palgrave communications
HUMANITIES | SOCIAL SCIENCES | BUSINESS

ARTICLE

https://doi.org/10.1057/s41599-019-0227-8 OPEN

Divide and rule: ten lessons about Russian political influence activities in Europe

Geir Hågen Karlsen[1]

ABSTRACT The purpose of this study is to improve understanding of how Russia is conducting political influence activities against Europe. It examines current thinking and perceptions on this topic among Western secret services and is based on an analysis of approximately 40 annual reports from 15 secret services in 11 Western countries, covering the period 2014–2018. This activity is by nature covert, and the analysis given in these reports from Western secret services complements other research and shows the broad range of tools and techniques employed for political influence, and much detail on the execution of these activities. According to these secret services, Russia is the foreign state that tries to influence European politics and decision-making most, and more so than China and other states. These influence activities support three main Russian strategic objectives: regime security, predominance in Russia's near abroad, and world-power status for Russia. The long-term objective of Russian influence activities is to weaken NATO and the EU. In the shorter term, it is to lift the sanctions imposed after the Russian intervention in Ukraine in 2014. Russia also has more specific objectives related to each individual country. Russia is targeting the West through a divide and rule approach, using multiple tools of influence. The population is mainly reached through media and social media, exploiting divisive issues. Minorities, refugees, and extremists are used to further this divide and rule approach. Human intelligence and cyber operations are important covert tools of influence. Russia also uses the energy sector, business, and corruption as venues for influence. It has an extensive network of allies and front organizations, and reconstructs reality and rewrites history to legitimize itself and undermine others. Finally, military force is Russia's ultimate tool of influence. These influence activities are of large-scale, and the threat should be taken seriously, but the reports studied also indicate that the effects of these activities are limited.

[1] Norwegian Defence University College, Oslo, Norway. Correspondence and requests for materials should be addressed to G.H. K. (email: ghkarlsen@hotmail.com)

Introduction

States, organizations, and individuals have always tried to influence others to achieve what they want. Multiple means and methods have been used, some legitimate, some not. The conflict between Russia and Ukraine brought the term propaganda back on the front pages of mainstream Western media. The U.S. presidential election campaign and subsequent investigations shattered any remaining illusions about Russian interference in Western politics. Concerns about fake news, cyber-attacks, and manipulation of elections abounded all over Europe, and it became clear that Russian secret services were not only involved in espionage, but also aiming to influence Western politics. Russia was conducting political influence operations supported by intelligence activities. The German security service described the close interaction between Russian intelligence and influence activities:

> Russia´s priority is gathering early information about the views of the Federal Government, political parties, and institutions, regarding the handling of the crisis and future German policy towards Russia. Not least, the Russian services are also attempting to present their point of view to the public and to use their contacts to exert influence (BfV, 2015: p. 40).

During the cold war, the Soviet Union had an extensive and complex apparatus for disinformation and influence operations. The general Western understanding was that intelligence services' main role is to collect information. It is, however, essential to understand that in the Russian tradition the role of influencing societies and decision-making processes is equally important, and some claim even more important (Karlsen, 2016: p. 194).

The purpose of this study, covering the period 2014–18, is to improve understanding of how Russia is conducting political influence activities against Europe. It will examine current thinking and perceptions about Russian influence activities among Western secret services. It is based on about 40 annual reports from 15 intelligence and security services in 11 Western countries. Such influence activities are often covert, and studying this topic is challenging. It is difficult to assess the truthfulness of sources and accuracy of information, and it also involves dealing with denial, deception and disinformation. Secret services work to reveal covert activities, and this study will establish an understanding of these services' view on the totality of Russian influence activities, the broad range of tools and techniques employed, and much detail on the execution of these activities. These findings can then supplement other sources and open for further and more profound studies of the topic. This study does not pretend to reach a final conclusion regarding Russian influence activities; for one reason, as we shall see later, the use of these sources poses its own challenges. Influence activities are here defined as activities aimed at influencing someone to agree with your opinions or do what you want (Collins, 2017).

The responsibility for covert influence activities lies with the Russian intelligence services, and they are using various methods, including cyber activities and agents, or human intelligence in this work. Russia has three main intelligence services operating abroad. The Foreign Intelligence Service (SVR) is the civilian foreign intelligence service, the Main Intelligence Directorate (GRU) of the General Staff is the military intelligence service, and the Federal Security Service (FSB) is a national security service also performing some intelligence tasks abroad. In addition to collecting information, all three services are involved in influence activities. There is broad agreement that these services are highly professional, well-resourced and very active.

Russia also has a multitude of other capabilities and venues for political influence, including diplomacy, political communication, media and social media, Russian diaspora and compatriots, various parts of civil society (including foundations, NGOs, academia, think tanks, and the Orthodox Church), the business and energy sectors, sympathizing political parties and organizations, and ultimately their military forces. Some of these assets are controlled by Russian intelligence or other state organs, while others share values or sympathize with Russia. Russia has a whole-of-government approach to influence and can employ the entire state apparatus for this purpose (DIA, 2017: V; EIB, 2017: p. 16). The latest Russian National Security Strategy published in December 2015 identifies the U.S. and the North Atlantic Treaty Organization (NATO) as Russia's main threat. Conceptually, these influence activities are part of Russian thinking about strategic deterrence, where anything from social media to nuclear capabilities can be used, in peacetime or war, to shape and stabilize the environment according to Russia's liking (DIA, 2017: p. 15, pp. 22–23).

First, we will look more closely at the sources for this article, the annual reports from 15 Western secret services, and the limitations and challenges of using this type of empirical material. This article is about the perceptions of Western secret services regarding Russian influence activities, and these will be summarized in ten lessons. In various ways all these findings have been covered by other academic works, and they also show a continuation of influence activities from the Cold War:

1. Russia is the main threat.
2. Russia conducts political influence activities, and the main purpose is to weaken the European Union (EU) and NATO.
3. Russia is targeting populations; their approach is divide and rule.
4. Russia uses minorities, refugees and extremists to further its divide and rule approach.
5. Human intelligence is an important covert tool of influence.
6. Cyber operations are another important covert tool of influence.
7. The energy sector, business and corruption are used as venues for influence.
8. There is an extensive use of allies and front organizations.
9. Russia is reconstructing reality and rewriting history to legitimize itself and undermine others.
10. Military force is the ultimate tool of influence.

The first lessons describe the purpose and targets of Russian influence activities in Europe, while the subsequent ones describe the tools and techniques used by Russia. These tools and techniques are not stand-alone activities, they are employed together, sometimes depending on each other or reinforcing each other, to achieve the political objectives of the Russian government. Before concluding, we will discuss the effectiveness and limitations of the Russian approach.

Methods

Russian influence activities are, at least partially, conducted by covert means, which makes it difficult to observe and analyze them. It is the task of Western secret services to unveil covert activity, and using data from intelligence reports gives access to information that is often not available elsewhere, or that may supplement other sources. This study examines the perceptions of Western secret services regarding Russian influence activities, and is conducted through an analysis of about 40 annual reports from 15 security services of 11 Western countries: Czech Republic, Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Netherlands, Norway, Sweden, and the U.S. Annual reports were selected as they give an overview of each service´s perspectives,

and thus deemed suitable for this study. There is a wealth of other material available, including from parliamentary hearings, inquiries, media coverage, websites, public statements, legal documents, and so on. Using these as reference material, however, would require substantial search and translation resources in many languages, but they certainly provide a basis for future in-depth study. The study includes reports since 2014 to account for the dramatic change in relations after the conflict in Ukraine. Many services publish descriptions of these threats so vague and general that they have been excluded, or publish reports on privacy or the observance of political, legal and other formalities that are irrelevant to this study. Others, like Austria, publish very detailed reports, but without mentioning Russia. No suitable reports were available from U.K., Poland, France, Italy or Spain, or other Southern or Central European countries. One U.S. report was included as it contained relevant material for the understanding of Russian activity in Europe, particularly regarding the use of military force.

In the end, this left about 40 reports, but with only a limited regional coverage. Using reports from 11 different countries gives a broad perspective on Russian influence activities in Europe. However, the publication of such reports describing foreign influence activities in detail seems, on the whole, to be limited to Northern Europe, and especially to the Baltic and Nordic countries. The findings of this article, therefore, should be seen as an overview of possible Russian tools and techniques rather than a description of ongoing activities in specific regions.

There are no standard formats for these reports, and Western secret services have different interpretations, perspectives and relations to Russia. Initially, common themes and recurring ideas about Russian influence activities were identified and thematically organized. This was an iterative process, and the empirical material provided a 'long list" of tools and techniques used by Russia that was later collapsed into the ten final findings of the study. The next step was to explore and explain more specifically how these different tools were used. This was an interpretative rather than aggregative process, identifying various aspects, preferably from several services and regions. Furthermore, the study does not warrant generalization about Russian influence activities in Europe as a whole, nor should we conclude that these reports cover all Russian tools. In some areas these reports contradicted each other, and in various ways they also raised doubt about the quality and efficiency of Russian influence activities. This is covered partly under each lesson, and in more detail in the final discussion.

Using these sources poses several challenges. First, there is a question about the role of these secret services. Their reports serve several purposes. One is to increase understanding and awareness, another is to support decision-making, and a third is to enlist public support for policies. The head of Finnish Supo describes national security as a joint effort (Supo, 2017: pp. 4–5), while EIB uses information for prevention and to counter disinformation (EIB, 2017: pp. 4, 6). Secret services also have their own interests, and they use these reports, explicitly (Supo, 2018: pp. 5, 7; DP, 2018: p. 16) or implicitly, to get more resources or gain support for legislative initiatives.

Second, it is necessary to understand what is included in and what is excluded from these reports. The information made public has most certainly been through a comprehensive vetting at several levels. Secret services do not tell the full story. They will not reveal their sources, methods or in other ways compromise their own operations. Reports of this kind have most certainly been approved at the political level, and some have introductions by ministers. There are also reasons to avoid or down-play certain topics. This could be to avoid political tension with Russia, or for domestic political reasons. It is not unlikely for instance that Russian exploitation of the refugee crisis in 2015 would be deemed highly sensitive in some countries.

