REPORT

RUSSIA AND CHINA THROUGH EYES OF NATO AND EU INTELLIGENCE AGENCIES

HOW DO EU MEMBER STATES’, CANADIAN AND THE UNITED STATES INTELLIGENCE AGENCIES ASSESS RUSSIAN AND CHINESE INFLUENCE ACTIVITIES?

Security Strategies Program 2019
EUROPEAN VALUES THINK-TANK
The European Values Think-Tank is a non-governmental policy institute defending liberal democracy. We
protect freedom, the democratic rule of law and the transatlantic alliance of the Czech Republic. We help
defend Europe against mass immigration, Islamic extremism and hostile influence of Russia and China. Our
vision is that of a free, safe and prosperous Czech Republic within Central Europe that is an integral part of
the transatlantic community and is based on a strong partnership with the USA.

Our work is based on individual donors. Use the form at: http://www.europeanvalues.net/o-nas/support-
us/, or send your donation directly to our transparent account: CZ69 2010 0000 0022 0125 8162.

www.europeanvalues.net              info@evropskehodnoty.cz             www.facebook.com/Evropskehodnoty

SECURITY STRATEGIES PROGRAM
A strategic program of the European Values Think-Tank which focuses mainly on security interests of the
Czech Republic in the context of Trans-Atlantic Alliance, relations with Poland and increasingly aggressive
behavior of Russia and China.

Authors
Martin Svárovský, Head of Security Strategies Program
Paula Zvejniece, Intern at Security Strategies Program
Aiden Tamasauskas, Intern at Security Strategies Program

Image Copyright:
Pages 1, 7, 13, 23: President of Russia, en.kremlin.ru

This is a joint publication of Konrad-Adenauer-Stiftung and the European Values Think-Tank. Konrad-Adenauer-Stiftung assume
no responsibility for facts or opinions expressed in this publication or any subsequent use of the information contained therein.
Sole responsibility lies on the author of the publication. The processing of the publication was concluded in 2019.
Contents

Key Findings ...................................................................................................................................................................................................................4
Introduction and Methodology ...........................................................................................................................................................................6
Groups 3 and 4: The Hesitants ............................................................................................................................................................................8
Group 2: The Acknowledgers ...........................................................................................................................................................................9
Group 1: The Most Alarmed .........................................................................................................................................................................11
Cross-Group Analysis .................................................................................................................................................................................... 14
China ............................................................................................................................................................................................................................... 18
Conclusion ................................................................................................................................................................................................................... 19
Annex 1: Source List ............................................................................................................................................................................................... 20
KEY FINDINGS

Group 1: The Most Alarmed

The Baltic states, the Czech Republic and Denmark

Intelligence services of these states identify Russian and Chinese influence strategies as the largest threat to national security

Provide far-reaching condemnations of Russian interference, but also detailed explanation of geopolitical infringement

Direct economic pressure applied by actors of Russian interest was key to the assessment of national threats

Difficult for the Czech Republic: having Russian stakeholders, engaged in illegal activities, tied up in the Czech private sector

Possible military threats: All countries surveyed (except Belgium) perceived the situation in Ukraine as one of the most significant security threats post-2014

Group 2: The Acknowledgers

Belgium, Croatia, France, Germany, Netherlands, Sweden, UK, US, Canada

Acknowledge the threats and tactics utilized by Russia and China but do not single them out as a priority

Display a significant number of trends in terms of the ways in which Russia and China pose a threat to Europe

Acknowledge cyber-espionage, media disinformation campaigns and active measures carried out in ‘the near abroad’ ex-Soviet space as the largest threat Russia poses to European security

Perceive the threat that Russia poses to the democratic institutions as a problem for the West, acknowledge that the states in group one are the most susceptible victims of Russian influence.

Group 3: The Hesitants

Austria, Bulgaria, Finland, Ireland, Italy, Portugal, Slovakia, Slovenia, Poland

States for which Russia and China do not appear as threats

Public intelligence reports without explicit concern for Russian and Chinese interference/influence

The lack of public intelligence community acknowledgement should not necessarily be interpreted as a lack of threat perception

Special explanation needed in case of Poland and Finland
Case of China

Even though Russia featured most heavily in the reports, Chinese influence activities also spanned concerns listed by states in all three Groups.

Some of the trends detected: political and economic pressure applied by China in order to obtain support for their policies (i.e. promoting condemnation of Taiwan and Tibet or territorial disputes in the South China Sea), manipulation of Chinese diaspora for intelligence reasons, and the use of diplomatic covering-up of nefarious operations. China’s interests in Europe are also extended and complicated by their alignment with Russia.

