role on this front. If Berlin takes this threat seriously, it will be the game changer for EU-Russia relations and Russian will to interfere aggressively in the EU's domestic affairs. Advocacy and lessons-learnt visits should be made to Berlin by the most concerned governments.

IV. Best NGO practices:

- **Recommendation 12**: Each country must conduct in-depth research and investigations of pro-Kremlin outlets, their structures, modes of collaboration, content-related trends, and financial ties. Good examples include the Czech Republic, Slovakia, Hungary, Latvia, Lithuania, Estonia, Finland.

- **Recommendation 13**: In-depth investigations of the Kremlin’s ties to national actors must be pursued. Good examples include Die Zeit (Germany), Respekt (Czech Republic), Re:Baltica (Latvia).

- **Recommendation 14**: Government-NGO partnerships must be built to share experience, provide voluntary briefings and trainings, or share knowledge and capabilities. A good example is Propastop.org, an anti-propaganda blog operated by volunteers, mostly members of the


Estonian Voluntary Defence League (Kaitselit),\(^{32}\) which itself works under the Ministry of Defence.\(^{33}\)

- **Recommendation 15:** National audits of electoral rules and practices must be completed. A good example is the LSE (UK).\(^{34}\)

- **Recommendation 16:** Detailed sociological analyses of specific national vulnerabilities must be conducted. Good examples include GLOBSEC Trends Report.\(^{35}\) Vulnerability study by Latvian Defence Forces Academy.\(^{36}\)

- **Recommendation 17:** Projects looking at who and why is advertising on disinformation outlets are much needed. Good examples include the Slovak project Konspiratori.sk, which made 1400 Slovak companies take down their advertisements from disinformation outlets.

- **Recommendation 18:** Boost solid policy assessment and development needs based on shared knowledge and experience from the concerned countries, which can be transplanted and implemented in other states. Very limited work has so far been done on this front. Good examples include CEPA: Winning Information War,\(^{37}\) Full-Scale Democratic Response to Hostile Disinformation: A 50-measure policy toolbox.\(^{38}\)

---


\(^{33}\) See <https://www.propastop.org/eng/>.


\(^{38}\) Janda (2016).
5. Recommendations for Donors

I. Outlook of EU28 with Group Categorisations

<table>
<thead>
<tr>
<th>Brief description</th>
<th>GROUPS D, E &amp; F</th>
<th>GROUPS B &amp; C</th>
<th>GROUP A</th>
</tr>
</thead>
<tbody>
<tr>
<td>States that are more or less indifferent to this threat</td>
<td>States that have begun to address this threat through various policy initiatives, but lack solid consensus within the political establishment</td>
<td>States with comprehensive understanding of the threat at all levels of government</td>
<td></td>
</tr>
<tr>
<td>Total ranking</td>
<td>0 – 5</td>
<td>6 – 12</td>
<td>12 – 15</td>
</tr>
</tbody>
</table>

What is needed

| PRIORITY STEP 1: Strong support for investigative journalism and fact-checking and myth-busting initiatives | PRIORITY STEP 4: Support for non-governmental advocacy initiatives to push for a clear political consensus on this issue | PRIORITY STEP 7: Support for the development of specific policy proposals and assessments of existing policy initiatives from other countries in order to update national strategies |
| STEP 2: Support for data collection and specialised polling in order to document the severity of the threat | STEP 5: Support for the development of specific policy proposals and assessments of existing policy initiatives from other countries in order to establish national strategies | STEP 8: Support for data collection and specialised polling in order to tailor policy measures to local contexts |
| STEP 3: Support for non-governmental advocacy initiatives aiming to place this issue on the public agenda | STEP 6: Support for data collection and specialised polling to tailor policy measures to local contexts | STEP 9: Support for activities focused on sharing national experience and lessons learnt with states in the previous two categories |

List of countries

| Cyprus, Greece, Hungary, Austria, Croatia, Luxembourg, Malta, Portugal, Slovakia, Slovenia, Ireland, Italy, Bulgaria | Belgium, France, Spain, Denmark, Netherlands, Romania, Finland, Czech Republic, Germany, United Kingdom, Poland | Sweden, Estonia, Latvia, Lithuania |
II. Specification of Suggested Steps

<table>
<thead>
<tr>
<th>STEP</th>
<th>STEP OBJECTIVE(S)</th>
<th>EXAMPLE(S)</th>
<th>PRACTICAL SUGGESTION FOR DONORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY STEP 1: Strong support for investigative journalism and fact-checking and myth-busting initiatives</td>
<td>Boost national and international investigative journalists and projects working on exposés of disinformation outlets. Boost national and international fact-checking organisations investigating the content of disinformation stories.</td>
<td>Re:Baltica New Eastern Europe NATO STRACOM COE Case study on online trolling Investigative work of Finnish journalist Jessikka Aro Stopfake.org Polygraph.info</td>
<td>The UK, Swedish, and Dutch governments might be interested in this move. Projects from countries in Groups B &amp; C should be prioritised. A funding scheme could be set up for investigative journalism and fact-checking that would: <strong>SUGGESTION 1:</strong> Provide short- and mid-term grants to individual journalists and investigative groups on specific topics or periods of time (e.g., electoral campaigns in targeted countries) <strong>SUGGESTION 2:</strong> Provide long-term grants for in-house fact-checkers in major publishing houses in selected vulnerable countries <strong>SUGGESTION 3:</strong> Provide long-term grants to fact-checking organisations</td>
</tr>
</tbody>
</table>
### Overview of countermeasures by the EU28 to the Kremlin's subversion operations

**Priority Steps 2, 6 & 8:** Support for data collection and specialised polling in order to document the severity of the threat and in order to tailor policy measures to local contexts

- Support projects that will deliver credible data on the structure and intensity of disinformation campaigns
- Support research into the societal penetration of pro-Kremlin narratives

**GLOBSEC Trends Report**
- Vulnerability study by Latvian Defence Forces Academy
- Comprehensive outlook of Czech disinformation outlets done by European Values Think-Tank

**Suggestion 4:** Contract a selected group of reliable think-tank experts who have experience with empirical research in this field and have them prepare a methodological handbook for practical research, including definitions, criteria, and methods.

**Suggestion 5:** Based on this handbook, create a grant scheme for support of empirical research projects in selected countries.

**Suggestion 6:** Directly subcontract the development of vulnerability studies (based on model Vulnerability study by Latvian Defence Forces Academy) in countries in Groups B & C.

**Suggestion 7:** Set up an annual specialised polling program to measure the success of Kremlin narratives and messaging in selected countries.

**Priority Steps 3 & 4:** Support for non-governmental advocacy initiatives aiming to place this issue on the public agenda and push for a clear political consensus on this issue

- Support activities that can push this issue onto the public and political agenda by demonstrating the urgency and complexity of the threat
- Enhance activity where expert knowledge can be used for advocating towards selected policy-makers on the international level

**Suggestion 8:** Set up a grant scheme for advocacy-oriented projects in targeted countries (mainly in Groups B & C).

**Suggestion 9:** Find a regular platform for an in-depth exchange of best practices among leading organisations in the advocacy field. For example, specialised restricted sessions can be held at big league conferences like GLOBSEC, MSC, and WSF, or at specialised events like STRATCOM SUMMIT.

**Suggestion 10:** Contract a small specialised team of reliable think-tank experts who will constantly brief key European and U.S. policy-makers at the parliamentary and executive level. Enhance Tour de Capitals advocacy initiative which IRI Beacon Project is already pursuing.

---

39 Expert recommendations: Ben Nimmo (Legatum Institute), Stefan Meister (DGAP), Yevhen Fedchenko (StopFake.org), Alina Polyakova (Atlantic Council), Anton Shekhovtsov (Institute for Human Sciences), Peter Kreko (Political Capital Institute), Roland Freudenstein (WMCES), Keir Gilles (Chatham House), Elliot Higgins (Bellingcat), Kai Olaf Lang (SWP), Jakub Kalenský (EEAS East STRATCOM), Aivar Jaeski (NATO STRATCOM COE), Jakub Janda (European Values Think-Tank)
### PRIORITY STEPS 5 & 7: Support for the development of specific policy proposals and assessments of existing policy initiatives from other countries in order to establish or update national strategies

<table>
<thead>
<tr>
<th>STEPS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 &amp; 7</td>
<td>Boost solid policy assessment and development based on shared knowledge and experience from the concerned countries, which can be transplanted and implemented in other states.</td>
</tr>
<tr>
<td></td>
<td>Very limited work has so far been done in this field. At least two complex policy papers stand out:</td>
</tr>
<tr>
<td></td>
<td>CEPA: Winning Information War</td>
</tr>
<tr>
<td></td>
<td>Full-Scale Democratic Response to Hostile Disinformation: A 50-measure policy toolbox</td>
</tr>
</tbody>
</table>

### SUGGESTION 11:

Contract a NATO and PfP-wide comprehensive overview of policy initiatives in this field to a group of 12 reliable think-tank experts (suggestions above). Fund this group to work for 12 months with several study trips in order to present public and non-public assessments of implemented policies, together with suggestions about what steps to take and avoid in the future.

### PRIORITY STEP 9:

Support for activities focused on sharing national experience and lessons learnt with states in the previous two categories

<table>
<thead>
<tr>
<th>STEPS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Make maximum use of the knowledge and experience of frontline countries for lesson-sharing with other concerned states.</td>
</tr>
<tr>
<td></td>
<td>Training courses conducted by NATO STRATCOM COE, even though those are targeted at state officials only.</td>
</tr>
<tr>
<td></td>
<td>NATO Science for Peace Seminars and Workshops, even though those are targeted mainly at PfP countries.</td>
</tr>
</tbody>
</table>

### SUGGESTION 12:

Identify 10-15 lecturers from countries in Groups A & B and organise (or outsource organising) monthly workshops in concerned countries.

### SUGGESTION 13:

Subcontract the development of 'lessons learnt' handbooks from countries in Group A.

---

40 Based on experience of ongoing activities of this kind in European cities, four reasonable training modules can be identified: 1) Basic course for general security-related state officials: important information about disinformation operations; 2) Advanced workshop for STRATCOM-related state officials: discussion of implemented practices and policies; 3) Basic course for journalists: important information about disinformation operations and best practices for investigative journalism; 4) Advanced workshop for activists and experts: discussion of best practices and methods of researching and countering disinformation.
Diagram: Domains of support

**States that are more or less indifferent to this threat**
(Italy, France, Hungary, Slovakia)

- Investigative journalism and fact-checking and myth-busting activities
- Data collection and specialised polling to document the severity of the threat
- Non-governmental advocacy initiatives to place the issue on the public agenda

**States that have begun to address this threat through various policy initiatives, but lack solid policy consensus within the political establishment**
(Netherlands, United Kingdom, Germany, Czech Republic)

- Non-governmental advocacy initiatives to push for a clear political consensus on the issue
- Development of specific policy proposals and assessments of existing initiatives from other countries in order to establish national strategies
- Data collection and specialised polling in order to tailor policy measures to local contexts

**States with comprehensive understanding of the threat at all areas of government**
(Estonia, Latvia, Lithuania, Finland, Sweden)

- Development of specific policy proposals and assessments of existing initiatives from other countries in order to update national strategies
- Data collection and specialised polling in order to tailor policy measures to local contexts
- Activities focused on sharing national experience and lessons learnt with states in the two previous categories

Activities focused on sharing national experience and lessons learnt with states in the two previous categories
6. Individual profiles of the EU28

I. Austria

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Austria’s bilateral relationship with Russia is between ‘friendly pragmatist’ and ‘strategic partner’
- Austria’s most successful far-right political party, the FPÖ, has exceptionally close ties to Russia
- Vienna is a major target for Russian intelligence activities as well as interference in domestic politics

Relations with the Russian Federation

Description: Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of a threat.\(^41\)

Austria is a non-NATO EU member state with a long tradition of neutrality throughout the Cold War. Its relations with Russia have not suffered significantly due to the conflict in Ukraine. In particular, energy interests continue to shape the two countries’ relationship and remain a cornerstone of Austrian diplomacy with Russia. For this reason, Austria is sceptical about the EU sanctions regime against Russia and is less concerned than many other EU member states about the threat Russia poses to European stability. In sum, Austria’s “behaviour reflects the habits of a small, isolated, and neutral country trying to get along in between rival political blocs.”\(^42\) However, a large Chechen diaspora in Austria (20,000-25,000), the product of Russian policy in the Northern Caucasus, is perceived to be a potential national security risk. Overall public support for Russia remains low: according to the latest Eurobarometer, only 28% of Austrians had a positive view of Russia.

---


Political acknowledgement of the threat

The threat of disinformation and/or other hostile influence operations stemming from Russia does not feature on the Austrian political agenda. On the contrary, following its tradition of neutrality, and in order to protect its national energy and trade interests, Austria endeavours to walk a conciliatory and diplomatic line between Russia on the one hand and its commitment to Europe on the other. This attitude is exemplified by the Austrian Foreign Ministry’s long-term priorities for European, foreign, and integration policy: “As demonstrated by the Ukraine-Russia conflict, the EU and its members need a clear neighbourhood policy […] which provides our Eastern neighbours with the opportunity to participate in common solutions and saves them from having to choose between Russia or the EU. […] Sustainable safety and security in Europe can only be achieved in cooperation with Russia and not by working against Russia – and the same holds true vice versa: Russia too, can only ensure long-term safety and security by working with and not against Europe.”

There is no mention of security threats associated with disinformation or hostile influence activities in particular.

Government activities against Russian influence & disinformation

The Austrian government is undertaking no discernible action to counteract Russian disinformation or other means of subversive influence. Indeed, Austria continues to see Russia (along with the U.S.) as a strategic partner in both national and European security. This failure to acknowledge Russian subversion is noteworthy given that Austrian politics have proven vulnerable to Russian meddling. The right-wing Freedom Party (FPÖ), which won a substantial 47% of the vote in the 2016 presidential run-off, is the most notable proxy agent of Russian influence, frequently hosting Russian politicians and nationalist intellectuals. Following its strong electoral performance in 2016, the FPÖ signed a cooperation contract with the United Russia Party – an act that was widely criticised by other Austrian elites. However, mainstream Austrian parties have also at times proven receptive to a pro-Russian agenda (e.g., the centre-left SPÖ and centre-right ÖVP). In sum, a “dovish’ attitude” towards Russia dominates across the Austrian political spectrum, with vested interests eager to return to “business as normal” with Russia.

46 Gressel (2015); Weidinger et al. (2017).
The approach of intelligence agencies to Russian interference

Vienna serves as the base of operations for a large number of Russian security service agents (estimates vary from several dozen\(^{48}\) to several thousand\(^{49}\)). “From time to time, the Austrian media report […] on Russian secret service activities in Austria. The Austrian side is usually overly keen to restore everything to normality as soon as possible: From its point of view, spy scandals must not spoil its ‘good and cordial relations’ with Moscow – and, especially, the natural gas supply”.\(^{50}\) Gert René Polli, the former chief of Austria’s counter-terrorism agency, told The Telegraph, “Vienna is a stock exchange of information. We have the most liberal laws governing spying activity in the world.”\(^{51}\) Austria’s annual constitution protection reports mention Russian secret service activities; the latest notable incident occurred in 2011, when a Russian secret agent couple with Austrian identification documents was arrested in Germany. The ensuing investigation “significantly substantiated the suspicion of illegal activity.”\(^{52}\)

Nonetheless, the 2015 counterintelligence report (Verfassungsschutzbericht) does not identify Russia as a threat to Austrian security, but rather names Russia as an important partner in fighting Islamist terrorism.\(^{53}\)

Activities of the non-governmental sector

There are no significant non-governmental initiatives in Austria seeking to mitigate the threat of Russian disinformation and attempted hostile influence. However, the Austrian media (e.g., Der Standard, Die Presse) frequently reports on cases of Russian information manipulation, though primarily about incidents in other countries. In addition, several civic media watchdog groups have emerged in recent years that are concerned with fact-checking, debunking false stories, and media literacy. These include: FPÖ Watch, mimikama.at, hoaxmap.org, digitalks.at, werdedigital.at, saferinternet.at, oiat.at.

At the same time, there is also an extensive and growing network of so-called ‘NGOs’ and think tanks agitating on behalf of Russia. These include the Suworow Institute in Vienna, which has ties to the FPÖ, and the Center for Continental Cooperation, which appears to benefit from Russian government financing. In addition, Russian influence is palpable at the level of far-right civic youth movements. In particular, the popular Identitarian Movement, an extremist group founded in 2012 opposing U.S.