Third, there is question about the type and quality of information. The Baltic services publish substantial reports with details on individuals, political parties and organizations. Other countries' reports provide more general descriptions, with few or no examples or little or no evidence, making it difficult to assess the quality of the information. It is difficult, therefore, to identify the basis for the services' conclusions. The analysis gives a clear picture of the views held by these services, but we do not know if that is influenced by preconceived perceptions, political pressure or other things, nor if the services have genuine intelligence and the analytical capability to back up their claims. Former intelligence chief Sir David Omand has described the multiple ways in which intelligence can be distorted. Sometimes it is based on single sources of varying quality or credibility, or on sources with their own agendas. Assessments might be based on lacking procedures or analysis, or intelligence is politicized or distorted in complex decision-making processes. History has also shown examples of intelligence officials seeing themselves above political processes and compromises, secrecy used to cover incompetence, services following their own agendas, and sheer paranoia (Omand, 2010: pp. 144–146, pp. 252–253, pp. 312–314). This study found no indications of such distortion, but that would also be very difficult to identify. The biggest challenge with these reports is probably the lack of detail and examples. There are obvious reasons for this, but it makes it very difficult to verify the evidence. Sometimes reports leave much room for interpretation. While talking about Russia, the head of the Swedish SAEPO pointed out that conflicts can be won through non-linear warfare, using influence operations and economic pressure (SAEPO, 2016: p. 5). The question then is whether this is an indirect way of telling us that Russia is doing or preparing this, or just a more general observation.

This article will use the official abbreviations the services use themselves in the English language. It is worth noting that the various services have different dating policies, so while the Norwegian NPSS 2018 report was published in February 2018, the German BfV 2017 report was published in July 2018. This study will follow standard academic practice of referring to the year the report was published (Table 1).

Existing literature. There is a large body of research covering this topic. Much first-hand information became available through defectors during and after the cold war, and this is still relevant. Titles like *The Deception Game* (Bittman, 1972), *The KGB and Disinformation* (Bittman, 1985), *Dezinformatsia* (Shultz and Godson, 1984), *Soviet Active Measures and Propaganda* (Romerstein, 1989) and *Disinformation* (Pacepa and Rychlak, 2013) speak for themselves. Other works on Soviet intelligence also covered influence activities in much detail (Andrew and Gordievsky, 1990; Kalugin, 1994; Levchenko, 1989; Lunev, 1998; Andrew and Mitrokhin, 1999; and others). In the 80s the U.S. established the Active Measures Working Group, an inter-agency group to expose and combat Soviet influence activities. The group produced four major public studies and 32 reports that were widely circulated (Schoen and Lamb, 2012: pp. 121–123).

The attention on Russian propaganda and influence activities since the intervention in Ukraine has led to numerous studies. Some have attempted to cover the whole range of Russian influence activities and the tools and techniques employed. The *Handbook of Russian Foreign Policy* (Tsygankov, 2018) describe seven tools: diplomacy, natural gas, intelligence, military, cyber, media and public diplomacy, and the Russian Orthodox Church. In *A Definition of Contemporary Russian Conflict* (Seely, 2018),

Table 1 Western secret services used as sources for the study

Country	Name (English)	Name (national language)
Czech Republic	Security Information Service (BIS)	Bezpečnostní informační služba (BIS)
Denmark	Danish Defense Intelligence Service (DDIS)	Forsvarets efterretningstjeneste (FE)
Estonia	Estonian Internal Security Service (EISS) Estonian Foreign Intelligence Service (EFIS)[a]	Kaitsepolitseiamet (KAPO) Välisluureamet
Finland	Finnish Security Intelligence Service (Supo)	Suojelupoliisi (Supo)
Germany	Federal Office for the Protection of the Constitution (BfV)	Bundesamt für Verfassungsschutz (BfV)
Latvia	Latvian Security Police (DP) Constitution Protection Bureau (CPB)	Drošības policija (DP) Satversmes aizsardzības birojs (SAB)
Lithuania	State Security Department (SSD) Second Investigation Department MoD	Valstybės saugumo departamentas (VSD) Antrasis operatyvinių tarnybų departamentas (AOTD)
Netherlands	General Intelligence and Security Service (GISS)	Algemene Inlichtingen-en Veiligheidsdienst (AIVD)
Norway	Norwegian Police Security Service (NPSS) Norwegian Intelligence Service (NIS)	Politiets sikkerhetstjeneste (PST) Etterretningstjenesten (E-tjenesten)
Sweden	Swedish Security Service (SAEPO)	Säkerhetspolisen (Säpo)
USA	Defense Intelligence Agency (DIA)	Defense Intelligence Agency (DIA)

[a]Until 1 July, 2017, EFIS was known as Estonian Information Board (EIB): http://www.kaitseministeerium.ee/en/news/estonian-information-board-become-estonian-foreignintelligence-service

about 50 tools of state power are grouped into seven elements: political conflict, culture and governance, economics and energy, military power, diplomacy and public outreach, and information and narrative warfare, all bound together by command and control. *Controlling chaos: How Russia manages its political war in Europe* (Galeotti, 2017b) covers the whole range of tools, including intelligence, crime, business, religion, think tanks, media, soft power, diplomacy, military and fronts. *Putin's Propaganda Machine* (Van Herpen, 2015) mentions the use of undercover work, cultural diplomacy, influencing public opinion, PR and lobbying, media, social media, financing politicians, spies, the Russian Orthodox Church, undermining Western alliances, building new political alliances, economic interdependence and use of civil society. In *The Russian Challenge* (Giles et al., 2015) a broad spectrum of instruments was scrutinized, including energy, trade, minorities, cyber, co-opting business and political elites, border disputes, military force and information warfare and propaganda. The 'Kremlin tool kit" (Pomerantsev and Weiss, 2014) is assessed to include disinformation, media, social media, a wide range of alliances, exploitation of divides, use of the Orthodox Church and NGOs, co-option and corruption, PR, covert military force, money, commerce and energy. In *Hard Diplomacy and Soft Coercion—Russia's Influence Abroad*, James Sherr (2013) identified a range of tools used, including military, state and public diplomacy, business, energy, media, and social and cultural dimensions, and a number of tactics, like exploitation of division and vulnerabilities, penetration, co-optation, shell companies and shadow structures, agents of influence, linguistic manipulation, and propaganda.

There is also a large body of literature covering more specific aspects of Russian influence, like energy, cyber, the use of organized crime and secret services and so on. The NATO Center of Excellence for Strategic Communications has published a string of research reports and articles covering influence,[1] and continuous analysis of propaganda and social media activities is provided on a weekly basis by the EU External Action Service's Disinformation Review[2] and by the Atlantic Council´s Digital Forensic Research Lab.[3]

Thus, all the ten lessons of this study have in various ways been covered by previous academic works. There is no agreement on terminology related to influence activities, and different authors have taken different approaches, but other works certainly overlap with the conclusions of this study. Except for diplomacy and the use of border disputes, all the tools and techniques mentioned in these works were also in various ways covered by the reports studied. One reason for this might be that the academic works covered above to a significant degree are based on intelligence sources, either directly, or indirectly through media, leaks, background interviews and briefings, or statements by officials and politicians. This is important, as we are potentially looking at a case of what in intelligence terminology is called circular reporting (Jardines, 2016: p. 26), where a piece of information appears to come from multiple independent sources, but in reality originates from only one source. One important feature of the ten following lessons, therefore, is that they clearly show the views of Western secret services, thus making it easier for future studies to distinguish between different types of sources in a field where information is cluttered by denial, deception and disinformation.

Results

Russia is the main threat. Throughout the reports studied, Russia is described as the main intelligence threat. Some describe China as a similar threat, or as another major threat, and Iran is also often named. In addition, many services point out that opposition groups are targeted by their home countries' intelligence services. BfV also, as the only service, mentions allied activities, including one case of U.S. espionage against Germany, and influence activities against the Turkish community in Germany (BfV, 2016a: pp. 246, 262–263; BfV, 2017a: pp. 277–280).

Russia is also described as the foreign state that tries to influence European politics and decision-making most. The Russian intelligence services are viewed as very competent, and their influence activities are intensive, and it is not expected that they will be reduced in the foreseeable future (BfV, 2018: p. 278; DDIS, 2017: pp. 17, 20; DP, 2018: p. 6; EFIS, 2018: pp. 4, 44–46; NIS, 2018: pp. 19, 21, 30–33; SSD, 2018, pp. 57–59). Several factors might contribute to this: a combination of deteriorating relations and internal Russian challenges (Kanet, 2017; Giles et al., 2015; Lo, 2015), both the capability and long-established habit of using such tools (Tsygankov, 2018; Seely, 2018; Galeotti, 2017b; Giles et al., 2015; Van Herpen, 2015; Pomerantsev and Weiss, 2014; Sherr, 2013), and possibly also because use of coercive influence activities reflects limited Russian options to engage with the West (Tkachenko, 2017). As for China, their focus is mainly on European political decision-making processes, on exile opposition, and on technical and industrial espionage (BfV, 2017a: p. 259). A recent comprehensive study attributed 80 percent of influence efforts in Europe to Russia, with China as the second largest state actor (Vilmer et al., 2018: p. 49).

NPSS explicitly mentions Russia as having the greatest potential to inflict harm on Norwegian interests and threaten

political decision-making processes (NPSS, 2015: p. 15; NPSS, 2018: p. 7). Some use the term "warfare" to describe Russian influence activities in peacetime or talk about "weaponization of information" (Ashley, 2018). The head of SAEPO points out that conflicts can be won through non-linear warfare, using influence operations and economic pressure, and claims Russia is preparing sabotage, spreading disinformation and propaganda, undermining trust in political leaders and media, and negatively influencing public debate (SAEPO, 2016: pp. 5, 62–63). SSD uses the terms "hybrid war" and "psychological information warfare" to describe Russian activities (SSD, 2017b). BIS uses the term non-linear warfare, claiming Russia could destabilize or manipulate the Czech society or political environment at any time, if they so wished (BIS, 2016: pp. 8–9). BIS also characterizes the Russian activity as a hybrid campaign against Ukraine, NATO and EU (BIS, 2017: p. 11).

The Baltic States paint a particularly grim picture, possibly because of their unique history, geography and ethnic composition. The Estonian view is that the Russian regime will remain aggressive, conducting hostile influence operations and consistently cultivating tension and undermining trust in democratically elected governments (EISS, 2016: pp. 2–5; EIB, 2017: p. 7). Russian influence activities in the information domain are seen as the main threat, having a detrimental effect on Latvia´s national security, and subverting democratic processes (DP, 2017: p. 5). Russia´s imperial ambitions and aggressive foreign policy is causing a tense security situation, and Russia is discrediting Lithuania, influencing political, social and economic processes and dividing the Lithuanian society (SSD, 2017a: pp. 7–8).

Political influence activities. Russian influence activities are long-term efforts to ensure Russian political interests and achievement of the country´s objectives. To quote the BfV: "Their government's political agenda dictates the priority areas of the individual intelligence services' activities" (BfV, 2017a: p. 258). Influence activities cover a wide range of spheres, including political, security, military, economic, energy and technological issues. In countries with Russian minorities they also cover ethnic, social and historical issues.