Concerns about Chinese control and investment in the country’s critical infrastructure identified, which suggests a distinctly different kind of possible economic coercion than that exhibited by Russia.

China’s use of political espionage in an effort to gain insights into the workings of the EU or the use of G20 summits also registered.

Some of the reports delve into Chinese “profiling” - seeking out individuals for their network of contacts and building long-term relationships. The Lithuanian report notes that China builds relationships with expensive trips, gift giving and so on. An increase of Chinese intelligence activities has also been noted in the Czech Republic.

China identified as a front-runner of international cyber-espionage campaigns and an increasingly relevant player in special services activity in general. Also, it seems that while China’s espionage has traditionally been perceived as economically motivated, this perception is changing as China leverages its economic power and wealth to accomplish foreign policy goals.

While, presently, the Russian threat is both better studied and, at least in Europe, more urgent, a clear conclusion emerges from reading these intelligence reports - that the Chinese threat is serious and will demand an increasing amount of intelligence resources in the coming years.
INTRODUCTION AND METHODOLOGY

Our research team compiled and analyzed European Union, Canadian and US state intelligence reports in order to detect trends among them concerning the threats posed by Russia and China.

The aim of this research is to address the prevailing lack of understanding within the journalism, non-governmental research and policy-making communities on what national intelligence agencies see and assess to be the main foreign interference threats. While there is a growing amount of existing data on specific foreign interference incidents (particularly with regards to Russian interference in Europe and the US), as well as an increasingly sophisticated understanding and research on the illegitimate tools employed by the Russian and Chinese governments to achieve foreign policy aims, there is not an in-depth understanding of exactly what those aims are and how they differ across regions and states. There is also a lack of understanding on how the European and North American intelligence apparatuses have been assessing and responding to these emerging threats. This research paper therefore aims explicitly to address that gap and thus serve as a tool to further the international conversation on how to respond appropriately and effectively.

The data analyzed covers the period starting from 2013 up to the most recent reports released for the 2018 yearly period, where available. This time frame has been explicitly chosen to evaluate how the threat assessments have changed since the start of the war in Eastern Ukraine and the Russian annexation of the Crimean Peninsula.

Excluding the states that did not have publicly accessible reports (Group 4), we categorized countries into three groups according to the degree of centrality that Russia and China played in their national intelligence threat assessment. Namely, Group 1 includes states where intelligence services display a thorough understanding of Russian and Chinese influence strategies and identify them as the major threat to national security; Group 2 contains states where, while acknowledging threats and tactics utilized by Russia and China, the intelligence did not single them out as a priority; finally, Group 3 consists of states for whom Russia and China do not appear as threat as far as the content of available reports is concerned. Our analysis compared states within and across these three groups in order to ascertain common intelligence tools employed by state services and to provide an in-depth appraisal of trends among perceived Russian and Chinese aims, targets, mechanisms, and narratives.
Intelligence services of many states identify Russian and Chinese influence strategies as the largest threat to national security.
GROUPS 3 AND 4: THE HESITANTS
RUSSIA IS NOT EXPLICITLY ASSESSED AS A THREAT

Firstly, a separate note needs to be made on the states which either did not publish any intelligence outputs (Group 4), or where the intelligence outputs did not explicitly mention Russia or China as security threats (Group 3).

Austria, Bulgaria, Finland, Ireland, Italy, Poland, and Portugal are the states which fell within the so-called Group 3. While these states provided public intelligence reports, none of them displayed an explicit concern for Russian and Chinese interference/influence. The most surprising states in this group are Poland and Finland given both these states’ history of geopolitical skirmish with Russia. Meanwhile, Italy and Austria’s track-record of political ties to the Kremlin plausibly explains the hesitance and obfuscatory language used to explain threats to European stability.

Additionally, it should also be noted that the availability of annual reports from Security Services varied particularly in this group. That is to say, some of the states’ produced intelligence outputs came not in the form of declassified annual reports (produced for public consumption) but rather as National Security Strategies (Austria, Bulgaria, France, Hungary), Committee Hearings (US), National Security Budgets (Bulgaria), or, in the case of Finland, a Security Intelligence Service Yearbook. The lack of source consistency across the examined states can also partially explain the different emphasis apparent in different intelligence outputs. Namely, the aims and purposes of, say, a National Security Strategy might not be to outline specific threats or discuss specific intelligence community achievements, but rather serve as an overarching outline for the future. Similarly, the Finnish case can partially be explained by the fact that the only available output for the Security Services - the Security Intelligence Service Yearbook - appears to be designed to familiarize a broad national audience with the general work and structures of the Service, rather than to discuss specific threats and policy matters.