---


\(^{50}\) Malek & Luif (2013).

\(^{51}\) McElroy (2014).


\(^{53}\) Vergfassungsschutzbericht (2015).
‘hegemony’ over Europe, derives much of its ideological inspiration from the Russian nationalist intellectual Aleksander Dugin.\textsuperscript{54}

Since the onset of the conflict in Ukraine, a new Austrian fringe media has also emerged, united in its pro-Russian orientation and admiration of Vladimir Putin.\textsuperscript{55} Three outlets are particularly prominent: Neopresse,\textsuperscript{56} published since 2012; Contra Magazin,\textsuperscript{57} founded in 2013 by right-wing activists; and Info Direkt,\textsuperscript{58} a medium published since 2015, with its server located in Moscow.

\textsuperscript{54} Weidinger et al. (2017).
\textsuperscript{55} Krekó et al. (2016).
\textsuperscript{56} See <http://www.neopresse.com>
\textsuperscript{57} See <http://www.contra-magazin.com>
\textsuperscript{58} See <http://www.info-direkt.eu>
II. Belgium

Summary

- Though Belgium has historically maintained a pragmatic bilateral relationship with Russia, the Kremlin's destabilisation efforts in Ukraine have elicited a strongly critical response
- However, Russian disinformation and/or other hostile influence operations are not a security priority for Belgium
- Brussels is the target of extensive Russian intelligence activities, which are a major concern of the Belgian security services

Relations with the Russian Federation

Description: Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of a threat.59

Belgium is an integral EU and NATO member state, hosting both EU and NATO institutional centres. Though historically a pragmatist in its relations with Russia, Belgium is growing increasingly aware of the threat that Russia poses to the European Union. The conflict in Ukraine has made Belgium more eager to support Kyiv in the EU context and back pan-European measures to counter Russian aggression. However, the country’s geographic distance from the Russian border, combined with internal political difficulties as well as the threat of Islamist terrorism, mean that Belgium does not perceive Russia as a primary security threat. Nonetheless, Belgium does not deny that Russia poses a serious security challenge to Europe, and maintains a particular concern with Russian intelligence activities within its borders. According to the latest Eurobarometer, 26% of Belgians had a positive view of Russia.

Political acknowledgement of the threat

Disinformation and other hostile influence operations stemming from Russia are not a political priority for Belgium, given its geographic distance from Russia and other pressing domestic security issues. Since the start of the crisis in Ukraine, Belgium has noticeably cooled its attitude towards Russia;

previously, Belgium maintained a friendly pragmatist approach towards the Kremlin, based primarily on its interests in trade and energy relations. While Belgium is not pursuing any explicit national strategies to combat Russian disinformation and hostile influence, the country acknowledges the threat and supports a unified EU/NATO response to growing Russian aggression.

**Government activities against Russian influence & disinformation**

With respect to the relationship with Russia, Belgium chiefly advocates multilateral action through the EU/NATO and other European institutions, including the OSCE and Council of Europe. On EU-Russia policy, Belgium consults with the Baltic states, the Visegrad countries, Romania, and Bulgaria, despite strong divergences vis-à-vis historic experience with Russia as well as national interests and preferences.

In its policy focus, Belgium is less concerned with the potential domestic impact of disinformation than it is with the Kremlin’s destabilisation efforts in Ukraine. The 2016 Strategic Vision for Defence acknowledges Russia’s hybrid warfare and destabilisation efforts in Eastern Europe, and commits Belgium as a NATO member to security efforts in the region.⁶⁰ Foreign Minister Didier Reynders declared the Ukraine crisis to be a priority of the Belgian Presidency of the Council of Europe 2014-2015, and visited Ukraine with colleagues from the other Benelux countries, reaffirming Belgium’s support for Ukraine’s territorial integrity. In a 2015 speech on the priorities of Belgian diplomacy, Foreign Minister Reynders decisively called on Russia to “respect the territorial integrity of Ukraine”, but simultaneously stated that “Russia remains an important partner and we think it is important to keep the dialogue open”.⁶¹ The threat of Russian disinformation and hostile influence in Europe proper remains a secondary concern.

**The approach of intelligence agencies to Russian interference**

Belgium hosts international institutions such as the EU and NATO, which Russia considers an important element of the bilateral relationship that separates Belgium from other small EU member states.⁶² Given this unique position, Brussels is also the target of Russian intelligence activities. The Belgian state security service regularly reports on Russian “interest” in Euro-Atlantic defence policy, EU political decisions, EU economic policy, and the Russian-speaking community in Belgium.⁶³ Spy scandals are also not a rare occurrence.⁶⁴

---


According to the 2011 Annual Report of the Belgian State Security Service (VSSE), clandestine activities of intelligence officers under diplomatic cover and journalistic cover [...] remain at a high level. Investigations […] led to the identification of several Russian intelligence officers who, for many years, operated in Belgium and/or abroad using falsified Belgian or other non-Russian identities, sometimes dating back to the 1960s. Several Belgian nationals were recruited and manipulated by the Russian […] intelligence services. Political developments (electoral fraud, protests) in Russia and the region are closely monitored by the VSSE, as they may have consequences for the Russian and Russian-speaking diaspora in Belgium, the legitimacy of the future president, and bilateral relations.65

Activities of the non-governmental sector

Think tanks are the primary non-governmental actors in Belgium involved in research and counter-strategy vis-à-vis Russian disinformation and hostile influence operations. These include the Egmont Royal Institute for International Relations, Royal Higher Institute for Defense, and Ceci n’est pas une crise.

In the last three years, several NGOs (e.g., Bridge EU-Ukraine, Promote Ukraine) have emerged seeking to raise awareness about Russia’s destabilisation efforts in Ukraine, as well as to increase public support for Ukraine’s future as a “progressive, European, and democratic society”.66 These NGOs collaborate with Belgian universities and think tanks to organise educational events about the situation in Ukraine and Russian influence operations.67

As of May 2017, concerns about media literacy have not received much attention in Belgium. An exception is Média Animation ASBL, a prominent media education resource founded in 1972 and sponsored by the Belgian Ministries of Education and Culture. Média Animation targets media literacy in schools as well as amongst politicians and other decision makers, though disinformation is not its main focus.68

III. Bulgaria

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Bulgaria has historically close relations with Russia due to shared cultural ties as well as energy dependence
- Bulgaria has considerable internal political divisions with respect to Russia
- Despite facing pressure from pro-Russian groups, the current government is pursuing a tougher line on Russia

Relations with the Russian Federation

Description: Below-radar supporter. These countries harbour concerns about Russia, but given complicated historical relations and local context, typically stay away from vocal criticism of Russian aggression.69

Bulgaria is a relatively new EU and NATO member with deep historical and cultural ties to Russia. Bulgaria is highly dependent on Russian fossil fuels; thus far, however, the government has steadfastly followed EU guidelines and rejected several Russian pipeline projects. Though not explicitly pro-Russian, the political mainstream in Bulgaria seeks to reconcile a firm pro-EU and pro-NATO stance with friendly relations with Russia. Bulgaria considers the sanctions regime against Russia an obstacle to its own economy. However, over the past few years, Bulgaria has grown increasingly aware of the threat Russia poses to the rest of Europe. Yet thanks to the deep penetration of Russian interests in the economy, combined with domestic corruption, Bulgaria must also contend with powerful Russian efforts to influence policy. This situation of ‘state capture’ further complicates Bulgaria’s response to malign Russian influence. According to the latest Eurobarometer, 72% of Bulgarians had a positive view of Russia. On the other hand, another poll found that Bulgarians “do not believe that Russia can be a model for development and provide more credible guarantees for prosperity and security than membership in the EU and NATO.”70

---


Political acknowledgement of the threat

Internal political tensions in Bulgaria between pro-Russian and pro-Western factions have often contributed to a less than coherent message about the role of Russian influence in the country. For example, in 2014, a team around Defence Minister Velizar Shalamanov drafted a NATO strategy paper that named Russia as a threat to Bulgaria based on concerns including “propaganda warfare, Russia’s links with politicians and business people, energy dependence and influence over the media”. However, after a domestic uproar and pressure from Russia, Prime Minister Georgi Bliznashki withdrew and revised the report, eliminating explicit mention of Russia’s information war against Bulgaria. Thus, although Bulgaria has seen some political acknowledgement of Russian disinformation and attempts to exercise hostile influence, competing (pro-Russian) voices try to drown out the message. These include several radical pro-Russian parties and political groups that fuel Soviet nostalgia and are critical of the West, such as the Bulgarian Socialist Party, the far-right and ultranationalist Ataka, the new centre-left Alternative for Bulgaria, and the National Movement of Russophiles. Leaders of the BSP and ABV attended a United Russia congress in June 2016. These actors, although they remain on the political fringe, serve as Kremlin proxies within Bulgaria, suppressing any notion of a Russian threat while working to advance Russian interests within the country.

The only major Bulgarian party that has sought to distance the country from Russia is the centre-right Citizens for European Development of Bulgaria (GERB). The current Bulgarian President, Rosen Plevneliev, is constitutionally independent and has publicly asserted that Russia is waging “a hybrid warfare campaign aimed at destabilising the whole of Europe.” Meanwhile, Prime Minister Boyko Borisov (GERB) exercises greater restraint in his rhetoric to avoid disaffecting his pro-Russian coalition partners.

Government activities against Russian influence & disinformation

Bulgaria has thus far undertaken little concrete action to address the threat of Russian disinformation and hostile influence operations in the country. Despite extensive proliferation of pro-Russian disinformation by way of home-grown media outlets (e.g., A-specto, Duma, Rusia Dnes, Ruski Dnevnik), the Bulgarian government has been very slow to address this problem, and conspiracy theories are rife amongst the public. In 2014, President Rosen Plevneliev stated, “90% of the media in Bulgaria work...
for Russian masters."\(^{77}\) Given the competing political interests in the country, Bulgaria has often vacillated between “policy resistance and capitulation” with respect to Russian pressure and attempted influence.\(^{78}\) Nonetheless, the current Bulgarian government is supporting a tougher stance on Russia, despite opposition from the domestic radical fringe and public preference for a more “risk-averse” approach.\(^{79}\) On sanctions, Bulgaria continues to follow the lead of EU heavyweights like Germany and France. The government continues to be committed to both the EU and NATO, as well as to multilateral security and cooperation via other European and international institutions.\(^{80}\)

**The approach of intelligence agencies to Russian interference**

The 2015 annual report on the state of national security names several threats originating from Russia that pose a risk to Bulgaria: the destabilisation of eastern Ukraine; escalation of existing (frozen) conflicts; intensive attempts by Russia to restore and expand spheres of influence through military, economic and cultural means, including pressure on other states' foreign policy; hybrid war, involving attempts of foreign countries to influence public opinion through disinformation, propaganda campaigns, media manipulation, use of social networks and populist parties; and energy dependency.\(^{81}\)

Given Russia’s high stakes in the country, Bulgaria is also a key target for Russian intelligence operations. Earlier this year, Bulgarian officials revealed that a Russian spy delivered a document to the leader of the pro-Russian Bulgarian Socialist Party detailing a strategy for the country’s presidential campaign. This document provided instructions for planting fake news and drawing attention to rigged polls, along with criticising the West and calling for an end to sanctions on Russia.\(^{82}\)

**Activities of the non-governmental sector**

In Bulgaria, there are no relevant non-governmental initiatives explicitly dedicated to tackling the issues of Russian disinformation and other subversive influence operations. However, a few Bulgarian think tanks and academic/expert fora are occasional contributors on this front.\(^{83}\) These include: the Center for the Study of Democracy,\(^{84}\) a public policy institute that analyses, *inter alia*, the extent of Russian influence in Bulgaria and the post-Soviet space as well as Russian destabilisation efforts with respect to Western institutions; Bulgaria Analytica;\(^{85}\) and the Sofia Security Forum,\(^{86}\) an NGO active in publishing and organising conferences on matters of international security. There are no apparent initiatives dedicated to media literacy.

---

77 Bechev (2015).
78 Conley et al. (2016).
83 Bechev (2015); Conley et al. (2016).
84 See <http://www.csd.bg/>.
IV. Croatia

Political acknowledgment

Government activities

Intelligence services approach

Summary

- With rare exceptions, politicians in Croatia do not recognise nor acknowledge the threat of Russian disinformation and/or influence operations
- The activities of the government and civil society are limited to enhancing media literacy
- Concern about declining press freedom makes Croatian society more vulnerable to hostile influence operations

Relations with the Russian Federation

Description: Below-radar supporter. These countries harbour concerns about Russia, but given complicated historical relations and local context, typically stay away from vocal criticism of Russian aggression.  

While Croatia has been wary of the Russian Federation since gaining independence in 1991, given Russian support of Serbia in the Yugoslav Wars, it nonetheless sustains positive relations at the business level. However, the two countries have lost significant common ground since Russia’s occupation and subsequent annexation of Crimea. Recently, Croatia has begun to express concerns about Russia’s frequent joint military exercises with Serbia. The country has also been attempting to become an alternative supplier of gas for Central, Eastern and Southern Europe, to limit dependence on Russia.

Croatia has been generally supportive of EU policy against the Russian Federation and has condemned the violence in Ukraine. After the EU sanctions were put in place, the Croatian Ambassador to Moscow declared that Croatia shares the EU’s principles and does not recognise the annexation of Crimea. The Croatian political representation has maintained its stance on sanctions being strictly dependent on


implementation of the Minsk agreements. However, Croatia has kept cooperation with Russia alive on other issues, for example on dealing with the crisis in Syria.\textsuperscript{89}

**Political acknowledgement of the threat**

Disinformation campaigns or influence operations originating in Russia or even in general are not on the Croatian agenda. In November 2016, the current Croatian President Kolinda Grabar-Kitarovic said in an interview that Russian “hybrid warfare” together with Russian connections with Serbia in the form of “intelligence, information and disinformation campaign” represent a threat in Croatia’s immediate neighbourhood,\textsuperscript{90} but so far there has been no concrete action of the state administration.

These threats have not been acknowledged or described in any strategic documents. The Croatian Foreign Minister’s Strategic Plan (2016-2018)\textsuperscript{91}, Foreign Policy Aims\textsuperscript{92} and the Activity Report of the Ministry of Foreign Affairs (2011)\textsuperscript{93} focus almost exclusively on economic relations and cooperation in the energy sector, as do the statements of Foreign Ministers Vesna Pusić and Miro Kovač from recent years.\textsuperscript{94}

**Government activities against Russian influence & disinformation**

Croatia has been more active in the area of media literacy. The Agency for Electronic Media of the Republic of Croatia, the official Croatian regulatory authority, launched an internet website\textsuperscript{95} aimed at educating teachers and parents about the media and how to pass the knowledge on to children within schools and at home. However, the country has more challenges to deal with in the media landscape. Croatian journalists have been recently raising concerns about the obstacles they face while conducting investigative work and, by extension, about the decreasing level of media freedom in Croatia. Some state measures, for example the removal of dozens of employees from the public broadcasters or the abolition of funding for non-profit media, have been widely criticised.\textsuperscript{96}


\textsuperscript{92} Foreign Policy Aims. Ministry of Foreign and European Affairs, Republic of Croatia. \texttt{<http://www.mvep.hr/en/foreign-politics/foreign-policy-aims/>}


\textsuperscript{96} “Croatia: Media Freedom in Turbulent Times.” South East European Network for Professionalization of Media. 10 August 2016. \texttt{<http://seenpm.org/croatia-media-freedom-turbulent-times/>}
The approach of intelligence agencies to Russian interference

The Croatian Security-Intelligence Agency (SOA) does not mention Russian activities in any form in its Public Report for 2015. It does, however, give space to information security, especially regarding the communication within state bodies. According to Rapid7, a security company from the United States that uses its Project Sonar software to compare countries according to their vulnerability to hacking, Croatia is the 40th most vulnerable country overall and 9th most vulnerable amongst the EU28. In December 2016, the Croatian Foreign and European Affairs Ministry also disclosed that during the previous government’s term, there had been a cyber-attack on its communication network. According to the Croatian press, there is suspicion that the attack was launched by Russian hackers; however, the culprits have never been revealed. According to the Public Report, the SOA conducts dozens of anti-bugging checks each year in important facilities across the country and abroad in order to ensure the safety of communication, but enhancing cyber-security and hacking protection is not the main priority.