According to the reports studied, Kremlin has three main strategic objectives (EIB, 2017: pp. 4,9,11; DDIS, 2017: pp. 17–21; NIS, 2017: p. 22; SSD, 2017a, 2017b: p. 37; EFIS, 2018: p. 24), perspectives shared by academics like Loftus and Kanet (2017; pp. 14–15, 18–19) and Lo (2015). First, to ensure regime security and maintain their own power. Second, to ensure predominance in Russia's near abroad, usually understood as the former Soviet Union minus the Baltic States. Finally, to secure world-power status for Russia with the commensurate influence and respect internationally. The latter two directly support the primary objective of regime security. Russian influence activities are of a political nature, and logically support the achievement of these strategic objectives. The main and long-term objective is to weaken the two major Western alliances, NATO and the EU. In a short-term perspective, Russia aims to have the sanctions imposed since 2014 lifted (BfV, 2018: p. 275; EISS, 2018: p. 5; NIS, 2018: p. 30; SSD, 2018: pp. 9–10).

GISS describes how Russia drives a wedge between NATO members, and how Kremlin constantly applies a strategy of divide and rule to undermine the unity of EU policy towards Russia (GISS, 2015: p. 12). BIS asserts Russia is disrupting both the coherence of NATO and the EU and Czech-Polish relations (BIS, 2016: p. 9). DDIS's view is that Russia attempts to deepen internal discord and division both in Western countries and within Western organizations (DDIS, 2017: p. 20). According to SSD, Russia makes every effort to fragment the EU and undermine Western unity and trust in Western institutions, including Article 5 of the North Atlantic Treaty. One way of dividing Western societies and dissuading military support to the Eastern NATO members is portraying this as "provoking Russia" (SSD, 2016: p. 7; SSD, 2017a: p. 6). Provocations to test Western solidarity and determination could be employed to create tension (NIS, 2017: p. 35).

BfV gives an illustrative example of how Russia is conducting political influence activities. To counter the sanctions imposed after their aggression in Ukraine in 2014, Russian intelligence was tasked to find out what Russian steps would be completely unacceptable to the German Government; if there were any red lines; what sanctions Russia should expect, and how these could be prevented; if the EU would act as one; and if there were any differences in interests between the government and business (BfV, 2015: pp. 146–148). They would obtain information on the views of the government, political parties and institutions, how they would handle the conflict, and their future policy towards Russia. To prepare their influence activities, they would try to obtain information on the decision-making processes, and to find out to what extent it was still possible to influence them. (BfV, 2016a: pp. 246–7, 254–5). They would then use their contacts to spread the Russian point of view, calm them about Russian policy, and shift the blame for the situation to the West and to Ukraine. In general, Russia would use all available venues to wield influence, including Government, political parties, institutions, business, and the public through media and social media (BfV, 2016a: pp. 254–5). Intelligence priorities change as the political situation changes, and from 2016 Russia would also focus on issues like relations between the EU and Turkey, the EU's handling of Brexit, EU defense and security policy, and possible sanctions caused by Russian bombing in Syria (BfV, 2017a: p. 267).

In addition to the main objective of weakening NATO and the EU, there are more specific objectives related to individual countries. Russia is a major energy exporter and has used this as a tool for political influence on numerous occasions. Unsurprisingly, countries heavily dependent on Russian energy supplies report Russian attempts to influence their energy policy and investment decisions. Likewise, Russia attempts to influence decision-making related to Norwegian energy export (NPSS, 2015: p. 21; 2016: p. 7). Finland and Sweden are non-NATO members, and report more aggressive Russian attempts to influence their security policy. DDIS believes that Russia will influence and deter Swedish and Finnish cooperation with NATO through political means and aggressive rhetoric (DDIS, 2017: p. 18). In Estonia, the areas of interest have remained stable over the past ten years, and include NATO and EU policies, international relations, Estonian politics, defense and security services, and cyber security (EISS, 2017b). In Finland, the main targets of intelligence and influence are relations to NATO, Artic Council chairmanship, EU sanctions, Baltic Sea region security and steps to counter foreign information operations (Supo, 2018: p. 21).

One very worrisome development is the increased Russian meddling in elections, a trend that is expected to continue (EISS, 2018: p. 15; DDIS, 2017: p. 20; SSD, 2018: p. 59). The activities to influence the U.S. presidential election were both complex and more aggressive than anything previously seen. Cyber operations were used to get access to e-mails from the Democratic National Committee, and content seen as compromising and useful to influence the outcome of the election was later leaked (DDIS, 2016: p. 26; BfV, 2017a: pp. 263–64). These operations require a lot more than the capability to hack into e-mail servers or other systems. They also require linguistic skills and intimate political understanding of the target country to assess how such information will be received by the media and political

opponents, and how it will play out to achieve the political objectives of the operation. The likelihood of such use of compromising information could rise in case of political conflicts (DDIS, 2017, p. 12).

The reports studied also claim that Russia conducted cyber-attacks against the Lithuanian parliament (SSD, 2017a: p. 26), was involved in the attempted coup during the 2016 Montenegrin elections (DDIS, 2017: p. 19; EIB, 2017: p. 9), conducted a multi-year cyber operation against political targets leading up to the 2017 German elections, and undermined the campaign of the now French president Emmanuel Macron (BfV, 2017b). The operation against Germany included persistent cyber-attacks against the parliament and political parties, most likely collecting compromising material that could be used to influence elections or political decision-making. However, in hindsight, the German security service found no attempts to influence the election through propaganda or disinformation, and believe this was because of substantial preventive steps taken by Germany (BfV, 2018: pp. 270–271, 276). Legal action has been taken against a large number of Russian intelligence officers, indicating that there is good evidence to support the secret services' claims. Two have been tried in absentia in Montenegro (Bajrovic et al., 2018), and thirteen have been indicted for interference with the U.S. elections (U.S. District Court for the District of Columbia, 2018). Seven officers have been charged with hacking and related influence and disinformation operations in Europe (U.S. Department of Justice, 2018), of which three were also indicted in the previous case, and one with 'political and electoral interference operations" in Europe and the U.S. (U.S. District Court for the Eastern District of Virginia, 2018).

Divide and rule—targeting the population. Influence activities directed at the populations of Europe aim to disrupt and create distrust. The divide and rule approach is to create as many cleavages at as many levels as possible. Russia, as a large power, would then more easily deal with a multi-fragmented Europe (EFIS, 2018: p. 6). We can see three levels of the divide and rule approach. First, at the European level, attacking the alliances, NATO and EU. Second, at the interstate level, creating division and distrust between nations. Finally, at the intrastate level, creating division internally between various groups in individual countries. The lines between these levels are blurred, any activity fueling discontent with the EU can certainly also create division between countries and within a country with an EU-friendly government.

According to SAEPO, Russia is using information operations and disinformation campaigns to influence public opinion and democratic decision-making. One technique is to question the credibility of political leaders, equating democratically elected leaders with authoritarian ones, thus reducing openness and trust in democracy (SAEPO, 2016: p. 63). BfV assess that disinformation and propaganda is used to destabilize the German government (BfV, 2018; p. 276). NPSS describes how intelligence services work actively to weaken confidence in the authorities or sowing division between population groups or regions (NPSS, 2016: p. 8). GISS, under the headline "Divide and rule", describes how Russia´s principal weapon is to amplify Europe´s own internal divisions, assessing Russia is running a global campaign to influence public opinion (GISS, 2015: pp. 12, 30).

The main venues to reach the general population are media and social media. In addition, as will be covered later, Russia also uses minorities and refugees, businesses and front organizations. Russian propaganda and disinformation operations are extensive, and large and well-resourced media outlets are loyal tools for the Russian government (SAEPO, 2016: p. 63). TV is under complete control, and the Presidential Administration provides editors-in-chief with instructions weekly, detailing topics and key phrases to be covered (EIB, 2016: p. 23). The most prominent foreign language media are RT and Sputnik, operating in numerous languages. Russia communicates trough TV, radio, the Internet and public events, and employs paid journalists in Western and other media (DIA, 2017: p. 39). In spite of substantial resources, the effectiveness of the media activities is questioned. Russian language media content is not necessarily relevant for Russian minorities in places like the Baltic States, and ratings indicate that RT and Sputnik are not particularly effective (SSD, 2017a: pp. 2–3,5).

The importance of social media is increasing. They can be used remotely with hidden identities, spreading pro-Kremlin information, disinformation and comments, and mobilizing and organizing protests, especially on issues important to Russia, like the shooting down of flight MH17 over Ukraine (GISS, 2018: p. 9). In another case, Russian media and social media claimed Latvia was a staging ground for aggression, and that nuclear weapons would be placed in the country (DP, 2018: pp. 23–26). Sometimes a flow of comments is posted to manipulate opinion or disrupt discussions on social media (BfV, 2016a: pp. 254–5). Russia is also using so-called bots, automated accounts pushing content on social media (DP, 2018: p. 25; DIA, 2017: p. 40). They can support other users or spread particular messages, and drown out real content and disrupt genuine conversation. Mapping of social and professional relations, and infiltration of friend´s networks on social media is done to enhance dissemination of disinformation and propaganda. Action has also been taken to reduce the influence of opposing voices. This includes harassment and high-jacking of social media profiles, mass-fabrication of false complaints on Twitter and Facebook to shut down accounts, and slander and threats via SMS and voice. On one occasion, in 2015, thousands of Polish militaries received calls from a Russian number, apparently trying to demoralize personnel (NIS, 2017: p. 34–7). Other sources support the views of these secret services. The EU vs. Disinformation campaign has identified 3 800 cases of disinformation and issued more than 100 newsletters analyzing the issue (EEAS, 2018). Likewise, Twitter released an archive of nine million tweets by fake accounts affiliated with a Russian troll factory, directing polarizing content against British, French, U.S. and other audiences (DFRL, 2018).

There is apparently also a myriad of Russian-supported news outlets integrated with social media activities. It is claimed the Baltnews portals in the Baltic States are financed through outside front enterprises, and linked to Russian mainstream media, working together to spread disinformation. These outlets are provided with hacked material, falsified opinion polls, and technical support to ensure optimal reach and spread of information. In one case, hacked information from the website of the Lithuanian Armed Forces was misrepresented, and the claim that Lithuania had intentions to annex Kaliningrad was spread through local outlets and eventually to Russian media (EISS, 2016: pp. 8–9; SSD, 2016: p. 38). Russian media also claimed the Baltic States would receive U.S. nuclear weapons (DP, 2018: p. 26).

BIS is of the opinion Russia has covertly infiltrated media and the Internet and used Czech organizations and individuals to spread massive amounts of propaganda to create internal tension and undermine NATO, the EU and the US. Other activities have been aimed at creating tension with Ukraine and Poland. Activities are also played back to Russia, where disinformation from external sources aim to create a threat perception among the Russian population. A range of techniques are used to disrupt and create distrust, including disinformation, information overload, relativization of truth, claiming that "everyone is lying",

supporting populists and extremists, spreading rumors and using fear of war with Russia as a possibility. (BIS, 2016: p. 9).