While it is unclear whether or not these reports showed an unwillingness to publicly acknowledge, criticize, or explicate the specific intelligence threats posed by Russia and China, it is clear that myriad explanations can be used to explain the responses of democratic states who fall into this least-engaging group. In other words, a lack of public intelligence community acknowledgement and exposure should not necessarily be interpreted as a lack of threat perception. Within this context, special explanation will be needed in case of Poland. It requires further study of other sources which will be done later on by the research team.

Additionally, a number of countries did not have publicly available intelligence reports, and the team was therefore unable to assess these countries along with the others. This was the case with Cyprus, Greece, Hungary, Luxembourg, Malta, Romania and Spain. It is important to note that, while in Group 3 the lack of explicit discussions of the threats from Russia and China most likely represent a conscious choice (as is most likely the case with countries like Poland and Finland), a political direction or a genuine lack of threat perception, the same cannot be said for countries in Group 4. Rather, the decision not to publish any intelligence assessments can more plausibly be explained with institutional or organizational culture, the character of national security discussions, and decision making and political strategy. In this context, one cannot reliably infer whether Russia and China are perceived as threats and how their activities are assessed in the intelligence community.
GROUP 2: THE ACKNOWLEDGERS
RUSSIA AMONG OTHER THREATS

Group 2—those who engaged the Russian threat in a substantive way, without naming it as a priority—displayed a more notable perception of the ways in which Russia poses a threat to Europe at large. Across the board, Group 2 acknowledged that the largest threat that Russia poses to European security is in the form of cyber-espionage, media disinformation campaigns and active measures carried out in ‘the near abroad’ ex-Soviet space. Specifically, all but three states in Group 2 openly denounced Russian aggression towards Ukraine. The tendency to describe the situation in Ukraine as a threat even to countries without a geographic proximity to the ex-Soviet region speaks to a collective perception of European security, both in terms of NATO membership as well as an understanding of national security that extends into collective political stability of the region and a protection of common European interests.

The three countries which did not mention Russian interference into Ukraine as a threat - Canada, Sweden and France - did, however, stress that Russian interference was conducted in the form cyber-espionage and partisan media support and coverage. This illustrates that similar methods have been used and noted by countries who do not experience a direct geographical threat to their territory, but do still feel that their information systems and overall national interests are being undermined using technologies which allow for physical distance as well as a degree of anonymity.

Predictably, as economic-political leaders of the EU, France and Germany expressed the need to counter these Russian threats carefully, as to maintain and slowly strengthen the economic and security-based ties that Europe and Russia share. Belgium wrote extensively about Russian infiltration of their parliament. The Skripal affair featured most heavily in the United Kingdom’s report, with WikiLeaks dictating much of the American appraisal.

Conversely, Croatia singled out their dependence on Russian oil as one of their largest concerns. Croatia is also the only non-Baltic country - as examined later in Group 1 - where “unnamed foreign powers” (whose narratives are consistent with anti-EU and anti-NATO sentiments) have aimed to amplify the power of Serb extremists and to capitalize on narratives related to protection of minorities. However, the latest available SOA’s report from 2017 notes that extremism is marginalized, and largely rejected by the general population. In sum, Group 2 perceives the threat that Russia poses to the democratic institutions as a distinctly Western problem, but expressly acknowledges that the states in Group 1 are some of the most susceptible victims of Russian influence.
The situation in Ukraine perceived as one of the most significant security threats post-2014 by the intelligence services.
GROUP 1: THE MOST ALARMED

Unsurprisingly, the Baltic states as well as the Czech Republic and Denmark displayed intelligence reports that made no doubt as to who posed the largest security threats to their domestic institutions. Not only did Group 1 provide the most far-reaching condemnations of Russian interference, but also provided detailed explanations of geo-political infringements.

There are numerous overlaps between Group 1 and Group 2 regarding concerns about Russian influence campaigns, but there are also several influence campaigns and strategies that seem to be employed only in the 5 countries comprising Group 1. The enlarged presence of these methods of influence, the implied conflict with Russia over certain spheres of influence (legitimate or otherwise), and therefore the increased Russian threat to a nation’s interests explain why fears of foreign interference loom particularly large in these countries.

There are several methods which appear to have been used almost exclusively in the Baltic states (with a possible exception of Croatia, where these methods are present, but are not appraised as central to national security), as identified by our team. These methods are support for extremists, manipulation of national policy discussions through the local Russian diaspora, and the use of Government Sponsored NGO’s or GONGOs. The overarching narrative and justification for these activities is Russia’s protection of Russian-speaking “compatriots”, and the defence of their rights and freedoms at the expense of other countries’ national interests.