Activities of the non-governmental sector

The non-governmental sector in Croatia has also been active in the field of media literacy. The project established by the Agency for Electronic Media mentioned above has been supported by UNICEF for its emphasis on the importance of media literacy and the education of adults and children. Domestic partners also participate in the project, including professional and academic organisations such as the Croatian Audiovisual Centre, the Croatian Film Association, the Academy of Dramatic Arts, and the Faculty of Political Science.

VI. Cyprus

Summary

- The Cyprian government considers Russia an ally in supporting the integrity of the country, although there are doubts about Russia’s actual interests amongst some journalists.
- The Cyprian media have been speculating about Russia’s hypothetical ulterior motives for meddling in Cyprus’ internal affairs with an agenda different than publicly claimed.
- Cyprus’ political representation has not acknowledged these speculations in any way.

Relations with the Russian Federation

**Description: Kremlin friendly.** These countries do not feel threatened by Russia and rather advocate for better relations with the Kremlin, despite any atrocities Moscow has committed. They often support the Kremlin’s foreign policy objectives, such as pre-empting further sanctions, by way of arguments related to appeasement or alleged business ties.¹⁰²

Cyprus belongs to the group of EU countries that does not perceive any threat coming from Russia and instead maintains a close relationship with the regime. Russia has supported the integrity of the island since the Soviet era, which makes Moscow a key foreign partner of Nicosia. Cyprus is also Russia’s primary offshore banking haven, home to 40,000 Russians and a popular destination for Russian tourists. The Cyprian government has opposed sanctions against Russia, especially on the basis of the two countries’ economic ties, although the actual economic impact of the sanctions has been limited. At the same time, there is considerable Russian intelligence activity in the country and Cyprus fears that Moscow is using social and mass media, as well as its ties to fringe nationalist parties and the Greek Orthodox Church, to undermine the settlement talks.¹⁰³


Political acknowledgement of the threat

There has been no official acknowledgement of Russian influence operations and/or disinformation campaigns in any policy document. However, there have been voices expressing concerns about Russian meddling into the peace settlement between the parts of the island. Still, bilateral relations with Russia remain at a high level, even despite events in Ukraine. Either no official activities exist or they are not publicly admitted for domestic political reasons.

Cyprus is not a NATO Member State and the cooperation between NATO and the EU is not a high political priority; on the contrary, Cyprus often tries to decrease it. No shift has been noticeable even in the recent years. Cypriot officials are some of the most steadfast supporters of the idea that Russia is Cyprus’ true and honest ally and would not partake in any international activities targeted against it, unless absolutely unavoidable.

Government activities against Russian influence & disinformation

Several media outlets in Cyprus have breached a long-time taboo and recently begun speculating about their concerns that Russia might actually want to block the settlement on the island, as opposed to what it officially claims. These speculations arose following suspicious activities of the Ambassador of Moscow in Cyprus, Mr. Osadchiy. However, these worries have not been reflected by the majority of authorities. No measures to counter subversive influence have been taken thus far.

The approach of intelligence agencies to Russian interference

There are no known intelligence activities in Cyprus attempting to counter Russian influence operations, especially because such a target has not been identified in any strategy documents, nor are Russian channels perceived to be a threat to the country. There are also no known initiatives concerning cybersecurity.

Activities of the non-governmental sector

There are no relevant non-governmental activities or organisations focusing on disinformation campaigns or influence operations. There are several projects in place aimed at enhancing media literacy and internet security. CyberEthics Cyprus Safer Internet Center, co-founded by the European Union, established the Safer Internet Programme. This organisation participates on international projects and regularly reports illegal content on the Internet. It also tries to engage with the government and civil society and contributes to the eradication of cybercrime.

The topic of cybercrime has also been picked up by the Cyprus Cyber Crime Centre on Excellence for Training, Research and Education (3CE), which provides specialised training for people from both the public and private sectors.


VI. Czech Republic

Political acknowledgment

- - - - -

Government activities

- - - -

Intelligence services approach

- - - -

Summary

- The Czech Republic is one of the leading countries regarding countering Russian subversive influence: it understands the threat and actively reacts on the state level
- Civil society in the Czech Republic is active and has succeeded in placing the topic on the public agenda
- The position of the Czech Republic is undermined by its President, Miloš Zeman, who is thought to be one of Russia’s most prominent allies in Europe

Relations with the Russian Federation

Description: The awakened. These countries have significantly updated their policies and concerns following Russian aggression in Ukraine.\(^{106}\)

The stance of the Czech Republic towards Russia changed significantly following the crisis in Ukraine and Russia’s subsequent annexation of Crimea. Despite the ambivalent positions of some individual politicians, as well as a high dependence on imports from Russia, the Czech Republic is fully aware of the threats Russia poses. However, pro-Russian President Miloš Zeman plays a significant role in maintaining relations with the Kremlin, having denied the presence of Russian troops in Ukraine after the Crimean annexation and repeatedly criticising the EU sanctions against Russia. Zeman also retains strong ties to Russian business.\(^{107}\)

Political acknowledgement of the threat

Czech strategy documents are quite sophisticated in terms of their identification and description of Russian influence and disinformation operations. The Defence Strategy from 2017 clearly states that the Russian Federation uses a set of hybrid campaign tools against the member countries of NATO and EU, including targeted disinformation activities and cyber-attacks.\(^{108}\) The Security Strategy from 2015


already mentioned the hypothetical threat of hybrid warfare and disinformation intelligence operations, although without specifically naming Russia as the perpetrator.\textsuperscript{109} In the Long Term Perspective for Defence 2030, the Czech Ministry of Defence expressed its expectations that the misuse of information, technologies, and the media will play a significant role in the future and that the international misuse of the media for information warfare will grow.\textsuperscript{110}

But the most fundamental document was the product of the National Security Audit conducted by the government in 2016 with a chapter devoted to the influence of foreign powers. It includes a SWOT analysis summarising the strong and weak aspects of the Czech Republic’s vulnerability and presents specific recommendations for enhancing resilience, including the establishment of centres for evaluation of disinformation campaigns within relevant authorities, creation of a system of education for public officials to make them more resilient towards foreign influence, and active media strategies for important democratic institutions or measures concerning media law.

**Government activities against Russian influence & disinformation**

Based on these recommendations, the Center against Terrorism and Hybrid Threats was established in 2016 within the Czech Ministry of Interior and began operating in January 2017. The Center monitors threats related to the internal security of the Czech Republic, including disinformation campaigns.\textsuperscript{111} It is also tasked with advising the government on threats in the information space and with publicly debunking disinformation about domestic issues. It continues in its efforts despite the political backlash from President Zeman, who has accused the Centre of censorship.\textsuperscript{112}

In addition, the Czech government has a seconded-national expert at the EEAS East STRATCOM team in Brussels as well as an expert at the NATO STRATCOM COE in Riga (since 2016). It has not joined as a sponsoring nation.

**The approach of intelligence agencies to Russian interference**

The Czech intelligence services have been forced to acknowledge the existence of Russian threats due to the Kremlin’s intensive espionage activities on Czech soil. Russian spies are thought to be some of the most active foreign agents operating in the Czech Republic. They also try to cooperate with the Russian community in the country. Some of these agents have had to be expelled from the Czech Republic, although the Czech Foreign Ministry has not escalated the conflict publicly thanks to possible reciprocation from Moscow.\textsuperscript{113}


\textsuperscript{111} Centre Against Terrorism and Hybrid Threats. Ministry of the Interior of the Czech Republic. \textltt{http://www.mvcr.cz/ctih/clanek/centre-against-terrorism-and-hybrid-threats.aspx}


In its Annual Report for 2015\textsuperscript{114}, the Czech Security Information Service (BIS) warns against Russian activities, focusing on the information war regarding the Ukrainian and Syrian conflicts and on political, scientific, technical, and economic espionage. According to the Report, these information operations aim to weaken the Czech media, influence perceptions, confuse their audience, promote tensions, disrupt NATO and EU alliances, and isolate Ukraine. Together with China, Russia has been accused of being the gravest threat as far as state-led or state-sponsored cyber-espionage campaigns are concerned.

\textbf{Activities of the non-governmental sector}

Since the annexation of Crimea, Czech civil society has been notably active in terms of tackling disinformation. However ad hoc and reactionary their responses, many non-governmental organisations are well-established and have proven especially successful in monitoring disinformation circulated in the media space and in debunking fake reports.

The biggest shortage of activities exists in the areas of security issues, journalism, and media literacy. Attempts to promote educational activities in schools are rather small and none are systematic. These projects and organisations also often fall short in their coordination.

The European Values think-tank established a Kremlin Watch programme in 2015, which regularly fact-checks news reports originating in pro-Kremlin media, produces bi-weekly reports on disinformation trends and narratives spread in the Czech Republic, and cooperates with the EEAS STRATCOM East team as well as with other foreign partners on numerous projects. It also focuses on policy development and endeavours to motivate the state administration into taking further steps towards tackling disinformation campaigns.

The Association for International Affairs launched a Czech version of the Ukrainian website StopFake.org in October 2016, dedicated to verifying disinformation about the conflict in Ukraine. The Prague Security Studies Institute launched an initiative to raise awareness about pro-Russian disinformation in 2015; it publishes articles and reports on the topic and organises events and debates for both experts and the public.\textsuperscript{115} People in Need produced an educational pamphlet for teachers on Russian disinformation.\textsuperscript{116} Likewise, the Czech academic sphere has not remained behind. The Department of Political Science at the Faculty of Social Studies at the Masaryk University in Brno analyses manipulation techniques and emotions used by pro-Kremlin disinformation sources and provides training in media literacy. It also launched a student project called zvolsi.info in order to raise awareness about the importance of media literacy amongst young people.


\textsuperscript{115} "Russia’s Influence Activities in CEE". \textit{Prague Security Studies Institute}. <http://www.pssi.cz/russia-influence-activities-in-cee>

\textsuperscript{116} See <https://www.jsns.cz/cz/article/111/What_is_jsns.html?id=243>
VIII. Denmark

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Denmark’s free and competent press is one of the most important foundations of national defence against foreign subversion.

- The arrival of subversive warfare on the agenda in the past three years, along with the rise of cyber-attacks likely perpetrated by Russia or pro-Russian hackers, have made cyber-security and anti-subversion measures an important aspect of Russian government policy.

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.\(^\text{117}\)

Relations between Denmark and Russia have been relatively cool ever since Putin’s rise to power, spoiled by factors including the war in Chechnya, Russian human rights violations, and environmental concerns stemming from Russia’s pipeline building activities in the Baltic Sea. Today, Denmark faces persistent military and diplomatic pressures from Moscow, but remains a firm supporter of the international sanctions regime against Russia.

Political acknowledgement of the threat

The Danish Royal Defence College (Forsvarakademiet) mentions the danger of “hybrid threats” in its 2017 report on cyber-security, and briefly in its 2016 report.\(^\text{118}\) In April 2017, the Minister of Defence, Hjort Drefireksen, spoke about a “continuing war from the Russian side” in the field of cyber-attacks, which were, according to him, “connected to the intelligence agencies or key elements of the Russian government.”\(^\text{119}\)

---


Government activities against Russian influence & disinformation

The Institute for Strategy (IFS), a section of the Royal Defence College, has shown particular interest in analysing the strategic implications of developments in Russia, China, and the Middle East, not least due to Russia’s recent activities in the latter region. Denmark has also sent its expert to the EEAS East STRATCOM Team.

The approach of intelligence agencies to Russian interference

Denmark’s Center for Cybersecurity has been operating since 2012 under the Ministry of Defence. More recent initiatives also include the Computer Network Operations Capacity, which is tasked with both defensive and offensive operations against hostile cyber-infrastructure. In its 2017 assessment, the Center for Cybersecurity assessed Russia as one of the states most heavily invested in hacking.

Moreover, in 2015, Denmark became active in building up its offensive cyberspace capacity, demonstrating the high level of importance that cybersecurity holds in the country’s national defence capacity. This is not without a good reason, since Denmark’s Defence Ministry has fallen victim to Russian hack attacks in 2015 and 2016, resulting in hackers gaining access to the ministry’s employees’ emails and non-classified documents, potentially leading to employees’ personal data being used against them by criminals. The story about the email hack came months after Danish Defence Minister Claus Hjort Frederiksen warned that Russia is prepared to engage in a cyber-offensive against the Kingdom.

Activities of the non-governmental sector

The Danish Institute for International Studies (DIIS) has been involved in analysing the issue of foreign subversion and disinformation. Flemming Splidsboel Hansen, a senior researcher at the DIIS, is one of the Institute’s most notable experts on issues surrounding Russia and the former Soviet Union, and is an author of several articles on Russia. In 2016, Hansen analysed Russo-Western relations in the...
light of ontological issues of Russian self-identity vis-à-vis the West, which (according to Hansen) fuel Russian aggression and hostility towards the West.128

Danish newspapers have also written extensively about Russia’s circulation of fake news in the West. In his blog for Berlingske Business, Sten Løck raises the issue of how public debate in Western democracies is being diluted by disagreement about what facts to accept, and recommends an English-language website called Snopes.com for those wishing to ensure they are familiar with real rather than ‘fake’ facts.129 Djoefbladet’s Regner Hansen has written how fake news is hitting European states in the midst of several electoral cycles130. More recently, Uffe Ellemann, writing for Berlingske.dk, provides an example of his friend being deceived by fake media spreading a myth that 3500 U.S. tanks were deployed at Russia’s borders.131 The online magazine Zetland.dk features an article by Frederik Kulager outlining how Russian disinformation spreads in Denmark, and the role that certain local sources, like 24NYT, play as disseminators of disinformation.132

---


X. Estonia

Political acknowledgment ⬤ ⬤ ⬤ ⬤ ⬤
Government activities ⬤ ⬤ ⬤ ⬤ ⬤
Intelligence services approach ⬤ ⬤ ⬤ ⬤ ⬤

Summary

- Estonia has shown a particular interest in establishing defence against hybrid threats, not least due to its high Russian-speaking population
- Estonian government is actively engaged with volunteers and the country’s civil society in combatting hybrid threats and disinformation by Russia
- Highly digitised Estonian government infrastructure has been victim to Russian cyber-attacks, with some believing it to be the first target of a hybrid warfare tactic utilised by Russia, making cyber-defence and media fact-checking important aspects of Estonian national security

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.¹³³

Estonia has suffered from cyber-attacks and the agitation of its Russian minority by Russia in the past, and is often seen as one of the first victims of its “hybrid war” tactics. Estonia’s sizeable Russian minority and the government’s naturalisation policies are often brought up by Russian diplomats in order to paint Estonia as a human rights violator, despite the situation being far more complex than that. Russia plays a significant role in shaping Estonian national security policy, and the events of 2014 in Ukraine only assured Estonia that its fears were justified and that more EU member states will develop awareness of the Russian threat.

Political acknowledgement of the threat

Former President Toomas Hendrik Ilves has expressed concern that Russia may use hybrid tactics against Estonia.¹³⁴ His concerns are shared by the current President Kersti Kaljulaid.¹³⁵ However, the Centre Party, its former leader Edgar Savisaar, and the current Prime Minister Jüri Ratas have become

subject to scrutiny over their alleged ties to Putin’s United Russia Party. Still, Russia’s actions in Ukraine have alarmed the vast majority of Estonian policymakers, and the dominant consensus is that Estonia must be prepared to defend itself against potential repetitions of a Ukrainian scenario in the Baltics.

**Government activities against Russian influence & disinformation**

In 2016, Former Estonian Prime Minister Taavi Rõivas proposed establishing a permanent financing scheme for the EU Strategic Communication Task Force (EU STRATCOM).

Teabeamet, the official foreign news service of the Estonian government, publishes yearly analyses of threats and challenges that Estonia faces. This work is compiled in a report called “International Security and Estonia”, with the latest report for 2017 already available. This report analyses both Russian domestic and foreign policies, emphasising Russia’s goal of expanding its influence across the former Soviet states and the Balkans.

Estonia has a seconded-expert on the EEAS East STRATCOM Team and is one of the sponsoring nations of the NATO STRATCOM COE in Riga.

**The approach of intelligence agencies to Russian interference**

KAPO (Kaitsepolitsei), the Estonian Secret Police, is actively involved in combatting foreign influence by Russia, particularly by targeting Estonia’s Russian minority, since Russian espionage tactics frequently involve recruiting local Russian-speaking citizens, and Russian-language media often portrays NATO as an anti-Russian institution.