There seems to be a clear difference in the assessment of both the scale and the aggressiveness of these activities between the Baltic States and the Czech Republic on one hand and the other secret services on the other. Whether this is caused by different relations or different perceptions is hard to say. There are also contradicting views within these reports. The Estonians assess that the effectiveness of media projects is low because the visible reality, living standard, and peace and stability for Russians in Estonia is very different from the picture provided by Russian propaganda (EISS, 2017a: p. 9). On the other hand, in Lithuania the attempt to control the Russian language information space is seen as a very serious threat, and they point out that the majority of Russian-speaking Lithuanians rely exclusively on Russian-controlled media (SSD, 2016: p. 8). However, in another report it is claimed Lithuania is an unfavorable environment for pro-Russian journalists, that their activities are becoming less effective, and that the possibilities to expand their audience remain limited (SSD, 2018). Writing on Russian media and public diplomacy, Simons has noted that analyses of Russia is 'tinged with assumptions and projections that are simply not there" (2018: 207), while others emphasize that propaganda and manipulation are essential tools of Russian influence (Giles, 2016; Pomerantsev 2015; and many other). Continuous reporting from NATO, EU and the Atlantic Council certainly support the latter view[4]

Divide and rule—minorities, refugees, and extremists. Many countries promote their culture abroad through organizations like the British Council or the Goethe Institute. In most cases this is seen as benevolent, soft power activities that rely on attraction. The Russian approach is to mix their cultural activities with their intelligence activities to create an important foreign policy tool (EISS, 2017c). Compatriots, the Russian minorities abroad, thus become a tool for the Russian government, viewed both as supporters and implementers of Russian foreign policy.

Russia has comprehensive resources and a complex set-up of organizations at its disposal. There is a federal agency, Rossotrudnichestvo, the organization Russian World, and various funds promoting their compatriot policy. Abroad, at the receiving end, there is an array of foundations, think tanks and NGOs supported by Russia. These front organizations promote various Russian narratives to subvert and create division, rewrite history, and use and abuse culture to legitimize the Russian view, and then propagate it through local Russian-supported media projects or mainstream media. Sometimes they even support extremist groups. One key element is promotion of the idea of the so-called "Russian world", the places where Russians live and where Russia has special rights and the obligation to protect their compatriots. Support is also provided through Russian embassies, secret services, businesses, or other non-transparent channels. DP describe this as humanitarian influence measures (EISS, 2016: pp. 6–7; DP, 2018: pp. 5, 13–21).

In some countries, like Estonia and Latvia, compatriots make up about 25 percent of the population, and a comprehensive Swedish study concluded that Russian minorities in the Baltic States are used in a comprehensive strategy as tools of destabilization (Winnerstieg, 2014: pp. 4, 143). After the annexation of Crimea, obscure hostile resistance movements appeared in the Baltic States, with the so-called people´s republics of Vilnius, Latgale and Baltic Russians. They operated websites and social media, and caused concern about a repetition of the Ukrainian scenario, similar to the Peoples Republics of Donetsk and Luhansk (SSD, 2017a: p. 29). The divide and rule approach is not only limited to compatriots. Russia has attempted to disrupt Czech-Polish relations (BIS, 2015: p. 9), and to fuel ethnic conflict with the Polish minority in Lithuania. In 2017, the Russian-funded *sputniknews.lt* and *baltnews.lt* were used in an attempt to increase inter-ethnic tension and degrade relations between Poland and Lithuania (SSD, 2018: p. 42). Poles, like Russians, have been presented as culturally and linguistically persecuted, and propaganda and disinformation has been used to create distrust between communities. This is used to support exclusive rights for minority groups and claims for Polish and Russian cultural autonomies in the Baltic States. Russia has also attempted to weaken leaders of the Tatar minority in Lithuania, and to replace them with people that would support the annexation of Crimea (SSD, 2017a: p. 29).

The European refugee crisis was used to undermine public confidence in local authorities, the EU and NATO. It was claimed that NATO operations in Libya and Iraq caused the crisis, and that refugees would cause the collapse of Schengen, terror and demographic changes. Far-right protests were also presented as a positive resistance against the EU (SSD, 2016: pp. 46–7, 51). In the so-called Liza incident in Germany in January 2016, Russian media and various groups spread the rumor that a 13-year-old girl of Russian origin had been raped by immigrants, causing widespread demonstrations. This was further reinforced by aggressive statements from the Russian foreign secretary Sergey Lavrov. The purpose of this disinformation was to divide the German population, undermine trust in the media and the government, further inflame the debate about refugees, and thus strengthen pro-Russian parties and groups in Germany (BfV, 2017a: p. 268). However, sometimes the Russian efforts are counter-productive. What might have seemed, from Moscow, a successful operation, in the longer run damaged political relations with Germany and made society more aware of the threat (EIB, 2017: pp. 17–18).

The Estonian view is that Russian secret services systematically try to find or create tension within the society, and that Russia used the refugee crisis to put pressure on the public and on governments to split the EU. War and violence in Syria, with Russia as one of the main players, would increase the refugee flow to Europe. Russia would then provide financial, ideological and media support to populists opposing the migrants, and at the same time support leftist populists, based on historical and ideological ties. These three groups, refugees, national populists and leftist populists, would then be pitched against each other, creating splits and division within the EU (EIB, 2016: pp. 10, 44; EISS 2017a: pp. 5–6).

The Baltic States are more explicit than others about Russian use of the refugee crisis. It is unclear whether this reflects a difference in opinion, or a reluctance by others, for political or other reasons, to publicly discuss the issue. For instance, GISS would be very explicit about the challenges and tension caused by the refugees, and about Russia as a genuine threat to Dutch security through aggression and clandestine influence activities. They also point out how Russia uses the war in Syria to claim a place on the world stage, influence the EU and the US, and how this has been enhanced by the refugee crisis, without explicitly connecting the dots (GISS, 2016: pp. 1, 9–10, 25–6).

Russia also develops links to radical left and to right-wing groups (EIB, 2017: pp. 18–19), providing political and information support (SSD, 2018: p. 39), and exploiting the threat of terrorism to damage the West (EISS, 2018: p. 2). One example is the World National Conservative Movement, an international network of radical and anti-immigration activists, creating tension and putting pressure on European decision-makers in line with Russia's divide and rule approach (DP, 2016: p. 16). There is a plethora of Russian-supported or pro-Russian

extremist groups in countries with large Russian minorities. In Lithuania, school children set-up a team called the "Striking Battalion of Death" and took part in military simulation training and competitions (SSD, 2015a: p. 46). In Latvia, pro-Russian groups engaged in propaganda activities, provocative demonstrations, passport burning, hooliganism, anti-homosexual protests and anti-refugee protests (DP, 2017: pp. 14–16). Pro-Russian right-wing extremist groups and paramilitary groups were reported in the Czech Republic (BIS, 2016: pp. 11–12), and also Sweden reported Russian attempts to influence public opinion and political decision-making through support for extremist groups (SAEPO, 2016: p. 63). Sometimes too few extremists are available, and in one case a heavily tattooed Russian skinhead was sent from Saint Petersburg to a manifestation in Estonia as a "local Nazi activist" (EISS, 2017a: p. 8). As a whole, the threat from both left and right-wing extremists appears low, as these groups are usually small, fragmented, relatively isolated and lacking leadership (BIS 2016: pp. 11–13; DP, 2017: pp. 16–17; EISS, 2017a: p. 4; SSD, 2018: p. 39).

Covert tools of influence—human intelligence. The two main covert tools for information collection and influence activities are human intelligence (HUMINT) operations and cyber operations. Russian intelligence operatives are described as extremely professional with a high degree of operational capability and skilled in the use of propaganda and clandestine operations to exert influence (GISS, 2016: p. 26). Recruited agents can be used to access important information, but also to spread propaganda and influence decision-making (DP, 2016: p. 8; SSD, 2018: p. 26). Officials involved in decision-making or with direct access to important information are often aware of security risks and difficult to recruit. As a result, operations might be directed against people with access to decision-makers, including advisors, friends and family (NPSS, 2017: p. 21). DP assesses mid-level officials and representatives of political parties as most exposed to recruitment (DP, 2016: p. 7), while GISS assesses political and business communities as the main targets, but note that recruitment efforts are comprehensive, including culture and media (GISS, 2015: p. 30).

BfV indicates four criteria used by Russian intelligence. First, people that stay in Russia for longer periods of time. Second, people with good knowledge of Russian. Third, students that later might work in interesting public or business positions, and finally, people aiming at a career in politics, diplomacy, or business, particularly in the energy sector or in finance (BfV, 2016 b). People traveling to Russia, might be exposed to provocations and compromising situations, or available for cultivation (GISS, 2015: p. 30; SSD, 2017a: p. 17; NPSS, 2018: pp. 8–9), and cross-border cooperation projects are often used as cover (DP, 2017: p. 8). People might be recruited, blackmailed or infiltrated into organizations or positions where they can influence decision-making. Russia also encourages or coerces, directly or through family, own nationals living abroad to provide services (NPSS, 2014: 13–14; NPSS, 2017: p. 9).

Operatives use a variety of covers. The most common one is to operate from embassies, consulates, trade missions and so on, and typically, one third of diplomats are intelligence officers (SAEPO, 2018: p. 25; SSD, 2018: p. 25). So-called "illegals" have false identities and install themselves for long periods of time in foreign countries. To minimize risk, operatives also work cross-border from other countries or Russia, often meeting their sources in third countries. Some might work for other Russian state institutions or businesses like airlines, marketing organizations, or research establishments, or various other organizations. Working as a journalist gives ample excuse for digging around, including with regard to potentially sensitive issues like military activities (SSD, 2015a: pp. 23–7; DP, 2016: p. 8; BfV, 2017a: p. 286). There has been relatively little scholarly analysis of the role of the secret services in Russian foreign policy. They probably still play a significant role, but historically the Soviets were more successful in the technical than in the political sphere (Strokan and Taylor, 2018), and more recent analyses also point to limited political understanding and much infighting between the Russian services (Galeotti, 2016b). One key role is the so-called 'active measures", the various types of foreign manipulation and influence activities (Soldatov and Rochlitz, 2018), including the use of criminal networks (Galeotti, 2017a).

Covert tools of influence—cyber operations. The other main covert tool for intelligence and influence operations is cyber operations. Over time cyber activities have been given a greater role compared to human intelligence (BfV, 2017a, 2017b, 2017c: p. 259). Cyber operations can be carried out from abroad, and they are both effective and less risky than traditional human intelligence operations. (DDIS, 2016: p. 26). Developed countries offer plenty of vulnerabilities for cyber sabotage, and election campaigns are increasingly conducted on social media. The risk for disinformation campaigns and cyber-attacks against policy-making, political institutions and parties should therefore be taken particularly seriously (BfV, 2017c). As a tool for influence activities, cyber has several applications. First, gathering the background information necessary for the conduct of influence activities. Second, supporting social media and media activities as covered in a previous paragraph. Third, conducting more complex influence activities, like the hacking and leaking of information to influence the U.S. presidential election. Finally, using cyber sabotage as a tool of coercive influence in times of crisis. Others have made similar observations, claiming cyber can be used for 'intelligence collection, political-psychological warfare, deterrence signaling, discrete sabotage, combined-arms military attacks, and campaigns of mass disruption". (Perkovich and Levite, 2017: p. 250).

