NATO PARLIAMENTARY ASSEMBLY

SCIENCE AND TECHNOLOGY COMMITTEE (STC)

RUSSIAN MEDDLING IN ELECTIONS AND REFERENDA IN THE ALLIANCE

General Report

by Susan DAVIS (United States)
General Rapporteur

181 STC 18 E fin | Original: English | 18 November 2018

TABLE OF CONTENTS

I. INTRODUCTION

1. Russia under President Vladimir Putin has become deeply dissatisfied with the liberal international order—so much so that the Russian state is actively seeking to undermine it. It is unclear what marked the turning point. Many point to President Putin's speech at the 2007 Munich Security Conference when he harshly criticized the United States, NATO and even the European Union (EU) and called for a new world order. Others point to Russia's military actions in Georgia in 2008 or in Ukraine since 2014. What is clear today is Russia's desire to return to geopolitical zero-sum games and reclaim what it considers its spheres of influence. To reshape the international order along those lines, Russia seeks to undermine its most stalwart defenders in Europe and North America. The Russian regime seeks to destabilize their democracies and, indeed, the very idea of liberal democracy in order to prop up its own position.

2. Russia's subversive efforts take many shapes and forms. While Russia has used force in support of this strategy, most efforts are non-military and seek to probe and exploit weaknesses in others through, *inter alia*, political and informational means, economic intimidation and manipulation (NATO PA, 2015). In 2018, the Committee on the Civil Dimension of Security (CDS) of the NATO Parliamentary Assembly (NATO PA) examines Russian overall hybrid operations in its special report *Countering Russia's Hybrid Threats: An Update* (NATO PA, 2018).

3. To complement the CDS report, the General Rapporteur of the Science and Technology Committee (STC) has decided to focus this general report on one of the most worrying hybrid threats: meddling in elections and referenda via cyber and information operations. The Russian way of cyber and information warfare is to attack and/or exploit the very institutions that make liberal democracies strong, particularly freedom of the press, freedom of speech, and free and fair elections. As is becoming abundantly clear, Russia has targeted several elections and referenda over the last few years. This conduct is unacceptable. Credible elections and referenda are at the heart of liberal democracy. Elections are the expression of the will of the people and therefore the basis of a government's authority. Referenda are a highly valued form of direct democracy in many polities, including the Rapporteur's home state of California. If citizens lose trust in either of these processes, their democracies are at severe risk.

4. The challenge of Russian cyber and information operations, including against elections and referenda, is a strategic challenge for the Alliance. It requires responses at every level, in all forums and through every channel. As elected representatives of the people, it is of utmost importance that the lawmakers of the Alliance address the challenge and that the NATO PA devise clear and strong recommendations for Allied governments and parliaments.

5. This general report, adopted in Halifax, Canada in November 2018, first addresses the different motivational drivers behind Russian meddling in elections and referenda in the Alliance. Second, it examines a few important elections and referenda in the Alliance where meddling took place or was a serious concern. Third, it discusses a range of policy responses, which served as the basis for a resolution, also adopted at the 2018 NATO PA Annual Session.

II. RUSSIA'S MOTIVATIONS BEHIND MEDDLING IN ELECTIONS AND REFERENDA

6. Despite the rhetoric of its leaders, Russia cannot compete toe-to-toe with NATO members. Its Gross Domestic Product (GDP) amounts to about USD 1.3 trillion compared to the United States' USD 19 trillion and the EU's USD 17 trillion. By 2020, Russia is projected to spend USD 41 billion on military spending compared to NATO's USD 892 billion—at a time when Russia is militarily overstretched due to its involvement in conflicts around the globe (Meakins, 2017). Moreover, its government remains beleaguered by severe corruption and an inability to address growing social problems, including severe poverty and inequality.

7. Perceiving itself as being at a dangerous disadvantage against potential adversaries, Russia's "weakened geopolitical position forces it to play the role of spoiler to assert its interests" (Beaulieu and Keil, 2018). Russian leaders have thus, *inter alia*, used cyberattacks and other instruments that the Soviet Union once called "active measures" or information operations to discredit liberal ideals and undermine democracies. Information operations are not a new addition to Russia's toolkit, but their reach and effectiveness have been increased by the vast and often unsecured cyberspace, which "allows for the high-speed spread of disinformation" (Fried and Polyakova, 2018).