Identifying and apprehending Russian spies is an important part of Estonian counter-intelligence work. One of the most recent espionage-related arrests occurred in January 2017, while in 2016 two dual citizens of Russia and Estonia were apprehended and sentenced to jail for spying in Russia’s favour. The case of Uno Puusepp, a retired double-agent who eventually moved to Moscow, shows that Russian

---


intelligence activities in Estonia date as far back as the 1990s.\textsuperscript{142}

The more recent case of Eston Kohver, an Estonian security official kidnapped by Russian security in 2015, has brought attention to Russian intelligence activity in Estonia. Though Kohver was sentenced to 15 years in jail for espionage by a Russian court, he was released by Russia in exchange for Aleksei and Victoria Dressen, who had been charged and sentenced by Estonian authorities for Russian espionage in 2012.\textsuperscript{143}

**Activities of the non-governmental sector**

The Baltic Defence College, founded in 1998, organises events covering Russia, such as the Annual Baltic Defence College Conference on Russia, which began in 2014. The February 2017 conference looked at non-linear warfare perpetrated by Russia, namely its cyber- and memetic dimensions, among others.\textsuperscript{144}

The International Centre for Defence and Security (ICDS; RKK in Estonian) is a Tallinn-based think tank working in cooperation with the Estonian government, tasked with analysing a wide range of issues relating to Estonian security and national defence planning.\textsuperscript{145} Among events organised by the ICDS is the annual Lennart Meri Conference, which is to be held May 14-17 in 2017, and will present major issues facing the EU and NATO this year.\textsuperscript{146}

The Baltic Centre for Russian Studies (BCRS), founded in 1999 and directed by former Estonian Prime Minister’s advisor Vladimir Yushkin,\textsuperscript{147} raised concerns over potential hybrid warfare risks posed to Estonia by Russia.\textsuperscript{148} However, the BCRS’ activities remain elusive, and it is visible only via the figure of Yushkin and his media appearances.

Propastop.org is an anti-propaganda blog operated by volunteers – mostly members of the Estonian Voluntary Defence League (Kaitselit)\textsuperscript{149} – which itself works under the Ministry of Defence.\textsuperscript{150} The blog is tasked with countering disinformation that targets Estonia. It is currently publishing counter-propaganda material in the Estonian language, but also features an English-language page.
IX. Finland

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Major security concerns in terms of subversive actions have to do with strategic and tactical defence risks rather than risks posed to the country by disinformation by foreign actors.
- Finns have shown initiative in coming together with other EU member states, as well as with NATO, in order to counter subversive threats posed by Russia.
- Finnish civil society is active in highlighting the Russian state’s activities online and in combatting disinformation and fake news.

Relations with the Russian Federation

Description: The awakened. These countries have significantly updated their policies and concerns following Russian aggression in Ukraine.¹⁵¹

Finland is the one Nordic country that has always sought to find compromise with Russia due to its dependence on Russian fossil fuels and deep economic ties with Russia. Nonetheless, Finland is aware of the threat posed by Russia and engages in military co-operation with NATO in order to counter it. At the same time, Finland still sees hope in rebuilding EU-Russian relations.

Political acknowledgement of the threat

The Government Communications Department at the Prime Minister’s office issues press releases on recent government activities, but its Director General Markku Mantila has raised concerns about Russian influence in Finland.¹⁵² President Sauli Niinistö warned of “information warfare” in October 2015. In addition, Timo Soini, the Minister of Foreign Affairs, has said that Finland has become a target for hybrid threats through disinformation campaigns and malicious cyber activities. He has also claimed that


countering hybrid threats was a European priority. In acknowledgement of the threat coming from Russia, the Finnish government has decided to substantially raise its number of troops and increase military spending by 55 million euro.

**Government activities against Russian influence & disinformation**

The European Centre of Excellence for Countering Hybrid Threats is a recently founded Helsinki-based institution tasked with combatting subversive threats, working in close partnership with other EU member states, particularly the Baltics, Sweden, and Poland, as well as non-EU partners, such as the United States. Apart from this, Finland is also a partner country of the NATO STRATCOM COE in Riga.

Media literacy remains an important part of Finnish state policy, manifesting primarily in the country’s education sphere, with numerous media literacy initiatives targeting schools all around the country.

**The approach of intelligence agencies to Russian interference**

The Finnish Security Intelligence Service (Suojelupoliisi or SuPo) is tasked with combatting threats posed by foreign intelligence and terrorist groups, and cyber-threats in particular. However, its primary focus lies in the domain of counter-intelligence and anti-cyberwarfare measures.

**Activities of the non-governmental sector**

The Aleksanteri Institute of the University of Helsinki has produced publications analysing Russia’s subversion tactics and ways to counter them. One of these reports, authored by Bettina Renz and Hanna Smith, highlights the issue of Russians’ acquisition of critical infrastructure in the Turku archipelago, as well as that of Russia’s potential threat to communication satellite links in space.

The Finnish Institute of International Affairs (FIIA) is a publicly-funded independent institute that

---


publishes papers analysing Russia's war in Ukraine and Finland's preparedness to withstand foreign subversion, emphasising the role of psychological readiness for a potential attack. The Institute has published a report calling Russia a greater threat to Finland, highlighting the attempts of Russian intelligence to influence Finnish energy policy.

Faktabaari is an open-source project tasked with spreading factual information and fighting disinformation online. It is the pilot project of a wider EU initiative to establish national-level fact-checking services on the eve of the 2019 EU parliamentary elections.

In 2016, the editors-in-chief of several leading Finnish media outlets published a statement condemning fake or so-called 'alternative' media that present a danger to Finnish society as well as other countries.

Dr. Saara Jantunen has published a book detailing and debunking Russian disinformation and the tactics of harassment and false reporting used by pro-Russian trolls online. Jessikka Aro, an investigative journalist for the Finnish public broadcaster Yle, also played an important part in uncovering a troll factory in Russia in 2014.

The Finnish Society on Media Education (Mediakasvatusseura) is an organisation focused on improving media literacy in Finland, working in both Finnish and Swedish language towards that goal.

---


162 See [http://faktabaari.fi/in-english/]


167 See [http://www.mediaeducation.fi/finnish-society-on-media-education/]

54
X. France

Political acknowledgment
Government activities
Intelligence services approach

Summary

- The French government is concerned with disinformation and influence operations mostly from the perspective of dangers posed by Islamic propaganda
- The topics of Russian meddling, influence on political parties, and disinformation in the media have been raised in connection to the presidential elections
- The elections have been accompanied by a high level of activity among civil society, mostly in the areas of debunking disinformation

Relations with the Russian Federation

Description: Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of a threat.¹⁶⁷

Though traditionally friendly towards Russia, France’s stance has grown chillier following the 2014 events in Ukraine. French politicians are not without allegations of financial or intelligence ties to Russia, even though the government’s stance suffered through a radical U-turn on Russia following the annexation of Crimea. France was one of the key countries to initiate EU sanctions against Russia, but also one of the main countries to participate in negotiations between Russia, Kiev, and Ukraine’s pro-Russian separatists. In 2014, France decided to call off a deal with Russia regarding a sale of Mistral warships. Facing urgent domestic issues besides Russia, France’s national security focus is less concerned with Russian threats to the EU bloc and more with terrorism. Meanwhile, Eurosceptics and the far-right remain relatively popular, despite the alleged support of Russian intelligence.¹⁶⁸

Political acknowledgement of the threat

Although awareness is rising in France about the threat posed by Russian hostile interference – especially in connection with the recent elections, marred by allegations of Russian meddling – the country, which has recently suffered several terrorist attacks, is more concerned with battling Islamic terrorism.

¹⁶⁸ Ibid.
extremism and propaganda than it is with Russia. France is putting enormous effort into fighting Islamic radicalism; it has been in a state of emergency since the November 2015 Paris attacks, and measures aimed at countering terrorism and radicalism are undertaken systematically.

**Government activities against Russian influence & disinformation**

The French government has its own website targeted against Jihadist propaganda. Its year-old Action Plan Against Radicalisation and Terrorism mentions, among 79 other goals, that France should “continue to monitor, limit and obstruct all dissemination of extremist propaganda.” The French National Digital Security Strategy considers spreading disinformation and propaganda to be “an attack on defence and national security which is sanctioned by law.” Still, there are currently no publicly known measures aimed directly at countering Russian hostile activities.

Russian subversion may soon be dealt with more seriously with the inauguration of the newly elected French President Emmanuel Macron, who experienced Russian meddling during his own campaign. Macron’s official foreign policy adviser recently said: “We will have a doctrine of retaliation when it comes to Russian cyber attacks or any other kind of attacks. This means we are ready to retaliate against cyber attacks — not only in kind but also with any other conventional measure or security tool.”

France participates in the Finnish COE on Countering Hybrid Threats and has also joined the NATO STRATCOM COE. It does not have a seconded-national expert in the EEAS East STRATCOM team. The French military is also participating in NATO’s Enhanced Forward Pressure in the Baltics.

**The approach of intelligence agencies to Russian interference**

The 2013 French White Paper on Defence and National Security mentions several threats posed by Russia; however, disinformation and influence operations are not amongst them. Public documents of the intelligence committee and agencies (DGSE and DGSI) only mention Russia as a partner in fighting terrorism, since Russia is also a target of recruitment and disinformation by terrorist groups.

---

169 See <http://www.stop-djihadisme.gouv.fr/>


Activities of the non-governmental sector

The topic of Russian activities in cyberspace is addressed by the French Institute of International Relations (Institut français des relations internationals, IFRI). Also, the EU Institute of Security Studies (EU ISS) resides in Paris and engages with media issues such as Russian and Islamic propaganda and disinformation. One problem of the EU ISS is that it is not well known amongst other EU member states and therefore does not receive many tasks from them.

There are several important French experts on Russia – for example, Professor Cécile Vaissié’s book Russian Network in France received high praise. In the media, the topic of Russian propaganda and relations between the two countries is well documented in the liberal newspaper Le Monde and in the TV programme C dans l’air, broadcast on France5.

In order to fight fake news in France, Facebook and Google have joined the fact-checking initiative CrossCheck, which allows users to submit questions and gathers information provided by 16 French media outlets. In addition to that, Facebook decided to test its own fact-checking initiative in France – its users can flag information they suspect to be false and partnered media outlets then verify it. If at least two media sources label the information as false, the post appears on Facebook with a banner signalling that its content has been disputed.¹⁷⁵

Media literacy and critical thinking in general are being taught in schools, and journalism departments at prestigious universities, such as Sciences Po and the Sorbonne, are likewise engaging with these issues. However, a lot of graduates from such prominent universities often start their careers, for example, at the French Ministry of Foreign Affairs, already impregnated with a positive stance on Russia based on the rich historical ties between the two countries.

XI. Germany

Summary

- Germany is currently concerned with Russia’s meddling into its upcoming federal elections.
- Germany actively tries to boost its cyber defence and promote cyber security internationally.
- Over the past few years, Germany has started to take the threat posed by Russia more seriously.

Relations with the Russian Federation

Description: The awakened. These countries have significantly updated their policies and concerns following Russian aggression in Ukraine.¹⁷⁶

Though traditionally more sceptical about the threat posed by Russia than its eastern neighbours, Germany was a proponent of tough EU measures against Russia in the aftermath of the annexation of Crimea. Germany has witnessed a significant deterioration in relations with Russia in recent years, intensified by Russian attempts to spread fake news and influence the country’s internal political affairs (e.g., by backing populist parties and other pro-Russian groups through its network of contacts). These hostile efforts are exemplified by the ‘Lisa case’, in which a fake news story about the alleged raped of a 13-year-old Russian-German girl by migrants spread on Russian media websites in order to portray Germany and Angela Merkel as incapable of protecting its own (and Russian) citizens.

Russia remains Germany’s largest energy supplier, even though Germany was one of the first countries to advocate for better energy security during Russia’s natural gas disputes with Ukraine over the past decade. However, Russian meddling in Germany’s internal affairs remains a bigger threat than energy dependence on Russia so far. Right now, Germany’s main concern is countering Russia’s attempts to influence the outcome of the federal elections which will take place this fall.¹⁷⁷


¹⁷⁷ Ibid.
Political acknowledgement of the threat

Overall, following the ‘Lisa case’ and with the upcoming federal elections, the topic of Russia’s influence operations is gaining more attention in Germany both within the state administration and in the media. The 2016 White Paper on German Security Policy and the Future of the Bundeswehr considers cyber risks to be a major security threat and recognises that “the cyber and information domain has become an area of international and strategic importance that has practically no limits.” In November 2016, the federal government approved the State of IT Security in Germany 2016 report created by the BSI. This document provides a detailed analysis of the current situation in Germany, serves as a framework for interdepartmental cooperation in the field of cybersecurity, and foresees 30 strategic goals and measures for improvement in this area.

Government activities against Russian influence & disinformation

In 2011, the Federal Ministry of the Interior published its Cyber Security Strategy for Germany, which, among other things, called for establishing the National Cyber Response Centre and the National Cyber Security Council. Both of these institutions started functioning the same year.

The main goal of the National Cyber Response Centre is to optimise operational cooperation between all state authorities and to improve the coordination of protection and response measures for IT incidents. The Centre reports to the Federal Office for Information Security (BSI) and cooperates directly with important state institutions. The National Cyber Security Council, which represents the German Chancellor, the federal states, and a number of ministries, is tasked with strengthening cooperation between the state and the business sector in the area of cyber security.

The Bundeswehr (German military) has just recently launched the new Cyber and Information Space Command (CIR), which will have its own independent organisational structure, thus becoming the sixth branch of the German military. The Bundeswehr now sees itself “at the international forefront” regarding cyber warfare and plans to bring 13,500 German soldiers and civilian contractors currently dealing with cyber defence from a number of different locations under the CIR's roof.

At the beginning of April 2017, Germany unveiled a bill aimed to combat the spread of fake news and hate speech on the internet. If the bill becomes law, as now appears likely, it will amount to the boldest step yet by a major Western nation to control social media content. Social networks such as Facebook

---


and Twitter would have to rapidly remove fake news that incites hate and other “criminal” content or face fines as high as 50 million euros.¹⁸²

Germany is a sponsoring nation of NATO STRATCOM COE and participates in the Finnish COE on Countering Hybrid Threats; however, it does not have a seconded-national expert in the EEAS East STRATCOM team. The country is aware of the need for international cooperation on this front, which it often emphasises in its policy documents, together with its responsibility to take an active role.

The approach of intelligence agencies to Russian interference

According to the 2015 Annual Report on the Protection of the Constitution by German Ministry of the Interior, Germany sees Russia as one of the major players behind espionage activities and cyberattacks directed against Germany.¹⁸³ However, a year-long investigation conducted by German intelligence which was ordered by Angela Merkel in the aftermath of the ‘Lisa case’ has failed to uncover Kremlin-backed meddling into German politics. The intelligence report nevertheless stressed that Russia has been on “confrontational path” against Germany since 2014, that its media is “hostile”, and that German intelligence authorities are well-aware of the threat posed by Russia especially in connection with the upcoming federal elections.¹⁸⁴ “We have evidence that cyber-attacks are taking place that have no purpose other than to elicit political uncertainty. […] We have indications that [the attacks] come from the Russian region,” said Bruno Kahl, president of the Federal Intelligence Service (Bundesnachrichtendienst). Hans-Georg Maassen, president of the domestic BfV intelligence agency, said in an interview that cyberspace had become “a place of hybrid warfare” in which Russia is a key player.¹⁸⁵

Activities of the non-governmental sector

There are no known organisations or institutions in Germany devoting their activity solely to disinformation campaigns; however, lots of institutions engage in this topic within the broader scope of their activities. These include the German Council on Foreign Relations (Deutsche Gesellschaft für Aussenpolitik), whose main subject of interest is security policy and Russia; the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP), which focuses mostly on security and the region of Eastern Europe; and the Center for Applied Policy Research (Centrum für angewandte Politikforschung, CAP) at the University of Munich.

Education in Germany is directed individually by the federal states, but the Federal Agency for Civic Education (Bundeszentrale für politische Bildung, BPB) serves as an umbrella authority. Also important are the Mediale Pfade – Agency for Media Education, which develops new paths of learning and participation using media and focus on political education, and the Initiative D21, whose main objective is accelerating the transformation of Germany into a digital information society.