Cyber operations are conducted both by intelligence services and by elements controlled by these services, including criminal networks, activists and patriotic hackers. Commercial IT companies can also work for governments, conducting cyber-attacks or buying or managing necessary infrastructure (GISS, 2016: p. 23). Such use of proxies enables Russia to deny any links to the operations, while still appearing aggressive and putting pressure on its opponents (NIS, 2017: p. 35); others have also described the use of proxies in detail (Maness and Valeriano, 2015).

According to the reports, Russia is increasing its capabilities and concepts for cyber sabotage, and has a long-term perspective, mapping vulnerabilities in systems and infrastructure to maximize its ability to demonstrate power in future conflicts. When a malicious code has been introduced into a system, such attacks have been described as a "silent ticking digital bomb" (BfV, 2017a: p. 260), and attacks to paralyze vital infrastructure are considered a real threat (GISS, 2018: p. 10; Supo, 2018: p. 22). Cyber sabotage is a tool of influence, by creating chaos and exerting pressure in times of crisis (NIS, 2017: pp. 34–5), and also described as a component in the preparation for non-linear warfare, together with cruise missiles, information warfare and psychological operations (SAEPO, 2016: pp. 62–3). In its influence role, the destruction caused by sabotage is usually not the purpose. The real purpose would be to exert pressure directly on a government, or indirectly by undermining popular confidence in authorities, or creating fear or confusion among the population or military forces.

The reports studied describe several examples of cyber sabotage. Attacks on telecommunications, energy, power grids and other critical infrastructure can have both physical and psychological consequences. Broadcasting and digital media could be attacked to manipulate public opinion or affect decision-making processes. A large-scale attack on power grids took place in Western Ukraine in December 2015. The networks of several Ukrainian energy companies had been infiltrated for months, and about 500.000 people lost their power supply for an average period of 1 h. To increase the effect of the attack, the telephone hotlines of the energy companies were also jammed by a DDoS attack (BfV, 2017a: pp. 264–5). The likelihood of such cyber sabotage is seen as low, but could rapidly increase in times of conflict (DDIS, 2016: p. 26). Russia was also behind sabotage of the IT system of a rail company in Ukraine in 2016 (NIS, 2018: pp. 30–31), and was also linked to the cyber-attack on the French station TV5 Monde in January 2015 (DIA, 2017: p. 39). Other studies have characterized Russia as the most dangerous state in cyberspace (Maness and Valeriano, 2015: p. 208), and Stephen Blank claims Russia has incorporated cyber strikes and information operations into information warfare, that this has been a vital factor in all its conflicts since 2000, and that its capabilities have gradually evolved through operations in Estonia, Georgia, Crimea and Eastern Ukraine (2017).

Energy, business, and corruption. Russia's role as a major, sometimes the only energy supplier, is a key venue for influence. Maintaining control of energy supply is, therefore, a major objective, serving three purposes. First, it gives direct political influence as threats to turn off energy supplies may be made. That said, it would also involve huge economic and political consequences for Russia. Second, it gives Russia a major economic and therefor political role, involving energy, infrastructure, transit and transportation. Third, energy is the major source of income for the Russia, and therefore essential to maintain political stability (SSD, 2016: pp. 8, 32–34).

The major obstacle for Russia is the EU energy policy and integration of energy markets across Europe. Russia, therefore, exploits disagreements and makes every effort possible to weaken support for this policy (DDIS, 2016: p. 11), including the use of bilateral relations and lucrative economic offers, media and lobbying to promote its own and undermine other sources of energy. Such efforts can be directed at legislative processes, at decision-making regarding investment and policies, or public opinion. CPB regards Russian lobbying efforts as more effective than their media efforts (CPB, 2017: p. 3). Russia has used all levers available to promote the construction of the Nord Stream 2 gas pipeline, going directly to Germany through the Baltic Sea and thus around Poland and the Baltic States. Lithuania was totally dependent on Russian gas, and Russia actively worked against a new liquefied natural gas terminal and electricity interconnections with Sweden and Poland. Another example is the substantial effort to influence investment decisions and nuclear fuel supply in the Czech nuclear power industry. Corruption within government bodies or in strategically important sectors like energy, infrastructure, transportation and information technology, might be a threat to national security. This is particularly the case in larger strategic state-owned companies and foundations, where decisions often have both substantial financial and strategic consequences. Corruption is characterized as particularly dangerous if it hampers strategic investments, involves strategic infrastructure, or is used to influence major economic or political decisions (BIS, 2016: pp. 4–5, 8; EISS, 2016: pp. 3, 34–35; EISS, 2018: pp. 32–33).

Russia also attempts to maintain a grip on critical infrastructure, including pipelines, ports, terminals, railway infrastructure and electricity grids and interconnections. The Russian energy industry is used as a political tool, where decisions can be made based on political objectives and not only business potential or profit (BIS, 2016: pp. 4–5, 8; DP, 2016: p. 25; SSD, 2016: pp. 32–35, 37; EIB, 2017: p. 21). Business in general can serve as a platform for economic dependence and to counter sanctions. Consultancies have good connections and thorough understanding of political processes and decision-making, and can therefore, wittingly or unwittingly, be useful venues for influence (NPSS, 2015: p. 17). Norway is a substantial supplier of energy to Europe, and Russia therefore tries to influence decision-making in line with its political objectives. Russia might, in times of crisis, disturb or create uncertainty about Norwegian energy deliveries to Europe (NPSS, 2015: p. 21), and the sabotage threat should be assessed with respect to its consequences for Europe, both directly and as a means of influence (NPSS, 2017: p. 8). While there is broad agreement in general on the importance of business and energy as tools of influence (Collins, 2017; Maness and Valeriano, 2015; Sherr, 2013; and others), the question of how it plays out is more complex. Barkanov sees economic factors as subordinate to politics mainly 'when strategic interactions sour" (2018: p. 147), and others point out that there is a considerable structural overlap between politics and business, and also many competing interests between state, businesses and influential individuals (Gvosdev and Marsh, 2014: pp. 39–45).

FSB controls Russia's borders, and cross-border activity is virtually impossible without the consent of the FSB. This is exploited, either to pressure people through fictitious charges, or by granting criminals and smugglers licence to operate if they also work for the FSB (DP, 2016: p. 8; EISS, 2016: pp. 18–19; SSD, 2016: pp. 25–27; EISS, 2018: p. 13). Some smuggling groups are directly controlled and used by the FSB (DP, 2018: pp. 8–9). FSB actively monitors Russian investments in foreign countries and foreign investments in Russia. Businesses risk manipulation and blackmail, and FSB establishes both intelligence and corruption-based ties with foreign businesses (DP, 2016: pp. 8, 10; SSD, 2017a: p. 14). The views of the reports studied are shared by organized crime expert Mark Galeotti, pointing out the very close integration between Russian secret services and crime groups, and that they are used for a range of tasks, including political influence, cyber, illegal financing, assassinations, logistics and border crossing (2017a).

Allies and front organizations. During the Cold War front organizations were defined as 'ostensibly independent, non-governmental organizations that, in reality are Soviet-controlled. They function as disguised instruments of Soviet foreign policy, and are particularly useful for those wary of Soviet initiatives." The Soviet Union maintained more than a dozen international fronts, friendship societies, academic institutes, peace forums and other groups, (USIA, 1988: p. 57). Russia seems to continue this practice and will normally disguise state involvement by using non-state or Western actors (DDIS, 2017: p. 20). As previously described, Russia is using minorities as a tool for political influence, and front organizations are therefore often established among minority groups.

There are at least five categories of allies and front organizations: civil society and political activists, academic and research organizations, the media, extremist groups, and businesses. There is certainly a degree of overlap and synergies, and some fall into several categories. Civil society organizations advocate political issues, organize political influence activities and manifestations, and can serve to segregate Russian minorities, create tension and

undermine the EU and NATO (EISS, 2017a: p. 6). There is a range of interest groups, foundations, war veterans, NGOs, and in some cases political parties. It is claimed that Member of the European Parliament and leader of the Latvian Russian Union party Tatjana Zdanoka tries to polarize and split the Latvian society, and also that other named individuals and organizations work for Russian interests (DP, 2018: p. 18). Occasionally, fronts also reach out to international organizations, as when Russian-funded Russian School in Estonia and Legal Information Center for Human Rights took part in 2016 OSCE meetings, promoting anti-Estonian propaganda. Cooperation in areas such as culture or education can also be used to increase political tension. Sometimes Russia offers money to foreign political parties, or lucrative positions in companies to former politicians (DP, 2017: p. 12; EISS, 2017a: pp. 7–8).

Academic and research organizations legitimize and support views and issues desirable for Russia, and also provide the basis for debate and political influence. This category can also include various foundations, think tanks and history projects, and they sometimes perform much of the same functions as civil society organizations (EISS, 2017a: p. 6). The three other categories have been covered in previous paragraphs. Media promote the narrative, reach out to the public, and support political influence activities. Extremist organizations serve mainly to create tension within a society, while business creates dependence, and can also be used for specific purposes through consultancies or IT companies.

Identifying an organization as a front is challenging. Some are directly or indirectly financed and organized by Russia, but proof of this is very rare, even though claims abound. Others are ideologically or otherwise motivated, but sympathizing with Russia is not illegitimate, and it is very difficult to distinguish those working for their own causes from those that in various ways work for Russia. A much-featured case is French National Front's (since 2018 National Rally) 9-million-euro loan from a Russian bank. The party has been outspoken in its criticism of Western sanctions and supportive of Russia on several occasions. However, the explanation for taking the loan was simply that no French bank was willing to lend the money.

Maintaining a network of allies and front organizations is an important piece of the Russian influence apparatus. It reaches into the political debate and structures of foreign countries, provides legitimacy, and the direct or indirect involvement of Russia is obscured or deniable. However, it is not necessarily a simple task to organize and maintain these structures. Despite increased efforts lately, it is still difficult to recruit younger people even in countries with large Russian minorities. Financing is becoming tighter, and corruption and individuals' personal interests make these activities less than optimal. Longstanding attempts to organize the Russian diaspora in the Baltic states has overall failed because of divergent interests among age groups and organizations, growing awareness of Russia´s real objectives, and lack of credibility of the Russian rhetoric (DP, 2017: pp. 12–14; EIB, 2017: p. 21; SSD, 2017a: p. 3; DP, 2018: p. 19; EISS, 2018: pp. 4–8; SSD, 2018: pp. 2–3).