With regards to the use of Russian minorities, the Estonian Internal Security Service especially notes that Russia hosts a variety of “youth diplomacy” events, whose stated aim is to create a “network of young compatriots abroad” (KAPO report 2017, pg. 4). The Estonian service sees this as an attempt to cultivate a new generation of activists, which could later be used to further divisive political aims. This goes hand in hand with attempts to prevent the integration of these ethnic Russian youth into Estonian society, thus leaving it perpetually destabilized. The Lithuanian State Security Department notes that, while similar attempts exist, the Russian speaking youth is not keen to participate, and quotas for Lithuanians at Russian propaganda events often go unfulfilled. The Latvian Security Police notes a similar trend towards recruiting young people but notes that the main vulnerability comes from young Latvian citizens choosing to pursue higher education in Russia, which provides the Russian Security Services with relatively undisturbed recruitment opportunities.

The Latvian Security Agencies also especially stress that the manipulation of the Russian speaking population is done with the explicit justification of protecting their rights in Latvia. This goes together with frequent misrepresentations of Latvia as a fascist police state where Russian speakers are oppressed and denied their constitutional rights. This narrative is then expressed in international institutions in order to portray Latvia as a perpetrator of human rights violations. In Lithuania, according to the 2018 threat assessment, “the Russian media tries to present the minor events organized by the Lithuanian extreme right-wing groups as the evidence of popularity of extremist ideology in Lithuania” (2018 Threat Assessment, pg. 39) This narrative is tied with the use of political extremists and pro-Russian NGOs, who are the main actors spreading and amplifying these messages.

The politicization of contentious historical eras, particularly the World War Two era and the subsequent Russian occupation of the Baltic States, becomes particularly apparent each year in 9th of May, when Russia (and Russian speaking populations elsewhere) celebrates Victory Day in Riga, Latvia. The frequent use of the Russian flag and Soviet-era symbols in these celebrations, as well as a narrative of Russia as a “liberator” of the Baltic States, is coordinated by the Russian embassy and has become a frequent source of tensions. Similarly, Russia’s work to preserve and create military memorials (Latvian Security Service, 2018, pg. 21) is aimed to strengthen Russia’s positive image as the defender against Nazism by using Soviet-era nostalgia as well as by creating sites for contentious political gatherings. This exemplifies a larger trend of Russia...
creating its own, competing version of history, which often tries to undermine prevailing historical interpretations. As a bonus, any attempt to remove such memorials is followed by a public campaign that portrays such suggestions as evidence of the rebirth of Nazi ideology in the Baltics. The Estonian Internal Security Service also notes a number of historical conferences and research articles released in 2017 (commemorating the Centenary of the Russian Revolution) and in 2018 (aimed at undermining the Estonian State Centenary celebrations).

A crucial difference therefore between the Baltic States and the other countries analysed in this paper, is as follows. While all countries in Groups 1 and 2 note a use of several interference methods, it is only in the Baltics where the states appraise a coordinated intersection of several methods, all of which are aimed at winning support from the Russian speaking minorities. Due to historical factors, these minorities comprise a significant percentage of the overall population, and therefore possess notable political, economic and social power. The Russian interference policy towards the Baltics is therefore aimed specifically at these minorities, which is distinct from states in Group 2, where the policy aims to undermine the national interest as a whole. The interference is also multifaceted, aiming to create a completely alternative version of past and present reality that directly undermines the integrity of the Baltic states by deepening ethnic tensions while simultaneously trying to position itself as a defender of human rights and historical truth.

It should be noted, however, that despite the varied methods employed, all the Baltic states’ Internal Security Services note that Russia’s compatriot policy has not been particularly effective, as the majority of the population is not significantly swayed by Russia’s messaging.

The proximity for the Baltic states and the Czech Republic to Russia is such that the intensification of official and unofficial state-sponsored media campaigns seems to affect public opinion in their states more than much of Western Europe. However, the Czech Security Services declare the large presence of undeclared Russian intelligence officials in the Republic as the main threat. This is seen as a two-fold threat. Firstly, it is noted that the large Russian presence in policy-making circles provides opportunities for “unintentional contact” between Czech citizens and Russian intelligence officials. Rather vaguely, the 2017 BIS report notes that the risks are greatly exacerbated by the “reckless attitude of Czech citizens, primarily politicians and civil servants, towards unclassified, but inside, non-public information” (BIS report 2017, 6). The vague language in the report can be plausibly explained by the domestic sensitivity of the issue, however, it can serve as a hint that Russian infiltration into the Czech state apparatus is a serious and prevailing concern.