There are also some media outlets in Germany that have started investigating the issue of fake news (e.g., Die Zeit) and some independent fact checkers as well: for example, Correctiv is a team of German fact-checkers who work for Facebook but do not accept money from it, because they want to retain total editorial independence. Their work consists mostly of monitoring suspicious stories.\textsuperscript{186}

XII. Greece

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Greece has historically been one of Russia’s ‘Trojan Horses’ within the EU, advocating for the Kremlin’s interests in Brussels
- The current Greek government maintains exceptionally close ties with the Kremlin and other prominent Russian figures
- Greece does not acknowledge any threat pertaining to disinformation or subversive influence stemming from Russia

Relations with the Russian Federation

Description: Kremlin friendly. These countries not feel threatened by Russia and rather advocate for better relations with the Kremlin, despite any atrocities Moscow has committed. They often support the Kremlin’s foreign policy objectives, such as pre-empting further sanctions, by way of arguments related to appeasement or alleged business ties.187

Greece is one of the oldest NATO member states and the first Balkan state to join the EU. Greece’s difficult history with Turkey has urged it to look to Russia for support. Consequently, Greece has typically expressed opposition to any EU measures that could alienate Russia. The current Greek government, caught in the middle of a severe economic and financial crisis, has courted Russia in hopes of receiving aid that Brussels has failed to provide (and thereby also gain negotiation leverage). In 2016, Greece also signed a military partnership with Russia on the basis that it is necessary to maintain the Greek defence industry during the economic crisis. Greece is thus best described as one of the EU’s three ‘Kremlin friendlies’, together with Italy and Cyprus. For all this, Greece nonetheless remains committed to the EU and NATO, despite its extensive efforts to simultaneously maintain warm bilateral relations with Russia. According to the latest Eurobarometer, 66% of Greeks had a positive view of Russia.

Political acknowledgement of the threat

In Greece, there is no political acknowledgement whatsoever of any hostile Russian activity. On the contrary, the government is very sympathetic to Russian interests and worldview, according to which the

West is the aggressor and Russia is merely on the offensive. Indeed, rather than recognising the threat of Russia’s disinformation campaign and subversive efforts, Greek officials instead blame Western propaganda for fuelling the Ukrainian conflict. In 2014, for example, Defence Minister Panos Kammenos stated, “Western NGOs sponsored by Germany or foundations like the Clinton Institute provoked the crisis in Ukraine where a coup d’état overthrew the legal government”.188

**Government activities against Russian influence & disinformation**

Following the total lack of political acknowledgement, there are predictably no state efforts to counteract Russian disinformation or other hostile influence operations; indeed, these issues are officially treated as non-existent by the Greek government. Though Greece has historically maintained a friendly relationship with Russia, it has sought even closer ties with Moscow in light of the economic crisis and stringent demands of its creditors. The current government has notably intimate ties with Russia: the radical left-wing Syriza party has never supported EU sanctions on Russia and has very close contacts with Vladimir Putin, Russian nationalist Aleksander Dugin, and Russian oligarchs.189 Greece’s sympathy towards Russia is so strong that it verges on anti-Ukrainian: in 2014, Greek Prime Minister Alexis Tsipras accused Kyiv of harbouring neo-Nazis.190 Accordingly, Greece can be labelled Russia’s most important Trojan horse in Brussels. Within the EU, Greece serves a frequent advocate for Russian interests and maintains a stance of passive resistance to any punitive measures aimed at counteracting Russian belligerence.

**The approach of intelligence agencies to Russian interference**

Following the official government line, there do not appear to be any significant Greek counterintelligence activities vis-à-vis Russian disinformation or other hostile influence operations. There is no official acknowledgement of any such threat emanating from Russia.

**Activities of the non-governmental sector**

There are no non-governmental initiatives concerned with the threat of disinformation, hostile influence operations, or media literacy. On the contrary, public approval of Russia remains high, and the positions of various civic agents are in fact sympathetic to Russian narratives and disinformation about the West.

---

190 Dempsey (2015).
XIII. Hungary

Summary

- Hungary is vulnerable to Russian influence mostly because of its own domestic problems with emerging authoritarianism and press freedom
- Russia is not perceived as a threat; concerning media and the information space, the Hungarian government and intelligence are focused more on the topic of migration
- Civil society is being prevented from pursuing the goal of countering Russian influence

Relations with the Russian Federation

Description: Government using Russia-card for domestic reasons. While these countries have predominantly negative historical experience with Russia, the government uses relations with Moscow for domestic political and/or economic reasons, or as a tool against the EU establishment.191

The attitude of the Hungarian public towards Russia is generally hostile and the country remains dedicated to NATO, not least due to their troubled past marked by Russian occupation during the Communist era. However, the government of Prime Minister Viktor Orban uses good relations with Russia as leverage in Hungary’s relations with Brussels, and in order to support his own domestic authoritarian policies. It is a pragmatic fit since the Kremlin is known to support Eurosceptic and autocratic elements in European politics. After the annexation of Crimea, the Prime Minister sought to weaken European sanctions against Russia. Also, the far-right Jobbik party gravitates towards Moscow and promotes the Kremlin within the country, reportedly receiving Russian financial support.192

Political acknowledgement of the threat

Since the Russian Federation is an important economic, trade, and energy partner for Hungary, the strategic and policy documents of the country do not reflect the threats originating there, whether

conventional or unconventional. The National Security Strategy from 2012\textsuperscript{193} focuses on cyber security, stating that Hungary will have to face increasingly pressing and intricate challenges in the physical and virtual space of information technologies and the potential malicious use of these technologies by state and non-state actors.

**Government activities against Russian influence & disinformation**

The state organisation that might potentially deal with cases of disinformation campaigns and cyberattacks connected to internal security is the Counter Terrorism Centre (TEK) established by Prime Minister Orban’s government in 2010 within the Ministry of Interior. This SWAT agency specialises in counter-terrorism and hostage crises, but its role also extends to protecting the government and citizens.

In some cases, the Hungarian government is more inclined to enable the spread of Russian influence and conduct disinformation campaigns, for example in order to limit the freedom of the press.\textsuperscript{194} A large segment of the Hungarian mainstream media is under the control of the government, some outlets using Russian state media like Sputnik or RT as sources for their own coverage.\textsuperscript{195} The activities of civil society are openly unwelcome by the government.

On the international level, Hungary considers units like the EEAS East STRATCOM Task Force or the NATO STRATCOM COE important, but with limited influence. The country has no experts at any of them.

**The approach of intelligence agencies to Russian interference**

There are two intelligence services relevant in the case of dealing with subversive influence in Hungary. One of them is the Constitution Protection Office, an internal intelligence agency, and the second is the Information Office, or the civilian intelligence agency, which is involved primarily in non-military intelligence gathering operations abroad. But the members of these agencies are sometimes suspected of influencing or even threatening local Hungarian journalists.\textsuperscript{196} They are not known to be working in order to prevent the influence of foreign powers, with the exception of perhaps Islamist propaganda.

**Activities of the non-governmental sector**

Political Capital, an organisation focusing on policy research, is the most visible non-governmental institution trying to analyse and counter disinformation operations in Hungary. It often cooperates with

\textsuperscript{193} National Security Strategy (2012). *Ministry of Foreign Affairs, Hungary.*
other organisations mostly from Central and Eastern Europe and also works with the EEAS East STRATCOM unit. Already in 2009, this think-tank warned about the pro-Russian attitudes of Eastern European far-right parties and, in 2014, published a study revealing that the interests of the Kremlin were being furthered and incorporated into policy by far-right parties in Europe. The relations between Europe and the Russian Federation represent a significant aspect of their work, including Russian efforts to gain influence through political and cultural lobbying and disinformation campaigns.
XIV. Ireland

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Ireland has shown very little, if any, activity in terms of combatting threats posed by Russia
- Its geographic distance from Russia and limited political clout in the EU arena makes Ireland a less attractive target for Russian subversion than more prominent EU players

Relations with the Russian Federation

Description: No relations with Russia. These countries are geographically distant from Russia and have almost no interest in any of the relevant issues.\(^{197}\)

Ireland’s position towards Russia is barely identifiable, but in most matters of international relations, Irish politics tend to seek common ground with the United Kingdom. The primary interest Ireland has in Russia is commercial. When it comes to defence measures, Ireland tends to rely heavily on the UK’s military. So far, Ireland remains uninterested in abandoning its neutrality policy.

Political acknowledgement of the threat

Fine Gael MP Brendan Griffin urged the government to expel Russian Ambassador Maxim Peshkov over the assault of Aleppo, Syria.\(^{198}\) Taoiseach (Prime Minister) Enda Kenny also called for tougher sanctions on Russia in response to the siege.\(^{199}\) However, the issue of a potential Russian disinformation campaign and subversion against Ireland have not been highlighted by the country’s politicians, even though Russian military planes have come close to invading Irish airspace several times in the past.\(^{200}\)


Government activities against Russian influence & disinformation

There are no visible activities in this sphere by the Irish government.

The approach of intelligence agencies to Russian interference

Ireland’s Directorate of Military Intelligence (G2) is the republic’s secret service, tasked with upholding Ireland’s national defence capacity particularly in the field of counter-espionage. Little is known about G2 except that it is under Ireland’s Defence Forces command.201 Another important institution is the Crime and Security Branch (CSB) of the national police force (the Gardai);202 however, it remains elusive from public view.

The most prominent case of Russian spy activity in Ireland occurred in 2010 and had to do with US-based Russian spies using Irish passports to travel between countries.203 During the investigation of this incident, a Russian ambassador was expelled from the country.204

Activities of the non-governmental sector

The Irish Medical Organisation’s president Dr. Ann Hogan highlighted how “fake news” spread over social media have led to a decline of MMR vaccine uptake in the country.205


XV. Italy

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Countering Islamic propaganda is considered to be a much more relevant topic than countering propaganda spread by Russia
- Good relations with Russia and the existence of pro-Russian politicians prevent Italy from acknowledging Russian disinformation campaigns
- Civil society plays a crucial role in media literacy amongst Italian citizens

Relations with the Russian Federation

Description: Kremlin friendly. These countries do not feel threatened by Russia and rather advocate for better relations with the Kremlin, despite any atrocities Moscow has committed. They often support the Kremlin’s foreign policy objectives, such as pre-empting further sanctions, by way of arguments related to appeasement or alleged business ties.

Though traditionally a country with deep economic ties to Russia, Italy has shown strong support for a common EU and NATO stance on Russia. At the same time, Italy does not wish to completely alienate Russia, and continues to believe that a dialogue is possible. Although Italy has shown disapproval of Russian actions in Syria, its national security is more concerned with the refugee influx from the Mediterranean than with any immediate threats which Russia may pose. Italian politics is full of pro-Russian elements and many politicians believe that the EU sanctions are harmful to Italy and should therefore be lifted.

Political acknowledgement of the threat

Overall, Italian authorities are not particularly interested in the topic of Russian subversion, partly because of the good relationship between the two countries and the frequent presence of pro-Russian attitudes amongst Italian politicians. Countering Islamist propaganda is considered to be a much more pressing topic than countering propaganda spread by Russia.

---


207 Ibid.
The problem of disinformation started to resonate in Italy during and after the failed constitutional referendum in December 2016, when the former comedian Beppe Grillo and his populist party, the Five Star Movement, began circulating fake news and pro-Russian propaganda. Currently, the President of the Italian Chamber of Deputies, Laura Boldrini, has a leading role in the battle against fake news – for example, she has urged Facebook to do more to counter this problem in Italy and started a petition against fake news which has already been signed by thousands of Italians.208

**Government activities against Russian influence & disinformation**

Regarding cybersecurity, Italy is somewhat behind countries such as Germany and France. It is only in the last couple of years that the country has recognised cyberspace as a new domain of warfare.209 As far as Russian disinformation and influence operations are concerned, the current National Strategic Framework for Cyberspace Security from 2013 does not provide any information about such threats.210 According to the 2015 White Paper for International Security and Defence, “there is a high risk that in the future, even in conventional conflicts, enemy forces will use unconventional or asymmetric forms of fighting more frequently (hybrid threats),” which is almost everything the paper says about this issue.211

The Italian government is currently working on a new cyber security strategy, which should bring more effective prevention and reactions to cyberattacks. In early 2017, the Joint Command for Cyberspace Operations was established; however, it is not yet possible to evaluate how operational the unit is.

Italy is a sponsoring nation of NATO STRATCOM COE but does not actively engage in other joint activities at the EU level, including the EEAS East STRATCOM Task Force.

**The approach of intelligence agencies to Russian interference**

The Italian secret services are more concerned with the threat posed by Islamic extremism than with that posed by Russia.212 The vulnerability of Italian cyber defence was exposed in February 2017 when Italian authorities discovered a cyberattack on the Italian foreign ministry, which lasted for more than

---


four months. Russia is suspected of being behind the attack although, according to the Italians, no sensitive information was acquired by the attackers.213

Activities of the non-governmental sector

There are many institutions which, at least in part, deal with the topic of propaganda and disinformation campaigns (not only by the Russian Federation but also by ISIS/Daesh). These include, for example, the Centre for International Studies (Centro Studi Internazionali, Ce.S.I.), the Luigi Sturzo Institute, the Italian Standing Group on International Relations (SGRI) of the Italian Society of Political Science (SIPS), the Istituto Affari Internazionali, and other think tanks.

The non-governmental actors also play a crucial role regarding media literacy. Since there are neither legal/institutional frames for media education nor well established policies to promote it at the state level, grass roots projects and initiatives have played a particularly important role on this front for a long time.214


XVI. Latvia

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Latvian activities largely focus on restricting Russian media and trying to provide quality news reporting for the Russian minority in the country
- Latvia also has a sophisticated and coordinated network dedicated to cybersecurity
- The NATO STRATCOM COE resides in the Latvian capital and the country is a major supporter of international activities

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.215

Latvia was one of the first ex-Soviet states to join the EU and NATO in 2004 and remains a key NATO member state, sharing a border with Russia and Belarus. Latvia is the most Russified of the Baltic States. Like Estonia, it has a sizeable Russian minority, including non-citizens, living in the country. Due to its geographic location and existing infrastructure, Latvia was traditionally dependent on Russian fossil fuels. Large percentages of Russian speakers increase threats posed by Russian intelligence, fake news, and disinformation – something the Latvian government is acutely aware of. Still, Latvia is highly active in EU and NATO efforts to counter Russian threats; it is highly supportive of closer ties between the EU and Ukraine, and supports the sanctions regime against Russia for the annexation of Crimea.216

Political acknowledgement of the threat

Together with the other two Baltic states, Latvia is on the forefront of countering Russian disinformation and influence operations. Besides being very active in addressing this problem internationally, it has noticeably stood up to the Russian threat at home as well. The Latvian government is well aware of Russia’s influence in their country and develops measures aimed at countering it. This phenomenon is gradually becoming a significant tool of both Latvian domestic and foreign policy. Functioning democratic

216 Ibid.
institutions and the rule of law, together with healthy scepticism towards Russia by the vast majority of ethnic Latvians, have contributed considerably to Latvia’s resilience.217

The 2015 National Security Concept lays out priorities that Latvia should follow in order to prevent threats to its information space. These priorities are: “development of the public media, reduction of influence of the information space of the Russian Federation, and development of the Media Literacy and Media Education.”218

**Government activities against Russian influence & disinformation**

In 2016, the country temporarily restricted Russian media on three occasions, citing reasons of hate speech and warmongering. When Latvian authorities shut down the pro-Kremlin site Sputnik, they even called it a “propaganda tool”.219 Although the effectiveness of these actions is arguable, they served well as a statement of values. Latvian authorities and independent media also try to offer the Russian minority in Latvia their own programmes and sources of information which are not part of the Russian media machine.220

Latvia has its own Cyber Security Strategy, which was published in 2014. The development of cyber security policy, along with the planning and implementation of objectives and measures, is coordinated by the National Information Technology Security Council, which also ensures the exchange of information and cooperation between the public and private sector.221 The National Computer Security Incident Response Team (CERT.LV) is responsible for the country’s IT security. It cooperates with more than 600 IT specialists from government institutions and local authorities. In addition, the country also has a Cyber Defence Unit, consisting of a team of IT specialists and students from the public and private sector who are trained to help the national armed forces or CERT.LV in case of need.222

Perhaps the most important criterion when assessing Latvia’s impact on countering Russian influence in Europe is its offer to establish the NATO STRATCOM Centre of Excellence in Riga in 2013. Both of the Centre’s directors have been Latvians. Latvia also has a seconded-national expert in the EEAS East STRATCOM team in Brussels and participates in the Finnish COE on Countering Hybrid Threats.

---


Overall, Latvia actively promotes international cooperation on countering Russian disinformation and influence operations.