Of the reports studied, only the Baltic services pay much attention to allies and front organizations. It was well documented during the Cold War, but seems to have been ignored by the other services since. A comprehensive Swedish study supports the views of these Baltic secret services and describes the Russian activities in the Baltics as tools of destabilization (Winnerstig, 2014). Pomerantsev and Weiss (2014) draw the link from Soviet practices to the current Russian approach in the rest of Europe, and Van Herpen (2015) exposes the same types of activities and goes into much detail about Russian fronts in Germany and France.

Reconstructing reality, rewriting history. As a platform for their influence activities, Russia is trying to reconstruct current reality and rewrite history to serve its purposes, to legitimize its views and actions, and to undermine those of its opponents and neighbors. Russia's allies and front organizations are instrumental in this work, giving the impression that one receives the opinions of fellow citizens, while Russian diplomats and secret services act as organizers and instigators (BIS, 2015: p. 6; BfV, 2016a: pp. 254–5). One key element of this technique is to blame the current situation on Western hostile actions and ignorance, and create the impression that Russia is only reacting to Western aggression (EIB, 2017: pp. 7–8). Veterans' organizations, memorials and celebrations are used as tools for political pressure and to cause tension between various ethnic groups (EISS, 2018: pp. 7–10).

For the Baltic States, with their large Russian minorities and long history, Russia has developed a comprehensive narrative covering both the past and the present (DP, 2016: pp. 12–13, 18; SSD, 2016: pp. 36–37, 44–45; DP, 2017: pp. 12–19; EISS, 2017a: pp. 10–11). It is focused on the Baltic States' support of Nazism, and the Soviet Union as the savior and winner of World War II, while at the same time omitting Soviet oppression, occupation and deportations. The key themes of Russia´s description of the current situation in the Baltic States are that the Baltic States and NATO are aggressive and a threat to Russia; that these are failed states that, politically and economically, and depend on good relations with Russia; that Russophobia, discrimination and human rights abuses are widespread; and that Nazism and fascism are returning.

Russian embassies have established coordination councils to organize and finance the work of local organizations. Such groups often have verbose names, like the Center for the Protection and Research of Fundamental Rights in Lithuania, and the Legal Information Center for Human Rights in Estonia. Russia is also behind apparently international organizations like World Without Nazism, that are mainly preoccupied with accusing the Baltic States and Ukraine of Nazism and generally supporting the Russian narrative.

Also, others have observed Russian large-scale manipulation of information (Pomerantsev, 2015), and how this is used both to undermine Western will and justify Russian action (Giles et al., 2015: pp. 46–48). Pomerantsev has also masterfully described the absurd level of manipulation internally in Russia (2015). These narratives about both the present and the past are based on a mix of accusations, reinterpretation of history, and disinformation. They serve to weaken the Baltic States' independence, undermine NATO, the EU, and the countries' membership, discredit the countries internationally, legitimize Russia´s aggressive foreign policy, promote the idea of a "Russian world", and to gain equal status for the Russian language. This approach to reconstruct reality can also be employed more generally on other issues relevant for Russia, like sanctions or NATO missile defense.

Military force—their ultimate tool of influence. Military force is also a major tool for political influence, through its sheer existence, and obviously this is the case in times of crisis and conflict. Russia has invested heavily in its military capabilities over several years, and has demonstrated its increased will and ability through the annexation and destabilization of Ukraine, and the war in Syria since 2015. Conceptually, military force has several applications as a means of political influence, and that is before any shots are fired. First, their nuclear capabilities are their ultimate tool of deterrence and intimidation. Second, the ability to conduct long-range non-nuclear strikes against targets abroad is a serious threat. Third, Russia´s increased ability to reduce its neighbors' freedom of action and access to areas close to Russia, and finally,

as a messaging tool and a coercive political instrument through demonstration of military force.

Russia´s strategic nuclear deterrence is based on a triad of intercontinental ballistic missiles, air-launched missiles, and their strategic submarines, mainly located at the Kola Peninsula and operating in Northern waters (DDIS, 2016: p. 17; NIS, 2018: p. 21). This capability is of fundamental importance to Russia, and the only area where Russia has an equal status with the U.S., and it is used as a means of deterrence against nuclear as well as conventional threats.

The introduction of new long-range precision strike missiles adds a new "non-nuclear strategic deterrence" to the nuclear one (NIS, 2018: p. 21). Air-launched Kh-101 and sea--launched Kalibr missiles, with a range of up to 2500 km (DIA, 2017: p. 78; SSD, 2018: p. 13; EFIS, 2018: p. 19), were demonstrated with much media attention in Syria in 2015, and later deployed to the Baltics (DDIS, 2016: p. 16; DDIS, 2017: p. 19). These missiles add a new and credible capability that can strike targets in most of Europe. The previously described increasingly aggressive cyber capabilities can be employed as another long-range capability.

New weapon systems with the capability to restrict neighbor´s freedom of action and NATO's deployment of forces have been deployed to the Kola Peninsula, the Baltics and the Black Sea. Capabilities, with the range of up to 500 km, include S-400 (SA-21) air-defense systems, Bastion and Bal anti-ship missiles, and Iskander surface-to surface missiles (DDIS, 2016: p. 15; SSD, 2018: pp. 13–14). Similar weapons are also mounted on naval vessels. These so-called A2/AD (Anti-Access/Area-Denial) capabilities, together with long-range aviation and information operations, could be used to isolate an area of conflict and control escalation (DIA, 2017: p. 32–4; EIB, 2017: p. 41). Countering these capabilities will require a strong political will and the will to risk significant losses, thus giving Russia a local strategic advantage even though it is in general inferior to NATO (SSD, 2016: pp. 16–17; SSD, 2018: pp. 13–14).).

Finally, military force can be used for deterrence, strategic signaling, psychological pressure and coercion, increasing the impact of their rhetoric and political communication. The build-up of ground forces, along with the new systems mentioned, in the Baltics and close to the Ukrainian border demonstrates that these are parts of Russia´s sphere of interest and that others should respect Russia´s security interests (SSD, 2016: p. 15). It is Russia´s intention to deter NATO from increasing its military presence, and to deter Finland and Sweden from applying for NATO membership. Russia has also used low-flying fighter aircraft to deter Western military operations in international waters. In 2016, this was used to demonstrate that they would not tolerate a U.S. destroyer sailing close to Kaliningrad (EIB, 2017: p. 42).

The utility of military coercion is increased by several aspects of the Russian authoritarian political system. First, power is centralized, so decision-making and the use of force is potentially very rapid. Second, the leadership is bold and willing to take substantial risk even though its military capabilities are limited (DDIS, 2016: p. 11; DDIS, 2017: p. 21). Both these aspects were demonstrated in Ukraine and Syria. Third, the Russian elite is convinced it can only defend its interests from a position of strength, which leads to a constant demonstration of military threats. Furthermore, coordination between the various branches involved, and between military and civilian actors is improving. In addition, Russia has proved itself very apt at masking its intentions and actions. At the political level, this is done through disinformation and denial. At the military level, they are capable of very rapid troop deployments, covering their movements and removing insignia, as seen with the "little green men" in Crimea (NIS, 2017: p. 14). Russia is also capable of conducting snap-exercises with little or no warning time, increasing uncertainty and the potential for coercion.

While some argue that Putin has a master plan to destroy Europe and achieve regional hegemony (Schoen, 2016), more sober voices acknowledge that a strong military is an attribute of a great power, and one of a range of tools (Giles, 2016). They also point out that military force is used for limited political objectives, complementing the use of other tools like subversion and propaganda (Konyshev and Sergunin, 2018; Tkachenko, 2017). Mark Galeotti has used the term 'heavy metal diplomacy" to describe the use of military threats, wargames, deployments, intrusions and provocations, but emphasizes that these are political and not military moves and part of a range of coercive instruments for political influence (2016a).

How serious is the threat?. These reports give the impression that Russia has a large and complex arsenal of techniques, providing multiple, advanced and flexible venues for influence. However, they also describe several dysfunctional sides of the Russian society that are of relevance to the effectiveness of their influence activities. Russia is facing substantial economic and social challenges, corruption is widespread, and economic downturn limits freedom of action (NIS, 2018: pp. 10–11). Its claim to be a world-power rests on weak foundations, politically, economically and militarily, and its partners distrust its intentions (DDIS, 2017: p. 17). Internal political tension is growing, the elite is concerned with possible large-scale demonstrations, and parts of society see the stagnated, kleptocratic system as their main obstacle (EFIS, 2018: pp. 4–6). Their military is marred by neglect, corruption and theft, the increase in disciplinary violations indicate low morale, and turnover is high. (EFIS, 2018: p. 20).

With these dire descriptions, it is tempting to ask how likely is it that an authoritarian, corrupt and dysfunctional country also has world-class secret services running high-end influence operations. It is difficult to win an election or influence a political issue in your own country. Doing so from outside with covert means is certainly a challenging task. Through this article we have seen that their propaganda often does not correspond to the realities most people observe. Their effort is often not successful, even in places like the Baltic States, where they have a long history and a large Russian diaspora. Russian attempts to mobilize their diaspora there have largely failed because of a growing awareness of Russia's real objectives, and because the organizations involved often have a self-interest and waist resources. (DP, 2017: pp. 12–14; EIB, 2017: p. 21; SSD, 2017a: p. 3; DP, 2018: p. 19; EISS, 2018: pp. 4–8; SSD, 2018: pp. 2–3). Russian aggression has also made Western societies acutely aware of the problem and thus more resistant, the so-called Liza case alerted the German authorities and population to the threat of Russian meddling in political affairs (EIB, 2017: pp. 17–18), and human intelligence operations are struggling because of greater public awareness and because of the deteriorating security situation (NPSS, 2016: p. 7). EU energy policy has gradually reduced Russia's ability to use energy as a political tool. Steps taken include gas and electricity interconnections, new sources like LNG terminals, and increased transparency and market regulation (GISS, 2015: p. 12; SSD, 2016: pp. 8, 34, 37; DP, 2017: p. 28).

Some reports give contradicting impressions, and the latest Lithuanian one is an illustrative example. Throughout its 60 pages, Russia is portrayed as a major threat, but numerous examples also indicate that Russia is not particularly successful (SSD, 2018: pp. 4, 5, 37–43, 48): 'The influence of pro-Russian organizations remains limited, Lithuania is an unfavorable environment for pro-Russian journalists, their activities are

becoming less effective, the possibilities to expand their audience remain limited, Russia's compatriot policy is not particularly effective, extremist groups have become weaker, information attacks have had a negligible impact on attitudes to NATO, and the efforts of lobbyists and diplomats have not been successful." How effective can their secret services be, and how well coordinated can their 'whole-of-government approach" be in such an authoritarian, corrupt and dysfunctional system? Assessing the impact of communications is notoriously difficult. Some claim it is easy to understand the measure of activity, but much more difficult to measure the effect with any precision (Simons, 2018: p. 207), and NATO has struggled even to understand the effect of its own activities (Risso, 2014: pp. 253–255). The about 40 reports studied do not give the answer, only indications, so it might be useful to look to history, and other academic work on this issue.