Finally, the Danish case. While Denmark does not currently have an active land dispute with Russia, issues with Arctic maritime demarcation have occupied an increasingly large part of the Danish threat assessments. Russia has shifted from a collaborative to a dominant approach in the region, which Russia views as an area of prioritized interest. A military build-up accompanied and media campaigns, with the aim to protect Russia’s oil and gas fields as well as establish a claim to the Arctic sea routes is viewed as an economic threat by Denmark. While the Danish assessments do note that Russia’s build-up is defensive in nature, it increases the possibility of a conflict or an arms race with NATO in the region.

In sum, Group 1 is differentiated by two key factors. Firstly, while many of the threats discussed below in our cross-group analysis are also present in Group 1, all five cases are marked by an added problem that Russia presents to the state’s security and internal stability. Secondly, these specific threats are somewhat more invasive and, in all cases except the Czech Republic, display an implicit possibility that a territorial or constitutional threat may stem from current issues. The Baltics especially see a coordinated use of several tools aimed not just at gathering information or influencing the public opinion but rather to undermine the legitimacy of the country’s existence and connections to an international, democratic system. The intensity of this interference provides us with a plausible guess as to where Russia’s foreign interference priorities lie. Moreover, the long history of Russia’s threatening and invasive policies in the Baltics provides us with a glimpse of the methods which Russia has in its repertoire, including the ones which Russia has not yet chosen to use against its more powerful Western Allies.
The threat that Russia poses to the democratic institutions is a problem for the West, while the states on the Eastern Flank of NATO are the most susceptible victims of Russian influence.
Now, let’s turn to analyse those methods which did not differentiate across group lines. The most prominent threats across the board are the military threat, cyber-attacks and cyber-espionage, media disinformation, economic measures, and increased special services activity in select states.

1. Ukraine and Russian military threat as an overarching security threat in Eastern Europe.

An overarching security concern of states in groups one and two stems from the ongoing Russia-fueled crisis in Ukraine. As mentioned by each of the Baltic states, Russian aggression in Ukraine has set a dangerous precedent for those states that are situated along Russia’s frontier. Not only do Russia’s attempts to publicly justify their strategic campaigns in Ukraine with Russian diaspora cause worry for intelligence officials in the Baltics, but Russian-trained fighters returning from Ukraine to the Baltic states give each of the states cause for serious alarm. While the Baltic states have demonstrated the most thorough coverage of Russian military exercises and threats along their borders, our analysis has shown that the ongoing conflict in Ukraine has substantially altered the way that Russian military and intelligence threats are assessed by Western European states as well. Not only does Germany highlight the importance of a democratic resolution to the conflict, but they also reissue how imperative it is for the EU’s solidarity that Russian sanctions remain intact. While intelligence services from the U.K, U.S and Netherlands discuss what the resurgence of Russian state-based military threats means for overall European security interests, there are also economic effects that the crisis in Ukraine has posed to regions in Europe. Specifically, Croatia highlights how the cold-war style ‘frozen conflict’ in Ukraine has disrupted expected supply routes of Russian oil to the Southeast Balkans. With this it is clear that Russia’s aggression in Ukraine has ripples of complications that are felt beyond the realm of military strategy and response, directly effecting the economies of European states who, while remaining aware of the threat from the Kremlin, depend on Russian fuel.

A separate issue is that of potential military threats. Every country surveyed except Belgium felt explicitly that, while Russia did not threaten their sovereignty directly, the situation in Ukraine was nevertheless perceived as one of the most significant security threats post-2014 as part of an interconnected security environment. Predictably, the Baltic countries differ in that their reports tend to include realistic and careful appraisals of a direct military threat to their sovereign territory. The Estonian report especially analyzes current threats such as disinformation in the context of how they could be laying ground for Russian success in case of a potential military escalation.