The approach of intelligence agencies to Russian interference

Latvian intelligence authorities consider Russia to be the most significant threat to the country’s security. The content of Latvia’s important security policy documents and reports is predominantly about Russia, whose actions are considered to be harmful towards Latvia. These documents show not only how serious a threat Russia is to Latvia but also how well-aware Latvia is of that situation and that it is prepared to work towards being able to effectively counter it.

Activities of the non-governmental sector

As far as analysing Russian disinformation campaigns is concerned, Sandra Veinberg, a Latvian journalist working in Sweden, is an important and active voice who works extensively on disinformation in the media. Latvia-based Re:Baltica, the Baltic Center for Investigative Journalism, also plays a significant role in battling fake news and Russian propaganda, while the Pietek.com portal engages in debunking disinformation and concentrates on both domestic and foreign politics and on Russian propaganda in the Latvian media landscape. Also of significant relevance is the work of blogger Jānis Polis, who conducted a thorough study on Russian disinformation campaigns and whose activities even received praise from the Latvian Minister of Foreign Affairs, Edgars Rinkēvičs.

Regarding institutions dealing with media literacy in Latvia, the private university TURIBA based in Riga offers programmes focused on this issue. Also worthwhile is MansMedijs, a “media portal for students, professionals and users”, and another portal run by the Latvian Mediju institūts and the European Journalism Observatory.

See [http://lv.ejo-online.eu/observatoriju/mediju-instituts](http://lv.ejo-online.eu/observatoriju/mediju-instituts)
XVII. Lithuania

Summary

- Within the EU, Lithuania is at the forefront of efforts to counter Russian disinformation and other forms of aggression and hostile influence
- Given its strategic location bordering both Russia and Belarus, Lithuania has been a frequent target of Russian military intimidation
- Lithuania supports a stronger EU/NATO response to Russian aggression as well as increased aid to Ukraine

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.224

Like its two Baltic neighbours, Lithuania was one of the few ex-Soviet states to join the EU and NATO in 2004. Lithuania’s strategic location between the Russian enclave of Kaliningrad and the Republic of Belarus contributes to its acute awareness of threats posed by the Russian military. Moreover, Russian spy networks remain heavily active in Lithuania, although its Russian minority (at only 6%) is considerably smaller than that of Latvia or Estonia. Lithuania stands in the avant-garde of EU and NATO states in raising awareness about the Russian threat, while also rapidly implementing measures to lower national dependence on Russian energy supplies. Lithuania has been one of the chief advocates for an EU treaty with Ukraine, and the annexation of Crimea only intensified its concern and preparation for a potential hybrid attack by Russia. Lithuania is highly supportive of the EU sanctions regime and eager to aid Ukraine. Overall, Lithuania shares frosty political relations with Russia, and maintains a strong internal political and social consensus on mitigating Russian aggression and on related security issues.

Political acknowledgement of the threat

Within the EU, Lithuania is one of the states at the forefront of the fight to counter Russian disinformation and other hostile influence operations. Given its geographic proximity to Russia and strategic location between Kaliningrad and Belarus, Lithuania has acute security concerns about a Russian military

---

offensive, similar to that in Ukraine. Indeed, recent years have witnessed a number of military incidents in the region (primarily violations of Lithuanian airspace and threatening narratives). Even prior to the onset of the war in Ukraine, Lithuania sought to raise awareness of the Russian threat with both NATO and the EU, together with its Baltic neighbours. Now, it is a European leader in terms of education and strategy development to counter Russian aggression.

Government activities against Russian influence & disinformation

Russia’s disinformation campaign has also led to Lithuania’s prioritisation of information and cyber security issues. The Lithuanian Foreign Ministry has established a Strategic Communication Group that publishes a regular newsletter (Lithuanian Diplomatic Playbook, Weekly News from Lithuania) and maintains an active social media presence. Indeed, concerns about Russian aggression, disinformation, and other hostile influence feature prominently at every level of society, including politics, academia, and the public sphere. The Ministry of National Defence has even published several manuals on resisting Russian invasion. On one occasion, the Lithuanian radio and television commission suspended the Russian state-owned broadcaster VGTRK after strong anti-U.S. comments. Vladimir Zhirinovsky, a member of the Russian Duma, stated that if U.S. troops move near Russia’s borders, “they will burn down with the crew.” Lithuanian regulators considered this statement to be “an incitement to war, discord and hatred” and suspended VGTRK for three months.

Furthermore, Lithuania has requested an increased NATO presence (receiving a German-led battle group of 1000 troops) and increased its military spending by 50%. Significant security assistance also comes from the permanent presence of the United States and its sophisticated surveillance technology. Lithuania has also announced a plan to invest millions in missile defence systems that would fill a defence gap on the border with Russia.

Lithuania is a sponsoring nation of the NATO STRATCOM COE and has a seconded-national expert working on the EEAS East STRATCOM team. It is also a participant in the Finnish COE on Countering Hybrid Threats. In sum, Lithuania is at the forefront of European efforts to counter Russia’s disinformation campaign and other forms of subversive influence.

---

225See [https://twitter.com/LT_MFA_Stratcom?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor](https://twitter.com/LT_MFA_Stratcom?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)
The approach of intelligence agencies to Russian interference

Russian spies are thought to be the most active foreign agents operating in Lithuania. In 2014, Lithuania expelled three Russian intelligence officers operating under diplomatic cover and several diplomats had to leave their office before the expiration of their accreditation. Ten Russian intelligence officers operating under an unofficial cover were exchanged for individuals accused of collaboration with Western security services in Russia. Russia has also been accused of bugging the phone calls of Lithuanian diplomats. On multiple occasions since 2015, Russian spyware has been discovered on government computers, followed by attempts to hack and infect devices with malware. In addition, a NATO air base and intelligence sharing hub in the city of Siauliai was infiltrated by an alleged Russian spy ring. The Lithuanian State Security Department has launched a television advertisement urging the public to be wary of strangers and to call a new ‘spyline’ to check that they have not unintentionally being lured into espionage.

Activities of the non-governmental sector

A number of NGOs, foundations, and think tanks are involved in strengthening Lithuanian and regional civil society through promoting Western values and developing new defence strategies. Some of the more prominent include: the Eastern European Studies Centre (EESC), the National Defence Foundation, and the Institute of International Relations and Political Science (IIRPS). Lithuania also has concerns about the impact of Russian state propaganda on its Russian minority. Consequently, Lithuanian elites and NGOs have jointly launched projects to promote more accurate information for this minority.

---


XVIII. Luxembourg

**Political acknowledgment**

[ ] [ ] [ ] [ ] [ ]

**Government activities**

[ ] [ ] [ ] [ ] [ ]

**Intelligence services approach**

[ ] [ ] [ ] [ ] [ ]

**Summary**

- Luxembourg has close economic and financial ties to Russia, and is therefore reluctant to alienate Russia with punitive measures
- Luxembourg does not consider Russian disinformation or hostile influence operations to be a security threat
- No relevant initiatives addressing the disinformation threat exist at either the state, counterintelligence, or non-governmental level

**Relations with the Russian Federation**

**Description:** Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of any threat.235

Luxembourg is one of the founding NATO and EU nations, and one of the three Benelux states. Reputed primarily as a tax haven and banking hub, Luxembourg is a small and militarily insignificant country whose primary source of economic prosperity derives from its financial services. Due to high levels of investment from Russia (and vice versa), Lithuania is reluctant to implement EU measures aimed at restricting shady financials from Russia. However, although Luxembourg relies heavily on Russian financing, it supports common EU policies designed to penalise Russia for violating international law. Luxembourgian officials have also expressed hope that peace in Ukraine is attainable, and that Russia and Ukraine will reach compromise over their disagreements. According to the latest Eurobarometer, 21% in Luxembourg had a positive view of Russia.

**Political acknowledgement of the threat**

Luxembourg has thus far been slow in addressing the threat of Russian disinformation and other hostile influence in Europe. Luxembourg continues to see Russia as an important strategic partner and therefore takes a softer approach to the question of punitive measures. Although Russia’s violations of international law and the annexation of Crimea were strongly condemned by Luxembourg, there is

---

growing opposition to economic sanctions on grounds that they have proven inefficient in achieving their intended goals. In 2015, Foreign Affairs Minister Jean Asselborn declared in a parliamentary statement that lasting international isolation of Russia would be counterproductive, and that sanctions cannot be a solution to the Ukrainian conflict. "We must create a new basis of cooperation with Russia to keep peace and a certain level of normality," he said.\(^{236}\)

**Government activities against Russian influence & disinformation**

Given the lack of Political acknowledgement of the threat, it is unsurprising that no concerted state action has been undertaken to raise awareness of or counter Russian disinformation or other hostile influence operations. Although Luxembourg stays in line with EU and NATO policy, the Duchy would like to see normalisation of relations with Russia. It does not consider Russian disinformation and hostile influence to be a serious danger, and is currently not pursuing any state-level strategy to mitigate the threat.

**The approach of intelligence agencies to Russian interference**

There are no relevant counterintelligence activities or documents publicly detailing an official position on Russian disinformation or subversive influence. However, given the prominence and value of its financial sector, Luxembourg is particularly concerned with cybersecurity, and has a detailed national cybersecurity strategy.\(^{237}\)

**Activities of the non-governmental sector**

There are no relevant non-governmental initiatives concerned with disinformation or media literacy.

---

XX. Malta

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Malta showed that it takes cybersecurity seriously when it published its Cyber Security Strategy in 2016
- Neither the government nor civil society pursue any specific policies aimed at countering disinformation campaigns

Relations with the Russian Federation

Description: No relations with Russia. These countries are geographically distant from Russia and have almost no interest in any of the relevant issues.  

Malta is a small country dependent on oil imports, of which Russia takes the biggest share. Malta’s relations with Russia are insignificant. The Maltese government emphasises the EU’s mediating role in the Ukraine crisis.

Political acknowledgement of the threat

Being a state without significant relations or problems with Russia, the issue of Russian disinformation is not high on Maltese agenda.

Government activities against Russian influence & disinformation

Malta does not actively engage in dealing with this issue either at home or on the international stage. Nevertheless, the topic of cybersecurity is taken seriously in Malta, with its Cyber Security Strategy being published by the Ministry for Competitiveness and Digital, Maritime and Services Economy in 2016.

---


239 Ibid.

Counter-intelligence activities

There are no publicly known policies aimed specifically at countering disinformation or propaganda in Malta, however, as far as cyber defence is concerned, the country is operating under its new Cyber Security Strategy.

The approach of intelligence agencies to Russian interference

There are no known non-governmental organisations or institutions which would noticeably engage in the topic of Russian disinformation and influence operations. Nevertheless, there are several projects on Malta aimed at improving media literacy. The Centre for Literacy is involved in policy advice, consulting, and training for different educational and professional bodies. The eSkills Malta Foundation is a collation of various representatives from the government, industry, and education who are working towards a digitally enabled knowledge economy in Malta. The Be Smart Online! project focuses on education in order to ensure a safer online experience for children.241

XX. The Netherlands

### Political acknowledgment

- [ ]

### Government activities

- [ ]

### Intelligence services approach

- [ ]

**Summary**

- The issue of Russian subversion does not generally concern the Netherlands
- The Netherlands show some examples of counter-disinformation measures; however, it is difficult to say whether the government has the same level of awareness for disinformation threats from state actors as it does for propaganda by ISIS/Daesh and other religious extremist groups

**Relations with the Russian Federation**

**Description: The awakened.** These countries have significantly updated their policies and concerns following Russian aggression in Ukraine.\(^{242}\)

The Netherlands are generally too distant from Russia to concern themselves with the issue of immediate Russian threats. Thus far, the major dimension of Russo-Dutch relations has been economic. However, the downing of Flight MH17 from Amsterdam and Russian behavior in the ensuing investigation worsened the two countries’ relations. Though it is one of the more Eurosceptic Western European nations, the Netherlands did raise concerns that Russia’s behavior threatens international order and the integrity of the EU. This has led to the Dutch becoming more aware of and concerned by Russian threats, both military and ‘hybrid’. Furthermore, the Netherlands are hesitant but generally supportive of the common EU stance on Russia, even though the Dutch still believe that political reforms and democratic transformations in Russia are possible in the future.

**Political acknowledgement of the threat**

Prime Minister Mark Rutte called on Russia to stop spreading unsubstantiated rumours and disinformation about the MH17 flight, downed by pro-Russian separatists in Eastern Ukraine in 2014, and further highlighted the Russians’ refusal to co-operate in the investigation.\(^{243}\)

The Kingdom’s Foreign Minister Bert Koenders has noted that the Dutch government is highly aware of the threat posed by Russia, and during a trip to the US was tasked with obtaining more information on

---


this threat from the US. Koenders was also among the politicians who warned of Russian meddling in the 2017 Dutch elections. Furthermore, Koenders voiced his criticism of Russia’s refusal to accept the MH17 report’s conclusions, after Russia’s foreign ministry called them “biased” and “politically motivated”.

Dutch MP Kees Verhoeven (of the Democrats 66 party) commented that the failure of the EU-Ukraine association referendum in the Netherlands may have been influenced by Russia. Otherwise, however, there was hardly any government reaction to the spreading of Russian disinformation during the referendum.

**Government activities against Russian influence & disinformation**

Prior to the parliamentary elections in March 2017, the Dutch government ordered that votes should be counted by hand rather than software as it was previously done, stating fears of Russian hackers’ manipulation of the electoral outcome as a primary reason.

The Dutch government is involved in funding the International Visegrad Fund (IVF) whose tasks, among other things, involve combatting Russian disinformation in Europe. It is also a sponsoring nation of the NATO STRATCOM COE in Riga.

**The approach of intelligence agencies to Russian interference**

The General Intelligence and Security Service (AIVD) is the Dutch secret service. In its 2016 annual report it mentioned Russia using Cold War-era tactics to exert its influence on democratic Western societies. The kingdom’s cybersecurity lies in the domain of the National Cyber Security Centre under the Ministry of Security and Justice. On the eve of the March 2017 parliamentary elections, it was noted that the Netherlands still lack a resilient cyber defence structure and capacity, which may pose a risk for Dutch democracy, as the right-wing Party for Freedom (PVV) was expected to increase its

---


249 See <http://visegradfund.org/about/>


251 See <https://www.ncsc.nl/english/organisation>
number of seats in the Kingdom’s House of Representatives. Moreover, prior to the elections, Russian hackers tried to hack government employees’ email accounts, including one belonging to the head of the AIVD, Rob Bertholee.

**Activities of the non-governmental sector**

The Netherlands Atlantic Association (Atlantische Komissie) is one of the oldest Dutch NGOs and is tasked with analysing key issues surrounding NATO and trans-Atlantic relations. In particular, it publishes a subscription-funded journal called Atlantisch Perspectief in Dutch and English, and covers topics related, among other things, to the problem of Russia’s activities in the EU and NATO, and along their borders.

The Hague Centre for Strategic Studies (HCSS) is an organisation providing analysis and data on important issues relating to security issues in Europe and around the world. In March 2017, the Centre published a paper (in Dutch) on the impact of Russian disinformation efforts in Europe so far, which were relevant in the wake of the French presidential elections.

DROG is an experiment created by Ruurd Oosterwoud to test media literacy and combat disinformation and fake news online, supported by the public SVDJ fund, tasked with aiding journalists in the Kingdom.

During the Dutch parliamentary election campaign, several experts in cybersecurity warned the Kingdom’s political parties that they are vulnerable to hacking. Hacker Sijmen Ruwhof said that some of the parties’ websites did not have sufficient security measures installed for over a year. Individual citizens and IT security experts have been raising alarms over the Dutch political sector’s vulnerability in the cybersecurity sphere for at least 11 years now.

---


254 See [https://www.atlcom.nl/english/organization/](https://www.atlcom.nl/english/organization/)

255 See [https://www.atlcom.nl/media/atlantisch-perspectief/15297/](https://www.atlcom.nl/media/atlantisch-perspectief/15297/)

256 See [https://www.atlcom.nl/english/atlantischperspectief1/](https://www.atlcom.nl/english/atlantischperspectief1/)


258 See [http://wijzijndrog.nl](http://wijzijndrog.nl)

259 See [https://www.svdj.nl/over-ons/](https://www.svdj.nl/over-ons/)


261 Cerulus (2017).
XXI. Poland

Summary

- Poland considers cooperation between NATO and the EU its priority, and actively engages in activities of both organisations and seeks their assistance, including in the area of subversive influence of foreign actors.
- The country has two STRATCOM units within relevant departments, but its policy to counter influence operations lacks conceptualisation.
- Polish intelligence services are well aware of Russian attempts to spread its influence.