The Soviet Union took a very long-term perspective on its influence activities. The former journalist and KGB propaganda expert Yuri Bezmenov described their four-step subversion process after he defected (1983). First, there would be a long demoralization phase, taking subversive action against a society over a period of 15–20 years. Second, there would be a destabilization phase of two to five years, exploiting conflict lines in areas like the economy, law and order, the security apparatus, the media and so on. In the third phase, this would be escalated into a crisis where society would cease to function normally, creating the pretext for intervention and a regime change. Finally, there would be a normalization phase, solidifying the gains under Soviet control. The Soviets never succeeded, and none of the countries studied could be described as anywhere near the second destablization phase, and it is difficult to see how Russia could successfully demoralize any of them.

There has been much attention on social media manipulation, but when a Russian national was charged with involvement in a large-scale political influence operation against Europe, the U.S. and other countries, the U.S. Department of Justice stated that it had not affected the outcome of an election (2018). Likewise, an analysis of nine million tweets linked to a Russian troll factory indicated little effect (DFRL, 2018). Russia has a long history of coercion, but its effectiveness has been questioned (Sherr, 2013). Since 1990, Russia has repeatedly used the threat of energy interruptions as a political weapon. The net effect has been to make Europe acutely aware of the issue, to diversify supplies and take countermeasures (Collins, 2017). While the use of coercive methods is particularly prominent along the county's periphery, Russia is increasingly using intimidation against stronger entities like NATO, EU, and the U.S. This tendency to rely on coercive rather than cooperative means has often proved counter-productive, alienating allies, consolidating opposition and leading to diplomatic failures (Ziegler, 2018). It has been pointed out that the use of coercive means is a sign of weakness and not of power (Tkachenko, 2017), and Russia has also been described as a bully that fails because of its coercive strategies (Maness and Valeriano, 2015: p. 206). Holding the views of these authors together with the observations of the secret services studied, there is certainly reason to question the effectiveness of the Russian approach.

Conclusion

This study is based on an analysis of what Western secret services, mainly Northern European ones, have disclosed about Russian political influence activities in their annual public reports. According to these services, Russia is targeting the West through a divide and rule approach, and is using media, social media, minorities, refugees, extremists, human intelligence, cyber operations, energy, business, corruption, allies, front organizations, history, and military force for its political influence activities. Russia has specific objectives related to each country, but the overarching purpose is to weaken the EU and NATO and have sanctions removed. The study's main contribution is that it shows the wide specter of tools and techniques used by Russia, provide much detail on their use, and that it is complementing other research by a comprehensive analysis of the views of Western secret services in an area where much is covert.

Western countries are different, and have different relations with Russia, different history, different geography and different demography. These factors matter, and the relations with and perceptions of Russia certainly differ between, for example, the Netherlands and the Baltics. This study gives an overview of Russian influence activities in Europe, and specific issues and examples related to individual countries. There were no data available from Southern Europe and, therefore, the study does not warrant generalization about Russian influence activities in Europe as a whole, nor should we conclude that these reports cover all Russian tools. There are no common standards for the development of these annual reports, so it is challenging to compare the Russian approach to different countries. How these tools of influence are used probably depends on the context, what is available, what is deemed effective, and Russia´s prioritization of various countries. Russian influence activities are of a large-scale, and the threat should be taken seriously, but the reports studied also indicate that the effects of these activities are limited. There is widespread concern and broad consensus among these secret services that we can expect more interference and political influence activities (BfV, 2018: p. 278; DDIS, 2017: pp. 17, 20; DP, 2018: p. 6; EFIS, 2018: pp. 4, 44–46; NIS, 2018: pp. 19, 21, 30–33; SSD, 2018, pp. 57–59), and a risk that internal political and economic problems in Russia may cause more aggressive action abroad.

The tools and techniques identified in these intelligence reports complement other research (Tsygankov, 2018; Seely, 2018; Galeotti, 2017b; Van Herpen, 2015; Giles et al., 2015; Pomerantsev and Weiss, 2014: Sherr, 2013), but also add much detail and nuance to their use. There is a continuity from Soviet times, both in the wide specter of methods employed and in the scale and intensity of influence activities, and this was noted even before the conflict in Ukraine (Sherr, 2013). Technological development has added cyber and digital media to the toolbox, but both the purpose and the other techniques used for influence largely remain the same. One report, among many, at the end of the Cold War, concluded that there was 'a massive and highly organized effort by the Soviet Union and its proxies to influence world opinion", and disrupt and discredit the U.S. and its allies (U.S. State Department, 1986: p. iii). Furthermore, it is worth noting that the divide and rule approach has been used internally to balance the influence of competing factions within the Russian leadership (Reddaway, 2018) and to curb the opposition (Wilson, 2005). An Academic Outreach paper put it this way: 'The Kremlin's main adversary has always been, and still is, Russia itself. Virtually every type of action it has undertaken against the West was first implemented in Russia, against the Russian people, and against Russia's many ethnic, national and religious minorities" (Canadian Security Intelligence Service, 2018: p. 25).

This study opens for further research in several directions. In addition to the reports studied, there is much more material available from the secret services, through media search, websites, public statements, legal documents, political inquiries, and so on, and an analysis of such intelligence material would certainly complement other research. There is scope for more in-depth analysis of specific countries or regions, or alternatively of specific tools or techniques use by Russia, like support for extremists, use of front organizations, cyber and so on. Future studies could also

cover a longer time period, or one could conduct comparative studies on the Russian approach against different countries. Another very important, although difficult issue, is to get a better understanding of the effects of these Russian influence activities.

Russia is an authoritarian and corrupt state that regards the EU and, more specifically, NATO, as a challenge, a competitor and a threat. Its influence activities are malicious, undermining alliances and creating distrust, weakening what Moscow sees as their opponents and thus ensuring the survival of this authoritarian regime. Their interference is worrisome at several levels. First, Russia is undermining core democratic processes, like elections, and trust in the political system and its institutions. Second, their disinformation and manipulation of media and social media is directly undermining the political discourse, essential to democracy. Third, this is further exacerbated by their malicious attacks on individuals, like the Finnish journalist Jessika Aro, who has been tracked and harassed systematically after exposing Russian trolling of social media (Aro, 2015). However, the overall Russian approach is simple, divide and rule. These influence activities are almost always exploiting existing conflicts, fueling and enlarging them. If the Russian strategy is to divide our alliances and nations, sticking together would be to heed the advice of Sun Tzu: 'What is of supreme importance in war is to attack the enemy's strategy" (Gray, 2010: p. 70).

Data availability

Data sharing is not applicable as no datasets were generated or analyzed in this study.

Received: 5 July 2018 Accepted: 21 January 2019
Published online: 08 February 2019

Notes

1 Available at https://www.stratcomcoe.org/
2 Available at https://euvsdisinfo.eu/
3 Available at https://medium.com/dfrlab
4 See notes 2–4.

References

Andrew C, Gordievsky O (1990) KGB: The inside story of its foreign operations from Lenin to Gorbachev. HarperCollins, New York, NY
Andrew C, Mitrokhin V (1999) The Sword and the shield: The mitrokhin archive and the secret history of the KGB. Basic Books, New York, NY
Aro J (2015) My year as a Pro-Russian Troll Magnet. YLE Kioski, 30. Available at: http://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet
Ashley R (2018) Testimony before the Senate, 6 March. Available at: http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-.worldwide-threat-assessment/
Barkanov B (2018) Natural gas. In: Tsygankov AP (ed.) Routledge handbook of Russian foreign policy. Routledge, Abingdon, pp 138–152
Bajrovic R, Garcevic V, Kraemer R (2018) Hanging by a thread: Russia's strategy of destabilization in Montenegro. Foreign Policy Research Institute, Philadelphia
Bezmenov Y (1983) Lecture: The art of subversion. Available at: https://www.youtube.com/watch?v=T4YtgA2jnu4
Bittman L (1972) The deception game. Czechoslovak intelligence in Soviet political warfare. Syracuse University Research Corporation, New York, NY
Bittman L (1985) The KGB and soviet disinformation: An insider's view. Pergamon Brasseys, Washington
Blank S (2017) Cyber war and information war a la russe. In: Perkovich G, Levite AE (eds) Understanding cyber conflict. 14 analogies. Georgetown University Press, Washington, DC, pp. 81–98
Canadian Security Intelligence Service (CSIS) (2018) Who said what? The security challenges of modern disinformation. Academic outreach. CSIS, Ottawa
Collins English Dictionary (2018) Influence. Available at: https://www.collinsdictionary.com/dictionary/english/influence
Collins G (2017) Russia's Use of the "Energy Weapon" in Europe. Rice University's Baker Institute for Public Policy, Houston, Issue brief no. 07.18.17
Constitution Protection Bureau (CPB) (2017) Annual Public Report 2016. CPB, Riga
Danish Defence Intelligence Service (DDIS) (2016) The DDIS Intelligence Risk Assessment 2016. DDIS, Copenhagen
Danish Defence Intelligence Service (DDIS) (2017) The DDIS Intelligence Risk Assessment 2017. DDIS, Copenhagen
Defence Intelligence Agency (DIA) (2017) Russian military power 2017. DIA, Washington, DC
Digital Forensic Research Laboratory (DFRL) (2018) *#TrollTracker: Twitter Troll Farm Archives*. Available at: https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-d1b4df880ec6
Estonian Foreign Intelligence Service (EFIS) (2018) International Security and Estonia 2018. EFIS, Tallinn
Estonian Information Board (EIB) (2016) International Security and Estonia 2016. EIB, Tallinn
Estonian Information Board (EIB) (2017) International Security and Estonia 2017. EIB, Tallinn
Estonian Internal Security Service (EISS) (2015) Annual Review 2014. EISS, Tallinn
Estonian Internal Security Service (EISS) (2016) Annual Review 2015. EISS, Tallinn
Estonian Internal Security Service (EISS) (2017a) Annual Review 2016. EISS, Tallinn
Estonian Internal Security Service (EISS) (2017b) Areas of intelligence. Available at: https://www.kapo.ee/en/content/areas-intelligence.html
Estonian Internal Security Service (EISS) (2017c) influence activities. Available at: https://www.kapo.ee/en/content/influence-activities.html
Estonian Internal Security Service (EISS) (2018) Annual review 2017. EISS, Tallinn
European External Action Service (EEAS) (2018) EU vs Disinformation campaign. Disinformation Review. Available at: https://euvsdisinfo.eu/disinfo-review/
Federal Office for the Protection of the Constitution (BfV) (2015) Verfassungsschutzbericht 2014 (Annual report on the protection of the constitution 2014). BfV, Cologne
Federal Office for the Protection of the Constitution (BfV) (2016a) Verfassungsschutzbericht 2015 (Annual report on the protection of the constitution 2015). BfV, Cologne
Federal Office for the Protection of the Constitution (BfV) (2016b) Studierende, Wissenschaftlerinnen und Wissenschaftler im Visier Russischer Geheimdienste. Available at: https://www.verfassungsschutz.de/embed/faltblatt-2016-04-studierende-geheimdienst-russland.pdf
Federal Office for the Protection of the Constitution (BfV) (2017a) Verfassungsschutzbericht 2016 (Annual report on the protection of the constitution 2016). BfV: Cologne.
Federal Office for the Protection of the Constitution (BfV) (2017b) Arbeitsschwerpunkt der Spionageabwehr: Cyberangriffskampagne APT 28. Available at: https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/newsletter/newsletter-archive/bfv-newsletter-archiv/bfv-newsletter-2017-02-archiv/bfv-newsletter-2017-02-thema-04
Federal Office for the Protection of the Constitution (BfV) (2017c) Angriff auf unsere Souveränität – Gefahren aus dem Cyber-Raum. Available at: https://www.verfassungsschutz.de/de/aktuelles/meldungen/me-20170327-cebit-2017
Federal Office for the Protection of the Constitution (BfV) (2018) Verfassungsschutzbericht 2017 (Annual report on the protection of the constitution 2017). BfV, Cologne
Finnish Security Intelligence Service (Supo) (2017) Supo yearbook 2016. Supo, Helsinki
Finnish Security Intelligence Service (Supo) (2018) Supo yearbook 2017. Supo, Helsinki
Galeotti M (2016a) Heavy metal diplomacy: Russia's political use of its military in Europe since 2014. European Council on Foreign Relations Policy Brief, London
Galeotti M (2016b) Putin's hydra: Inside Russia's intelligence services. European Council on Foreign Relations Policy Brief, London
Galeotti M (2017a) Crimintern: How the Kremlin uses Russia's criminal networks in Europe. European Council on Foreign Relations Policy Brief, London
Galeotti M (2017b) Controlling Chaos: How Russia manages its political war in Europe. European Council on Foreign Relations Policy Brief, London
General Intelligence and Security Service (GISS) (2015) Annual report 2014. GISS, The Hague
General Intelligence and Security Service (GISS) (2016) Annual report 2015. GISS, The Hague
General Intelligence and Security Service (GISS) (2017) Annual report 2016. GISS, The Hague
General Intelligence and Security Service (GISS) (2018) Annual report 2017. GISS, The Hague
Giles K (2016) Russia's new tools for confronting the west. continuity and innovation in moscow's exercise of power. Chatham House, London
Giles K, Hanson P, Lyne R, Nixey J, Sherr J, Wood A (2015) The Russian Challenge. Chatham House, London
Gray CS (2010) The strategy bridge: Theory for practice. Oxford University Press, Oxford