2. Cyber espionage

With several states, including the Czech Republic, Belgium, and Germany, reporting significant cases of cyber security attacks at the government level, cyber espionage emerged in each report as an essential dimension of the Russian threat. Russian cyber espionage takes on the shape of diffused forms of disinformation attacks, direct interference in governmental servers as well as the slowing down of national IT systems. The Baltic states each observed highly advanced cyber tools used in espionage campaigns against the processes of state bodies. In the case of Lithuania, 2018 saw an attempted Russian-based cyberattack on their national energy sector. The Netherlands saw similar tactics utilized by Russian intel agencies seeking out information on the Dutch states’ scientific programs, economy, defense, and political policies. These digital attacks targeted foreign and defense ministries as well as inter-governmental organizations such as EU, NATO, and UN, as well as think tanks, NGOs and vital sectors. A similarity amongst these reports is noting the use of cyber espionage as a military tactic, aimed at destabilizing key national defense options and top-secret intelligence documents. Named by some as ‘active measures’ cyber-espionage, especially in Russia’s ‘near abroad’, is mentioned several
times as a return to cold-war tactics with an added insidious danger wrought on through the general anonymity of the internet. An overwhelming amount of states have named the Russian cyber threat as a paradigm-shifting phenomena that the world-at-large needs to combat. This phenomenon pierces through the realm of ‘spying’ and actually involves attempting recruitment. This new paradigm’s difficulty brings with it the problem of differentiating between nationally affiliated cyber actors and independent hackers and cyber-actors. The Baltic states, Netherlands and Sweden have all cited instances of Russian cyber intel initiatives attempting to recruit talented academics, ex-patriots, and military personnel through a variety of online tactics.

3. Media disinformation campaigns

Another massive facet of the cyber-threat emerging from Russia is the waging of both publicly executed and privately directed disinformation campaigns. Disinformation campaigns aimed at the curbing of foreign nation’s policy and public opinion has been described by the Czech Republic as part of Russia’s “hybrid strategy”. Germany notes that beyond espionage interests, the Russian services continue to attempt to influence political and public opinion in Germany. Pro-Russian information is spread through social media networks like Twitter, as well as through state-sponsored and private organizations/institutions. Russian state media and their various international affiliates disseminate disinformation about Germany and attempt to destabilize the German government. Strong hybrid campaigns against Germany’s endorsement of EU sanctions against Russia were mounted. The perpetuating of pro-Russian narratives and spreading of seemingly untraceable alternative mainstream discourses have been observed by most of the states in Groups 1 and 2. While some states actually named Sputnik and RT as appendages of the Kremlin’s official narrative, the priority of these reports were dealing with how to combat the nefarious spreading of online material that portrays overtly anti-EU, anti-NATO, anti-democratic, anti-pluralistic, and pro-Russian sentiments. The pro-Russian narrative, as observed by these reports, roughly represent a Euro-skeptical and pro-traditional family values politics that champions the measured conservatism and ‘strong-man’ politics displayed in Putin’s’ policies. Estonia, a leader of cyber-security in Europe observed that by using online news sites, video streaming/sharing sites, and social media Russia is able to pursue both strategic military and intelligence objectives by harnessing support through the soft effects that disinformation slowly implements. The UK PM also accused Russia of using disinformation to influence the Brexit vote and interfering with UK political party data. Even the United States acknowledged the creation of fake persons online by Russian accounts to send stolen data to journalists before the 2016 election. Also, the US noted that Russia’s state-run media is a propaganda machine that serves as a mouthpiece for the interests of the Kremlin. Canada substantiated these claims in their report, saying that “Russians watch television for an average of four hours a day. Putin and the media emphasize the stability and the greatness of Russia; the state is presented as a fortress and a champion of civilization, but is nevertheless surrounded by enemies.” Disinformation in the Baltics also takes on the form of the condemning of Russophobia (directed against the Russian minority in the region) and the labelling of Baltic nationalism as overtly anti-Semitic.

4. Economic measures

For states with invested Russian business assets, economic risks need to be taken into consideration. We have found that, in these cases, intelligence reports have reflected efforts by both foreign governments to improve their political and economic standings abroad by carrying out a variety of influence campaigns shrouded by diplomatic cover. The U.K. names fears that Russian investments in their critical infrastructure are linked to subversive and criminal finances. For countries with economic dependence on Russian energy, there are instances of reported pressure being applied to support Nord Stream II. It is fairly evident judging by the reports of France, Germany, Croatia, the Netherlands, and the Baltics, that the consensus among states on what is to be done about Russian aggression varies along economic lines. For instance, Estonia seems to provide the most positive appraisal of the sanctions, saying their consistency has both surprised Vladimir Putin as well as presented him with substantial and unforeseen domestic problems. Estonia seems to provide the most positive appraisal of the sanctions, saying their consistency has both surprised Vladimir Putin as well as presented him with substantial and unforeseen domestic problems. Croatia has reached a similar conclusion, stating that they perceive Russia’s attempts to thwart other Balkan states from acceding to the EU as economically fueled, and that they have certain dependencies on Russian...
energy but fear that the current economic climate could lend towards monopolistic gains taken by Russia. The Netherlands pointed out that vital interests of their state have links to private companies with unnamed foreign shareholders, naming this as a threat to their economic well-being. In a similar vein, the Czech Republic has issued a concern that Chinese and Russian career diplomats are attempting to softly coerce Czech officials into fulfilling foreign economic goals. There are many Russian figures tied up in Czech corruption cases and illegal activities and several Russian investors, stakeholders, and offshore companies involved in the Czech economy. This situation creates problems for the Czech economy because of some of these key Russian stakeholders’ involvement in illegal activities. On the other hand, states like Germany and France take a more conservative approach to how they condemn Russian economic endeavors. Both of them, in a predictably traditional diplomatic manner, claim that combatting Russian aggression economically must not completely ostracize them from the European community, as they serve as an import economic and political ally.