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.262

Although Poland was a part of the Eastern bloc for a long time, it does not hold a lot of sympathies towards the Russian Federation. The Soviet invasion of Poland in 1939 and the Katyn Massacre in 1940 left deep scars in the common history of Poland and the Russian Federation. The chilly relations with the Kremlin were later underscored by the death of former Polish President Lech Kaczyński and other Polish high officials in a plane crash in Smolensk in 2010. They deteriorated further yet after the annexation of Crimea.263 The Polish government has shown full support for sanctions against Russia. Its wariness of Russia is heightened due to a shared border with the Kaliningrad Oblast. Because of security concerns caused by being at the frontier, Poland requested an increased NATO presence and increased its military spending from 1.6% GDP in 2013 to 2.2% in 2015. US forces are deployed in the country as a deterrent, which the Kremlin perceives as an aggression and threat.


Political acknowledgement of the threat

According to the annual address on foreign policy goals from 2016, Poland acknowledges that Russia seeks to expand its sphere of influence and inhibit democratic transition of Eastern Europe by means of hybrid activities, including propaganda. Through the address, Poland also calls for enhancement of NATO-EU cooperation in the field of countering disinformation and influence operations and increasing cybersecurity.

Government activities against Russian influence & disinformation

Russian threats have not yet been described in any specific conceptual document or translated into a sophisticated counter-policy. However, there are two STRATCOM departments: at the Ministry of National Defence and at the Ministry of the Interior.

Poland is a sponsoring nation of the NATO STRATCOM COE and also participates on the Finnish COE on Countering Hybrid Threats. It is also one of the funding nations of the European Endowment for Democracy, a donor organisation supporting democratisation and resilience of societies in the European neighbourhood, including the area of counter-disinformation efforts. Anna Fotyga from the Law and Justice Party, a Polish MEP and a former minister of foreign affairs, was a rapporteur for the report on EU strategic communication to counteract propaganda against it by third parties in October 2016. Otherwise, Poland is not very active in the projects aimed at countering disinformation on the EU level.

The approach of intelligence agencies to Russian interference

The Internal Security Agency issued an activity report for the year 2014 where it reaffirmed a high level of activity of Russian intelligence services in Poland. The Russian spy network in Poland is quite extensive, including spies under diplomatic cover, which is why several Russian diplomats were expelled on suspicion of spying in recent years. For example, the former Russian military attaché in Poland, Eduard Shishmakov, was expelled for espionage; he is also currently accused of participating in the plot in Montenegro.

According to the report, the aim of Russian influence operations was to discredit the position of Poland and other NATO member states in the Ukraine crisis, to bring attention to the complex history of relations between Poland and Ukraine in order to cause antagonism between their societies, and to create and highlight divisions among EU and NATO members. For the implementation of such strategies, the Kremlin primarily used the media, but some citizens also represented the pro-Russian stance and, in


265 See <https://www.democracyendowment.eu/about-eed/>


some cases, turned out to be paid by the Russian Federation. There have been cases of Russian media spreading anti-EU and anti-American messages, especially by Eurosceptic politicians and other public personalities speaking against further sanctions and tougher policy on Russia.

The report summarises the activities of the Russian intelligence services in Poland as actively gathering information about political, economic, as well as scientific and technical character. Their activities also included lobbying for Russian entities operating on the Polish market.

The information war conducted by the Russian Federation is described in the report as an attempt to spread pro-Russian and anti-Ukrainian views among the Polish public through internet blogs, portals, and news services. The documents describe the activities of paid internet trolls as well as so-called ‘useful idiots’.

**Activities of the non-governmental sector**

There are two main non-governmental organisations which are focusing on relations with Russia and its policies. The Center for Eastern Studies (OSW) is one of the most prominent think tanks in Central and Eastern Europe. It conducts research and publishes studies and reports on the topic of socio-political process in Russia, Central and Eastern Europe, but also on Russian influence in the region.

The Foundation for Joint Europe, established in 2010, is a project of young experts from Eastern Europe. It is behind the Eastook.eu portal, a website with daily updates about the situation in Eastern European countries in cooperation with local politicians, journalists, and activists. The authors support the freedom of speech and highlight the necessity of accurate information about the events happening in the Eastern neighbourhood.

There are other institutions, namely the Center for International Relations and the Casimis Pulaski Foundation, which dedicate their work to the topic of Russian influence in the broader context of foreign and security policy issues.

Another notable activity is a Facebook page called “Russian fifth column in Poland”, run by journalist Marcin Rey. He uses this platform to publish materials on the activities of Polish nationalists with Russian connections.268 Also, the New Eastern Europe magazine, based in Kraków, focuses on the affairs of countries formerly under the influence of the Soviet Union.

Media literacy is mostly promoted in the academic sphere. There is also a Media Education programme in place, supporting media education classes at schools from kindergarten to secondary levels, community centres, and libraries, including providing lesson plans, exercises, and teaching materials.

XXII. Portugal

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Portugal is generally unconcerned with Russia, and remains outside of immediate Russian interests
- The government has developed a few media education policies, but these suffer from a lack of consistency and resources

Relations with the Russian Federation

Description: No relations with Russia. These countries are geographically distant from Russia and have almost no interest in any of the relevant issues.269

Portugal is a founding NATO member state and one of the westernmost EU member states. The country’s geographic distance from Russia makes it generally less aware of the issues at the EU’s eastern borders. It is generally independent from Russian fossil fuels. Portugal is mostly unconcerned with Russia and remains outside of immediate Russian interests as well.270

Political acknowledgement of the threat

Russian subversion operations do not pose a visible threat to Portugal. As a result, this topic is not of much relevance for the Portuguese.

Government activities against Russian influence & disinformation

Besides cooperation at the EU and NATO level, the Portuguese government currently does not show any activity regarding this issue.

The state is more active as far as media literacy is concerned and has developed a few media education policies; however, these suffer from a lack of consistency and a shortage of resources to be put effectively into practice.271

---

270 Ibid.
Given Portugal’s disinterest in the topic of Russian disinformation and influence operations, neither excessive activity nor obstructions are to be expected from the country. As for media literacy, academia and associations of civil society have played a very important role in promoting media education in Portugal and bringing the topic to the public agenda.\(^{272}\)

**The approach of intelligence agencies to Russian interference**

It is not known that the Portuguese intelligence agencies would occupy themselves extensively with the issue of Russia; however, a Portuguese spy was once caught selling secret NATO documents to a Russian handler.\(^{273}\)

**Activities of the non-governmental sector**

There are currently no known initiatives in Portugal focusing on the issue of Russian disinformation campaigns.

\(^{272}\) Ibid.

XXIII. Romania

Summary

- Romania has long had tense relations with Russia, which have deteriorated further since the start of the Ukraine crisis
- Romania explicitly identifies Russia as a threat to its national security in the realms of information warfare, cyberattacks, and other hybrid tactics
- Despite this acknowledgement, Romania’s strategic capabilities with respect to these threats are still relatively underdeveloped

Relations with the Russian Federation

Description: Below-radar supporter. These countries harbour concerns about Russia, but given complicated historical relations and local context, typically stay away from vocal criticism of Russian aggression.

Romania has been an EU and NATO member state since 2004. The country’s high domestic fossil fuel reserves make the question of energy secondary in Romania’s relations with Russia. Romania’s primary concern is with its immediate neighbourhood. It was supportive of pro-EU and pro-NATO measures in Georgia, and with forming a common Black Sea partnership within Europe. Moldova, Transnistria, and EU expansion are the defining issues of Romanian foreign policy. As Chisinau’s foremost advocate in Europe, Romania’s interests in Moldova’s accession to the EU have clashed with Russia’s desire to maintain the frozen conflict in Transnistria. Romania remains dedicated to deeper ties with the US and NATO, as well as with its Black Sea partners, such as Georgia and Ukraine. According to Eurobarometer, 53% of Romanians have a positive view of Russia, while 41% have a negative view.

Political acknowledgement of the threat

Romania’s complicated history with Russia, particularly concerning Moldova and Transnistria, has long fuelled Romanian suspicion of Russia. The onset of the crisis in Ukraine in 2013 only exacerbated these concerns. Today, Romania openly acknowledges the threat of Russian disinformation and subversive

---


efforts both to its own national security as well as to Europe at large – a stance that is increasingly reflected in government documents and official statements.

**Government activities against Russian influence & disinformation**

Despite overt political acknowledgement of the Russian threat, Romania’s response strategy is still nascent and relatively underdeveloped by comparison to other EU states like the Baltics and the Czech Republic. So far, these concerns have entered official government strategy documents, but have not been effectively put into practice. For example, the Romanian National Defence Strategy for 2015-2019 explicitly identifies Russia as a threat to Romanian and European security; *inter alia*, it recognises the danger of “hostile informational actions, which trigger the development of some support points on national territory, especially with an influential purpose”.276 In an implicit reference to Russian destabilisation efforts, the strategy report also names “cyber threats initiated by hostile entities, state or non-state” and the “perpetuation of the frozen conflicts in the Black Sea Region and instability in the Western Balkans” as crucial security issues for Romania.

Likewise, the 2016 Military Strategy of Romania names hybrid warfare, intelligence operations, and cyberattacks in its list of potential military risks and threats.277 According to the Centre for European Policy Analysis (CEPA), the new Romanian National Defence Strategy “makes quite clear that Russia’s illegal annexation of Crimea and Russian actions in the Black Sea region deeply affect the regional security environment”, which “is an important and novel element” of Romania’s defence orientation.278 While Romania’s 2010 strategy “mentioned the Georgian-Russian conflict as a destabilising factor […] it saw the main security challenges as coming from military conflicts outside the European continent, terrorism and weapons proliferation. Now […] the identified threats to Romania’s security derive from the changed security environment both inside and outside its borders: frozen conflicts and destabilising actions (by Russia) in Romania’s immediate vicinity, cyber threats and informational hostilities.”279

The Romanian Ministry of Foreign Affairs is also committed to the mission of the EEAS East STRATCOM Task Force and NATO STRATCOM COE.

**The approach of intelligence agencies to Russian interference**

Romania’s National Defence Strategy for 2015-2019 outlines intelligence and counterintelligence priorities. With respect to Russian disinformation and aggression, these include: “ensuring mechanisms to prevent and counteract cyber attacks […]; identifying and counteracting asymmetric and hybrid

---


actions; [...] knowing, preventing and eliminating risks and threats generated by hostile intelligence actions [...].”

Activities of the non-governmental sector

Currently, there is still a limited number of non-governmental initiatives in Romania concerned with addressing the impact of Russian disinformation and other hostile influence operations. Two stand out in particular: the Center for Conflict Prevention and Early Warning, an NGO focused on research in conflict analysis and crisis decision-making in the post-Soviet space, and the Eurisc Foundation, an NGO dedicated to the study of issues related to risk, security, and communication, “focusing on nonmilitary risks, security culture in relation to Romania’s European and Euro-Atlantic integration processes (EU and NATO), and civil-military relations”.

---


281 See <http://cpc-ew.ro/>

282 See <http://www.nira.or.jp/past/ice/nwdtt/2005/DAT/1265.html>
XXIV. Slovakia

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Slovak political representation is in a state of denial concerning Russian disinformation and influence operations, with the exception of President Andrej Kiska
- Civil society in Slovakia is very active, trying to raise public awareness and enhance education and media literacy amongst the youth
- The activities targeting the spread of Russian influence are interconnected with preventing radicalisation

Relations with the Russian Federation

Description: Government using Russia-card for domestic reasons. While these countries have predominantly negative historical experience with Russia, the government uses relations with Moscow for domestic political and/or economic reasons, or as a tool against the EU establishment.283 Slovakia belongs to the group of countries that were formerly part of the Eastern bloc and had negative historical experience with the Russian Federation. It is a firm supporter of the counter-measures against Russia taken by the EU and NATO after the annexation of Crimea. However, energy dependence and economic ties with Russia lead to occasional capitulation on the Slovak side, for example in the case of the deployment of the US missile shield. Hence, Slovakia remains one of the most pro-Russian countries in the EU.284 There are also pro-Russian fringe elements present in Slovak politics, such as ex-Communist politicians who continue to harbour sympathies for Russia.285

Political acknowledgement of the threat

In its strategic documents, the Slovak government highlights the necessity of maintaining pragmatic relations with Russia, although most of these documents have not been updated in recent years. The

---


existing Security Strategy, issued in 2005, mostly focuses on terrorism, though a new version should be completed in 2017. Slovakia considers support of a comprehensive approach and wider cooperation between the EU and NATO in cyber defence and countering disinformation as one of its foreign policy goals.  

**Government activities against Russian influence & disinformation**

Slovak political representatives generally do not consider disinformation campaigns a priority issue and do not actively try to develop state counter-measures. An exception is Slovak President Andrej Kiska who publicly proclaimed on 17 March 2017, “Slovakia is a target of information war and propaganda and Slovak security services are doing next to nothing to counter it”. There are no activities on the state level dedicated to strategic communication or any type of counter-measures to disinformation campaigns and influence operations.  

Slovakia does not actively participate in efforts to counter disinformation at the international level. The Slovak President warned against the danger of spreading disinformation in 2015 during a meeting with the NATO General Secretary Jens Stoltenberg. However, the Prime Minister and the rest of the political leadership do not consider the threat of Russian influence a priority.

**The approach of intelligence agencies to Russian interference**

The Slovak Intelligence Service (SIS) published an annual report for 2015 in which it dedicates no more than one sentence to the topic of subversive foreign influence. Foreign propaganda is mentioned in the 2015 annual report of the Slovak Military Intelligence Services, but does not name specific actors perpetrating these activities.

**Activities of the non-governmental sector**

Civil society in Slovakia is, unlike the political representation, a strong player in countering disinformation campaigns. There is a great number of individuals and organisations trying to tackle the challenges of manipulative and disinforming media, radicalisation and extremism (especially amongst the youth), and media literacy and education. Most of these groups and individuals are informally associated with a platform for stakeholders like journalists, NGOs, and government specialists called the Slovak Forum against Propaganda.

One of the most successful civic projects, Konspiratori.sk, was launched by the company Net Success. They created a database of dubious websites with false, conspiratorial, or propaganda content. The

---

288 Milo & Klingová (2017).  
289 Ibid.
sources in the database are evaluated by an independent committee. They cooperate with over 1,400 Slovakian companies which take down their advertisements from the outlets in the database and therefore refuse to support authors of these websites financially.

Another strong actor on the non-governmental front is the Globsec Policy Institute, organiser of the yearly GLOBSEC Bratislava Global Security Forum, which conducts analyses and studies of disinformation campaigns and Russian influence operations. The Slovak Security Policy Institute focuses on research and analysis of security challenges and has established an internet portal dedicated to cyber security (CyberSec.sk). It also runs the page Antipropaganda.sk where it debunks myths about foreign and security policy.

The Slovak Foreign Policy Association, established in 1993, serves as an open non-partisan discussion forum for international and foreign policy issues and also focuses on the topic of disinformation. There is also a number of individuals trying to raise public awareness and point out disinformation projects. Their outputs are often published in a special online section of a Slovak daily, Denník N, called “Disinformation Hoaxes Propaganda”.

There are also initiatives to enhance media literacy, creating educational materials for students and teaching them how to distinguish disinformation from serious news. The Media Literacy Centre, established in 2010 by the Faculty of Mass Media Communication at the University of Ss. Cyril and Methodius in Trnava, includes several research activities and its main output is the information interface medialnavychova.sk. The Faculty also provides accredited bachelor and masters study programs in applied media studies, which focus on preparing specialists for the field of developing media literacy, new media and media platforms, and programs used in education.²⁹⁰

XXV. Slovenia

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Slovenia acknowledges the existence of hypothetical disinformation campaigns and influence operations in general, but does not attribute them to any specific actor, nor does it consider them a threat.
- Civil society does not dedicate its resources to these issues either, except for projects targeting media literacy.

Relations with the Russian Federation

Description: Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of any threat.²⁹¹

After the annexation of Crimea, Slovenia fully supported Ukrainian integrity and fulfilment of the Minsk agreements, but it has also maintained pragmatic energy-focused economic ties with Russia. For this reason, Slovenia supports lifting the sanctions against the Russian Federation. Slovenes lack negative historical experience with Russian occupation; on the contrary, they have a certain sense of shared Slavic identity and an appreciation for the contribution of the Red Army in liberating part of Slovenia in WWII. Therefore, Slovenian politicians stress “mutual respect for different opinions” in relations with Russia. The Presidents and Prime Ministers of the two countries meet regularly.