Gvosdev NK, Marsh C (2014) Russian foreign policy. Interests, vectors and sectors. CQ Press, Thousand Oaks, CA
Herpen MV (2015) Putin's propaganda machine: Soft power and Russian foreign policy. Rowman and Littlefield Publishers, Lanham, MD
Jardines EA (2016) Open Source Intelligence. In: Lowenthal MM, Clark RM (eds) The 5 disciplines of intelligence collection. SAGE, Thousand Oaks, CA, pp. 5–44
Kalugin O (1994) The first directorate–My 32 years in intelligence and espionage against the west. St. Martin´s Press, New York, NY
Kanet RE (2017) The Russian challenge to the european security environment. Palgrave Macmillan, London
Karlsen GH (2016) Tools of Russian influence: Information and propaganda. In: Matlary JH, Heier T (eds) Ukraine and beyond: Russia's strategic security challenge to Europe. Palgrave MacMillan, London, pp. 181–208
Konyshev V, Sergunin A (2018) Military. In: Tsygankov AP (ed) Routledge handbook of Russian foreign policy. Routledge, Abingdon, pp. 168–181
Loftus S, Kanet RE (2017) Growing confrontation between Russia and the west. In: Kanet RE (ed.) The Russian challenge to the European security environment. Palgrave Macmillan, London, pp 13–36
Latvian Security Police (DP) (2015) Annual report for 2014. DP, Riga
Latvian Security Police (DP) (2016) Annual report for 2015. DP, Riga
Latvian Security Police (DP) (2017) Annual report for 2016. DP, Riga
Latvian Security Police (DP) (2018) Annual report for 2017. DP, Riga
Levchenko S (1989) On the wrong side. Dell Publishing, New York, NY
Lo B (2015) Russia and the new world disorder. Chatham House, London
Lunev S (1998) Through the eyes of the enemy: The autobiography of Stanislav Lunev. Regnery Publishing, Washington
Maness RC, Valeriano B (2015) Russia's coercive diplomacy: energy, cyber, and maritime policy as new sources of power. Palgrave Macmillan, Basingstoke
Norwegian Intelligence Service (NIS) (2017) Focus 2017. NIS, Oslo
Norwegian Intelligence Service (NIS) (2018) Focus 2018. NIS, Oslo
Norwegian Police Security Service (NPSS) (2014) Annual threat assessment 2014. NPSS, Oslo
Norwegian Police Security Service (NPSS) (2015) Annual threat assessment 2015. NPSS, Oslo
Norwegian Police Security Service (NPSS) (2016) Annual threat assessment 2016. NPSS, Oslo
Norwegian Police Security Service (NPSS) (2017) Annual threat assessment 2017. NPSS, Oslo
Norwegian Police Security Service (NPSS) (2018) Annual threat assessment 2018. NPSS, Oslo
Omand D (2010) Securing the state. Oxford University Press, London
Pacepa IM, Rychlak RJ (2013) Disinformation. WND Books, Washington, DC
Perkovich G, Levite AE (eds) (2017) Understanding cyber conflict. 14 Analogies. Georgetown University Press, Washington, DC
Pomerantsev P (2015) Nothing is true and everything is possible. adventures in modern Russia. Faber & Faber, London
Pomerantsev P, Weiss M (2014) The menace of unreality: How kremlin weaponizes information, culture and money. Institute of Modern Russia, New York, NY
Reddaway P (2018) Russia's domestic security wars: Putin's use of divide and rule against his hardline allies. Palgrave Pivot, London
Risso L (2014) Propaganda and intelligence in the cold war: The NATO information service. Routledge, Abingdon
Romerstein H (1989) Soviet active measures and propaganda. Mackenzie Institute, Toronto
Seely B (2018) A definition of contemporary russian conflict: how does the Kremlin wage war? Henry Jackson Society, London
Schoen DE (2016) Putin's master plan to destroy Europe, divide NATO, and restore Russian power and global influence. Encounter Books, New York
Schoen F, Lamb CJ (2012) Deception, disinformation, and strategic communications: How one interagency group made a major difference. National Defence University Press, Washington
Security Information Service (BIS) (2015) Annual report of the security information service for 2014. BIS, Prague
Security Information Service (BIS) (2016) Annual report of the security information service for 2015. BIS, Prague
Security Information Service (BIS) (2017) Annual report of the security information service for 2016. BIS, Prague
Sherr J (2013) Hard diplomacy and soft coercion: Russia's influence abroad. Chatham House, London
Shultz RH, Godson R (1984) Dezinformatsia: Active measures in soviet strategy. Pergamon Brassey's, Washington
Simons G (2018) Media and public diplomacy. In: Tsygankov AP (ed) Routledge handbook of Russian foreign policy. Routledge, Abingdon
Soldatov A, Rochlitz M (2018) The siloviki in Russian politics. In: Treisman D (ed.) The new autocracy: Information, politics, and policy in Putin's Russia. Brookings Institution Press, Washington DC, pp 83–108
State Security Department (SSD) (2015a) Annual review 2014. SSD, Vilnius
State Security Department (SSD) (2015b) Annual threat assessment 2014. SSD, Vilnius
State Security Department (SSD) (2016) National security threat assessment. SSD, Vilnius
State Security Department (SSD) (2017a) National security threat assessment. SSD, Vilnius
State Security Department (SSD) (2017b) Threats for the national security in Lithuania. Available at: https://www.vsd.lt/en/threats/threats-national-security-lithuania/
State Security Department (SSD) (2018) National threat assessment 2018. SSD, Vilnius
Strokan MA, Taylor BD (2018) Intelligence. In: Tsygankov AP (ed.) Routledge handbook of Russian foreign policy. Routledge, Abingdon, pp 153–167
Swedish Security Service (SAEPO) (2016) Säkerhetspolisens årsbok 2015 (Swedish Security Service 2015 Yearbook). SAEPO, Stockholm
Swedish Security Service (SAEPO) (2018) Säkerhetspolisens årsbok 2017 (Swedish Security Service 2016 Yearbook). SAEPO, Stockholm
Tkachenko S (2017) The coercive diplomacy of vladimir putin 2014–2016. In: Kanet RE (ed.) The Russian challenge to the European security environment. Palgrave Macmillan, London, pp 115–136
Tsygankov AP (ed) (2018) Routledge handbook of Russian foreign policy. Routledge, Abingdon
U.S. Department of Justice (2018a) U.S. charges Russian GRU officers with international hacking and related influence and disinformation operations, 4 October. Available at: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and
U.S. Department of State (1986) Active measures: A report on the substance and process of anti-U.S. disinformation and propaganda campaigns. Department of State, Washington, DC
U.S. Department of Justice (2018b) Russian national charged with interfering in U. S. political system. Available at: https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system
U.S. District court for the district of Columbia (2018) Netyksho et al. Indictment. Available at: https://www.scribd.com/document/383793138/Netyksho-Et-Al-Indictment#
U.S. District Court for the Eastern District of Virginia (2018) Affidavit in support of a criminal complaint. Available at: https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system
U.S. Information Agency (1988) Soviet active measures in the era of glasnost. A report to congress. USIA, Washington, DC
Vilmer J-B, Escorcia A, Guillaume M, Herrera J (2018) Information manipulation: A challenge for our democracies. Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris
Wilson A (2005) Virtual politics. Faking democracy in the post-soviet world. Yale University Press, New Haven
Winnerstig M (ed) (2014) Tools of destabilization. Russian soft power and non-military influence in the Baltic states. Swedish Defence Research Agency, Kista
Ziegler CE (2018) Diplomacy. In: Tsygankov AP (ed) Routledge handbook of Russian foreign policy. Routledge, Abingdon, pp. 123-137

Additional information

Competing interests: The authors declare no competing interests.