Direct economic pressure applied by actors of Russian interest also played a paramount role in the assessment of national threats in Group 1. In Latvia, the issue of investor visas has been contentious, as investor visas are denied to suspected Russian agents. Specific to Denmark is the issue of Arctic sovereignty and maritime demarcation. The Czech Republic makes it clear that having Russian stakeholders engaged in illegal activities tied up in the Czech private sector makes economic measures regarding Russia an intensely difficult situation.

5. Increased Special Services activity

The Skripal affair greatly affected the United Kingdom’s report, and also appeared in several other intelligence reports. There’s an ongoing Intelligence committee inquiry into the Skripal poisoning, and the UK’s National Security Capability review 2018 remarked that the “reckless and indiscriminate use of a military-grade nerve agent on British soil was an unlawful use of force by the Russian State” (2018, 6). The Belgian report claims that in the wake of the Skripal affair and the Belgian consul charged with serving the interests of the Russian SVR, Belgian intelligence services have ramped up efforts to root out Russian espionage. Overall the UK perceives this affair as cause to put into effect stronger censure policies and more effective counteractive-cyber measures against Russia. Meanwhile, the Netherlands’ security services have detected increased Russian recruitment efforts with the aim of acquiring political and scientific information, particularly as it pertains to Dutch technological advancements.

Another secret services tactic that has long been observed is the use of history to spread highly partisan propaganda and amplify societal tensions. Croatia is the only country in this group where “using history as a tool” and “support for extremists” is noted as an influence tactic, which is more reserved for Eastern European countries in Group 1. However, the Russian operation to interfere in the 2016 US Presidential election made heavy use of amplifying racial and class tensions in the US. Narratives which portrayed the US as a surveillance state with excessive police brutality or compared the US to Imperial Rome due to the rising economic inequality and increased concentration of wealth with the so-called “1 %” were amplified and supported. The US example shows Russia taking the tactics that have been at work in Eastern Europe for decades and successfully transferring them to the US context.

From our cross-group analysis, it is evident that the majority of states in Groups 1 and 2 are highly cognizant of the fact that Russian disinformation campaigns manifest in both the public media sphere (in the form of state and international television, online news sources, etc.) and ‘personal’ cyber-space (in the form of cyber-espionage, hacking, and spreading of untraceable narratives). Also, the denouncement of Russian geopolitical military intimidation was a similarity between Groups 1 and 2, extending its scope towards Ukraine, the Arctic, the Baltic coast, Belarus, and Syria among others. Groups 1 and 2 also acknowledged (whether or not they named Russia explicitly) that the global security paradigm has shifted, necessitating the need for intelligence services to ramp up their cyber-defense capabilities. Finally, Russian actors who carry out soft-influence initiatives in foreign states have also been singled out by both Groups as especially difficult to combat based on the protection afforded to them under the guise of diplomatic procedure.
The Chinese threat is serious and will demand an increasing amount of intelligence resources in the coming years.
Even though Russia featured most heavily in the reports that we compiled, Chinese influence activities also spanned concerns listed by states in all three Groups. The Chinese interference threat does not yet occupy the same importance as the Russian threat does (particularly in Eastern Europe). However, it is clear that states are becoming increasingly cognizant of the potential dangers involved in China’s growing economic and political ambitions and, consequently, power.

Some of the trends that we detected include: political and economic pressure applied by China in order to obtain support for their policies (i.e. promoting condemnation of Taiwan and Tibet, or territorial disputes in the South China Sea), manipulation of Chinese diaspora for intelligence reasons, and the use of diplomatic covering-up of nefarious operations. China’s interests in Europe are also extended and complicated by their alignment with Russia.

The Netherlands, Denmark and the UK all mentioned concerns about Chinese control and investment in the country’s critical infrastructure, which suggests a distinctly different kind of possible economic coercion than that exhibited by Russia. The Danish report also notes China’s economic expansion into the Arctic as a potential future complicating factor, as the region will get linked with other strategic interests. Similarly, Germany has mentioned China’s use of political espionage in an effort to gain insights into the workings of the EU or the use of G20 summits.