Political acknowledgement of the threat

In its strategic documents, Slovenia states that encouragement of EU-Russia cooperation is one of its priorities, especially on an economical level. Any kind of Russian influence is not perceived or acknowledged as a threat to the country. In the National Security Strategy from 2010,²⁹² Slovenia mentions hybrid warfare, including criminal and other irregular forms of warfare, information technologies, and various economic resources as a new type of security threat for the future. However,


these threats are mentioned regarding mostly non-state or transnational actors and as a danger connected to participation in international operations and missions.

**Government activities against Russian influence & disinformation**

The Defence Committee of the Slovenian Parliament established in November 2016 that Slovenia is under no form of security threat, although an increase was noted when it comes to "hybrid warfare threats from Russia". Internationally, Slovenia follows the development of responses to hybrid threats. No measures at the state or international level have been taken.

**The approach of intelligence agencies to Russian interference**

There are no known statements or proclamations of the Slovenian intelligence services that would suggest they are aware of the issue of subversive influence, consider it a threat, or are conducting any activities to counter it.

**Activities of the non-governmental sector**

The non-governmental sector in Slovenia is not dedicated to analysing or countering disinformation operations either. Slovenian universities are active in the field of media literacy. They organise courses for students in primary and secondary schools as well as for the wider public. The Infrastructural Programme of the Faculty for Media-Collecting, Managing and Archiving Data on Media Literacy, initiated in 2014 and funded by the Slovenian Research Agency, aims at analysing trends and indicators about media literacy in Slovenia over a longer period of time. The project launched a web portal, pisemnost.si, listing activities and resources concerning media literacy in Slovenia and in the EU, as well as organising events, workshops and trainings.

The European Institute for Communication and Culture, a non-profit organisation registered under Slovene law, conducts research in the area of mass communication and media studies and is particularly concerned with the intersection of mass media and issues of democracy and democratisation.

---

293 "Defence Committee Sees No Direct Threat to Slovenia, Notes Hybrid Warfare". *STA.si*. 8 November 2016.  

294 Priorities of the Republic of Slovenia for the 71st Session of the UN General Assembly. *Ministry of Foreign Affairs, Republic of Slovenia*.  

XXVI. Spain

Political acknowledgment

Government activities

Intelligence services approach

Summary

- Spain is actively engaged in countering ISIS/Daesh propaganda; however, the Russian Federation is not high on the Spanish security agenda due to limited Russian influence in Spain and the decent, though not significant, relations between the two countries
- There has been a slight shift in the statements of the Spanish government's representatives regarding Russia, but no specific measures have been taken
- The country has a Strategic Communication Plan, but its content is classified

Relations with the Russian Federation

Description: Trying to stay away from the issues. These countries have historical, energy-related, or economically preferential relations with Russia. They do not feel threatened by Russia and, excepting the conflict in Ukraine, do not acknowledge the existence of any threat.296

Spain is an EU and NATO member state located in the westernmost part of Europe. Being located far away from Russia and not affected by the same fears as the easternmost EU member states, Spain remains focused on engaging in dialogue with Russia. This, however, does not negate Spain’s concern with Russian military build-up and Russia’s actions in Ukraine. At the same time, Spain remains sceptical about possible European expansion, and Russia’s status as a strategic partner in the fight against terrorism has marked Spain’s attitude of hesitance in making strong moves to counter perceived Russian threats. However, this is more a sign of the lack of any serious ties with Russia rather than Spanish attempts to oppose other EU member states who have real concerns about Russian threats. Economy-wise, Russia does not play a significant role in Spanish energy imports, but Russian tourism plays a big role in the Spanish economy. Thus, Spain was one of the several countries to voice criticism against anti-Russian sanctions, but so far, Spain has joined other EU nations in supporting Ukraine’s territorial integrity.297

297 Ibid.
Political acknowledgement of the threat

Overall, Russian disinformation and influence operations are not high on the Spanish agenda. One reason for this is that there are few signs of Russian influence in Spain, as opposed to some other European countries. Another reason is that Spain is very actively engaged in countering propaganda spread by ISIS/Daesh, which Spain considers to be a significantly more serious threat than that posed by Russia.

Nevertheless, Spain has become more aware of the Russian threat after the Spanish Army participated in a 2015 NATO exercise in the Baltics, where it experienced the spreading of Russian disinformation targeted against the Spanish Army and efforts to directly influence Spanish journalists. It is thus possible to observe a slight shift in the statements of the Spanish government’s representatives regarding Russia. The current Minister of Foreign Affairs Alfonso Dastis has said that Spain needs to be aware of threats coming from Russia (such as cyber attacks or Russian propaganda in European countries) but that Russia is still a key player and partner of Spain. As a result, no concrete steps or measures have been undertaken or planned so far.

Representatives of the Ministry of Defence/the Defence Staff consider Russian propaganda to be a threat, though not a significant one, which should be dealt with by implementing measures in strategic communication.

Government activities against Russian influence & disinformation

Spain has a Strategic Communication Plan, although it is classified. It is expected that the Department for Strategic Communication under the Ministry of Defence will be boosted, in connection with the presence of Spanish troops in Eastern Europe within the engagement of NATO. Spain also has its own Cyber Security Strategy.298

The Spanish government fully supports activities at the EU and NATO level regarding the threat posed by Russia, although it does not actively engage in countering it. As stated previously, Spain is far more concerned with the threat of Islamic extremism and terrorism; therefore, it is more interested in international cooperation in connection with that issue. Concerning Spain’s military involvement, the country is providing forces for a NATO unit in Latvia.299

The approach of intelligence agencies to Russian interference

A few alleged Russian hackers were arrested on Spanish soil, based on US warrants.300 Nevertheless, Russian secret services are active on Spanish soil and even managed to get one Spanish counter-
intelligence agent to spy for Russia.\textsuperscript{301} In general, the focus of Spanish intelligence is heavily oriented at countering terrorism.

\textbf{Activities of the non-governmental sector}

The Spanish non-governmental sector is not particularly concerned with the issue of Russia. However, some individuals do engage with it, for example Nicolás De Pedro from the Barcelona Centre for International Affairs. Strengthening media literacy is not a part of Spanish public debate. There are several fact-checking websites active in Spain, though they mostly focus only on internal political issues.

XXVII. Sweden

Political acknowledgment
- - - - - -

Government activities
- - - - - -

Intelligence services approach
- - - - - -

Summary
- Sweden’s free and independent press is one of the country’s most important assets in combatting fake news
- Swedish academia is perhaps the most visible player in analysing and combatting Russian subversive tactics
- The main focus of the government so far is on building and maintaining efficient cyber defence and counter-espionage measures

Relations with the Russian Federation

Description: The awakened. These countries have significantly updated their policies and concerns following Russian aggression in Ukraine.302

Following the annexation of Crimea in 2014, Sweden condemned Russia’s violation of Ukraine’s territorial integrity and began rethinking its own defence policy, examining the country’s strategic vulnerability after a series of Russian military probes entered Swedish waters and airspace. Sweden’s interest in Russia is primarily concerned with human rights, the economy, and energy, though the latter plays a far less significant role since Sweden’s energy imports are very diverse.

Political acknowledgement of the threat

The Prime Minister’s office publishes the annual national security strategy, with the latest one emphasising the necessity of identifying and neutralising propaganda campaigns.303 Prime Minister Stefan Löfven warned that Russia may try to undermine the upcoming Swedish elections, citing the role that Russian hackers had in the US presidential elections.304


Government activities against Russian influence & disinformation

The Swedish Civil Contingencies Agency (MSB) is the national civil defence agency under the Ministry of Defence. Amongst its primary civil defence measures, MSB has a subdivision called the National Board of Psychological Defence (SPF), tasked with educating the public about being more critical towards news, among other things.

The Swedish Defence Research Agency (FOI) is a government research institute tasked with analysing and researching issues of relevance to national defence. It highlighted the threat emanating from Russia’s militarisation. Amongst the publications of the university, there is one about developing a system to analyse and counter disinformation on Twitter.

The approach of intelligence agencies to Russian interference

The Swedish Security Service (Sapo) has warned about Russian spy activity targeting key Swedish infrastructure objects, which raised suspicion that Russian spies may have been behind a 2016 sabotage of telecommunications masts used by Swedish intelligence.

The head of the Military Intelligence and Security Service (Must). Mj. Gen. Gunnar Karlson has stated that there was a clear intent to undermine Swedish democracy in cyber-attacks that allegedly came from Russia and that included elements aimed at spreading disinformation in Sweden.

Activities of the non-governmental sector

The Swedish Defence University focuses on military and war studies, including the concepts of ‘hybrid warfare’. In 2014, it held a symposium on Russia’s ‘hybrid war’ in Ukraine. Among courses the university provides is Military Science (Krigsvetenskap), which focuses on the concept of ‘hybrid warfare’ (as of January 2017).

The Utrikespolitiska institutet (UI), or the Swedish Institute for International Affairs, is a publicly-funded institute engaged in analysing and researching topics relevant to Swedish foreign policy. Its recent
events include a ‘Gymnasium day’ lecture on disinformation (in Swedish). Other important resources are its UI Brief publications on recent important events and trends in the EU and other areas. One of the first UI Briefs looked into international supporters of Putin’s regime and the reasons why some actors in the West become Putin’s advocates. The institute has been involved in highlighting Russian disinformation against Sweden, identifying 26 fake news pieces emerging on suspicious websites, among which was a fake email that claimed to show talks between the Kingdom’s defence minister and BAE Systems Bofors.

Among the UI’s prominent researchers are Martin Kragh, one of the authors of a study on Russian attempts to influence Sweden via fake news, and Anke Schmidt-Felzmann, who publishes papers on EU-Russia relations, including a paper outlining a potential scenario of a full-scale Russian assault on Sweden.

The Internet Foundation in Sweden (IIS) has published a guide on how to be more critical about online news.

See <https://www.ui.se/evenemang/tidigare/2017/februari/gymnasiedag-desinformation-och-digitala-spar/>


XXVIII. The United Kingdom

Political acknowledgment

Government activities

Intelligence services approach

Summary

- British civil society appears resilient enough to withstand Russian threats, even though the Brexit referendum has shown that the influence of Eurosceptics and even pro-Russian sentiments in some English tabloids remains strong.

- The UK government appears to be more concerned with the diplomatic and international aspects of Russian influence rather than malign domestic effects.

Relations with the Russian Federation

Description: Principled defender. These countries hold concerned views of Russian foreign policy and are now at the forefront of the European response to Russian aggression.\(^{319}\)

The UK was quick to condemn Russia’s actions in Ukraine as well as in Syria, and its firm stance remains unchanged even after the political reshuffle following the 2016 Brexit referendum. Although Russia does not play the foremost role in British security or international policy, Britain is aware of the threats posed by Russia in Europe and the Middle East, and is an active member of NATO efforts to counter these threats.

Political acknowledgement of the threat

In the UK’s 2015 National Security Strategy, presented by the Prime Minister to the UK Parliament, Russia’s subversive tactics involving media disinformation were highlighted and condemned as contravening international norms.\(^{320}\)

Prior to the June 2017 General Election, British politicians expressed concerns that fake news may be used to undermine the public’s vote, with Conservative MP Damian Collins highlighting the problem of...


fake news being read and shared far more widely on Facebook than factual news, and urging the social media website to dedicate more effort to combatting disinformation.321

Foreign Minister Boris Johnson has warned that Russia has the capacity to undermine the political status quo in the UK through hacking,322 and has also stated that Russia’s interference in other countries’ internal affairs is unacceptable.323

**Government activities against Russian influence & disinformation**

The United Kingdom has a set of strategic communication projects focused on Central Eastern Europe and Ukraine. The government also approved increased spending on cyber defence with the budget for 2011-2016 rising to 1.9 billion pounds.324 The country has its seconded-national expert in the EEAS East STRATCOM team in Brussels and is one of the sponsoring nations of the NATO STRATCOM COE in Riga. It also participates in the Finnish COE.

**The approach of intelligence agencies to Russian interference**

British Prime Minister Theresa May has voiced concern about fake news, calling for newspapers’ responsibility in delivering factual news and combatting disinformation.325 The National Cyber Security Centre (NCSC) is a government body tasked with combatting cyber-threats. In one of its reports, the NCSC highlighted (citing the United States’ FBI) how some of the hackers behind the Yahoo email hack were members of Russia’s FSB.326 Apprehension of the said hackers was achieved through the participation of MI5 (the UK’s national counterintelligence agency) agents.327 The NCSC also warned British political parties of potential hacking by Russia.328

---


MI5 chief Andrew Parker has warned that Russia’s threat to the UK is growing, and has stated that Russia’s spy activity in the UK is extensive, as is its subversion campaign in Europe in general.\(^{329}\) MI6 (Secret Intelligence Service, the national foreign intelligence agency) chief Alex Younger has likewise highlighted the issue of subversion and the disinformation campaign waged by Russia.\(^{330}\) It was the British intelligence services that alerted the US about the Democratic National Committee hacks and the alleged Trump-Russia connection in 2015.\(^{331}\)

**Activities of the non-governmental sector**

The Henry Jackson Society is a London-based think tank that focuses on analysing issues surrounding foreign policy in the Western world.\(^{332}\) One of its early 2016 articles highlighted Russia’s role in spreading disinformation via Facebook, even though the role of social media in spreading disinformation was often overlooked by traditional media in the past.\(^{333}\)

The Institute for Statecraft launched an Integrity Initiative to combat disinformation that may undermine democracy in the West, particularly through the use and proliferation of fake materials via social media.\(^{334}\)

Facebook has warned that the June 2017 British General Election may become a subject of attack by fake news and other disinformation online, which has led Facebook staff to develop new ways of identifying and suspending suspicious accounts that may spread disinformation.\(^{335}\)

The Daily Telegraph published a fact check paper on the arguments that resulted in the Brexit vote in the 2016 referendum, showing that the primary arguments that may have cost Britain its future in the EU were based overwhelmingly on false premises.\(^{336}\) The London Economic (TLE) website has shown how Britain First and similar Facebook groups may have deliberately spread Russian-made propaganda via


\(^{332}\) See <http://henryjacksonsociety.org/about-the-society/statement-of-principles/>


\(^{334}\) See <http://www.integrityinitiative.net/about>


social media. Carole Cadwalladr has published an investigation of Cambridge Analytica, a company characterised as “a psychological warfare firm” by its former employee, and its role in the Brexit referendum, as well as its alleged ties with Russia.

UK-based analyst Ben Nimmo has published several works outlining Russian subversion techniques against Europe and ways to counter them. He also wrote about Russian disinformation surrounding the MH17 investigation and Russia’s meddling in the US presidential elections.

LSE has published a report raising alarms about weak British electoral laws which can allow foreign interference to undermine British democracy by allowing an influx of funds from unknown or suspicious sources to fund political campaigns. Peter Pomerantsev, a visiting fellow at the LSE Institute of Global Affairs, has written books and articles examining the nature of Russian disinformation campaigns.

---


343 See <http://www.lse.ac.uk/IGA/People/Visiting-Fellows/Peter-Pomerantsev.aspx>


Do you like what we do?
Support us! Our work is possible due to individual donors such as yourself.

Use the form at: http://www.europeanvalues.net/o-nas/support-us/
Or send your donation directly to our transparent account: 2300405420/2010.

© Evropské hodnoty z.s. 2017
The European Values Think-Tank is a non-governmental policy institute defending liberal democracy.

Our vision is that of a free, safe and prosperous Czech Republic within Central Europe that is an integral part of the West.

We help to face aggressive regimes, radicalisation within the society, the spread of authoritarian tendencies and extremist ideologies including Islamism.

We provide decision-makers with expert recommendations and we systematically watch and evaluate their performance. We consider active citizens, accountable politicians, political parties that fulfil their role, as well as cohesive society that shares the values of individual freedom, human dignity and equal rights to be the principle elements of a functioning liberal democracy.

Since 2005, as a non-governmental and a non-profitable organisation which is not linked to any political party, we have pursued research and educational activities. In addition to publishing analytical papers and commentaries for the media, we organise conferences, seminars and training sessions for both experts and the wider public. Our events provide a platform for dialogue amongst politicians, experts, journalists, businesspeople and students.