The Dutch report delves quite substantially into Chinese “profiling” - seeking out individuals for their network of contacts and building long-term relationships. This is not exactly direct recruitment but is nevertheless marked as a concern for the Dutch agency. This mirrors concerns from the Lithuanian report, which notes that China builds relationships with expensive trips, gift giving and so on. An increase of Chinese intelligence activities has also been noted in the Czech Republic.

The fundamental take-aways from how China was handled in these intelligence reports is that they are a front-runner of international cyber-espionage campaigns and an increasingly relevant player in special services activity in general. Also, it seems that while China’s espionage has traditionally been perceived as economically motivated, this perception is changing as China leverages its economic power and wealth to accomplish foreign policy goals.

While, presently, the Russian threat is both better studied and, at least in Europe, more urgent, a clear conclusion emerges from reading these intelligence reports - that the Chinese threat is serious and will demand an increasing amount of intelligence resources in the coming years. There are notable differences in the Chinese approach in comparison to Russia, particularly as it pertains to economic measures, but there are also worrying similarities. China’s cyber-espionage campaigns have occupied much of the world’s attention in the last year. While they have often been different from Russia’s in aim as well as method, both countries have clearly realised the potential of cyberattacks and have the technological means to conduct them. With that in mind, it is safe to assume that more future research will need to be done on the Chinese case. And moreover, an understanding of Russian methods and corresponding Western vulnerabilities allows countries to use this understanding as a basis for building more comprehensive security strategies.
CONCLUSION

The Intelligence services of the majority of states studied identify Russian and Chinese influence strategies as a serious threat to national security. States most exposed to the Russian threat provide far-reaching condemnations of Russian interference and detailed explanations of geopolitical infringement or direct economic pressure. All countries surveyed (except Belgium) perceived the situation in Ukraine as one of the most significant security threats post-2014.

Also, the intelligence services of the states that do not see Russia as the No. 1 threat display a significant number of trends in terms of the ways in which Russia and China pose a threat to Europe. They acknowledge cyber-espionage, media disinformation campaigns, and active measures carried out in ‘the near abroad’ ex-Soviet space as the largest threat Russia poses to European security.

It is a general understanding that the threat that Russia poses to the democratic institutions is seen as a real problem for the West.

The Chinese threat is also serious and will demand an increasing amount of intelligence resources in the coming years.

While creating this research paper, our team compiled primary source material from intelligence agencies and other defence-related structures. These materials tell a lot about the current foreign interference landscape - the threats these countries are dealing with or, just as importantly, the importance countries assign to these threats. This research paper has attempted to map it within its scope and will hopefully provide a starting point for more in-depth discussion on the evolving threats our governments face.

More research is needed to systematize and map Russian and Chinese influence activities in Europe and North America and to create an understanding of their strategic direction.

This paper will be especially useful to support the subsequent phases of this project, which will involve meeting with professionals from security institutions as well as the creation of a handbook on mitigating third country interference on a personal level. An in-depth understanding of current security agency practices will hopefully create a base for fruitful and sophisticated discussions on further steps.
## ANNEX 1: Source List

<table>
<thead>
<tr>
<th>COUNTRIES</th>
<th>GROUP 1: THE MOST ALARMED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>Danish Defense Intelligence Service Intelligence Risk Assessments (2010 - 2018)</td>
</tr>
<tr>
<td>Estonia</td>
<td>Foreign Intelligence Service Security Environment Assessments (2016 - 2018)</td>
</tr>
<tr>
<td></td>
<td>Guidelines to the Minister of National Defence (2012 - 2021)</td>
</tr>
<tr>
<td>COUNTRIES</td>
<td>GROUP 2: THE ACKNOWLEDERS</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Belgium</td>
<td>State Security Service Activity Report (2017/18)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Intelligence and Security Service Annual Reports and other documents</td>
</tr>
<tr>
<td>USA</td>
<td>Senate Intelligence Committee Reports</td>
</tr>
<tr>
<td>COUNTRIES</td>
<td>GROUP 3: THE HESITANTS</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Austria</td>
<td>Austrian Security Strategy (2013)</td>
</tr>
<tr>
<td>Poland</td>
<td>Summary of the report on threats to national security (2015)</td>
</tr>
<tr>
<td>Portugal</td>
<td>Intelligence Activity and Contemporary Challenges (by Internal Intelligence Service)</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Annual Reports of the Ministry of Defence 2003-2017</td>
</tr>
</tbody>
</table>