8. While digital technology is undeniably a force multiplier, it is imperative to recall that information operations "are very human in design and implementation" (Watts, 2017). Those engaging in information operations try "to shape the target's preferences in line with the pre-defined aims of the sender" which involves "an active learning process on the part of the target" (Splidsboel Hansen, 2017). Information operations thus rely very much upon cutting-edge social, behavioral and cognitive sciences (Paul and Matthews, 2016).

9. The specific aims of Russia's meddling vary, depending on the circumstances, and they are not mutually exclusive. Indeed, analysts argue that the Russian leadership follows an "operationally opportunist approach" (Beaulieu and Keil, 2018). First, Russian meddling aims to **exacerbate pre-existing tensions within a society**. Wherever Russian meddling has been suspected, hackers and trolls have demonstrated a sophisticated understanding of the anxieties that divide a country. In the United States, Russian operatives purchased advertisements that inflamed religious and political grievances to undermine its civil society (Lecher, 2017). In Germany, Russian bot networks exploited debates over the government's refugee policies to try to weaken Chancellor Angela Merkel (Meister, 2016). Moreover, in Spain, Russian media and Russian bot networks fanned Catalonian separatism, contributing to one of Spain's biggest constitutional crises of the modern era (Emmott, 2017). These incidents show Russia's use of technology to weaken a sitting government, undermine the opposition or make liberal democracy appear undesirable (Alandete, 2017b).

10. Importantly, these divisions are not created out of thin air. Not every person who is involved in a divisive political debate is a Russian agent, nor is every bot network operated by Russian government operatives. Instead, Russian operatives insert themselves where they believe they can make an impact. Operatives exploit existing animosities by amplifying and elevating the most extreme voices to distort a country's public discourse. Media outlets like RT, which operates on a budget matching some of the biggest global media groups, provide conspiracy theorists and radical groups with the opportunity to spread their message. During the 2016 US elections, Russian agents masqueraded as US citizens on Facebook and Twitter to fuel highly partisan debates. Speaking about Russian bot activity, John Kelly, the founder of a social media marketing firm, noted that "[t]he Russians aren't just pumping up the right wing in America. They're also pumping up left-wing stuff — they're basically trying to pump up the fringe at the expense of the middle" (Rutenberg, 2017). As Mr Kelly told the US Senate: "The extremes are screaming while the majority whispers" (Kelly, 2018). In short, Russian meddling plays on existing fault lines in a society.

11. Second, Russian meddling seeks to **undermine faith in liberal democratic institutions**. Since the so-called color revolutions of the early 2000s, Russian leaders have, in the words of political sociologist Larry Diamond, "behaved as if obsessed with fear that the virus of mass democratic mobilization might spread to Russia itself" (Diamond, 2016). By weakening democratic institutions, Russian leaders see a way to weaken their perceived adversaries and level the playing field. Suggestions of corruption or official misconduct can force democratic governments to turn inward to deal with discontent and apathy within their own electorates. As early as the 2012 US presidential election, Russian media reported that US democracy was a "sham" and suggested, "that US election results [could not] be trusted and [did] not reflect popular will" (Office of the Director of National Intelligence, 2017). Following protests in Catalonia, observers argued that Russian bots circulated messages suggesting Spain was violent and undemocratic (Milosevich-Juaristi, 2017).

12. Moreover, delegitimizing democracy helps Russian leaders sell their system of government to citizens within Russia and abroad. As stated by the Minority Staff of the US Senate Committee on Foreign Relations: “If Putin can demonstrate to the Russian people that elections everywhere are tainted and fraudulent, that liberal democracy is a dysfunctional and dying form of government, then their own system of ‘sovereign democracy’ […] does not look so bad after all” (Minority Staff of the Committee on Foreign Relations, 2018). [Russian political leaders use the term “sovereign democracy” to describe the current political system in the country.] A weak West distracts from problems at home and provides a justification for holding onto power. Further, it makes Russia look more attractive to potential allies who could be alienated by the perceived failures and hypocrisies of the liberal democratic world order. If all politicians are corrupt and all elections are fraudulent, then there is no point in pursuing democracy at all (Zygar, 2016).

13. Third, Russian meddling tries to **advance politicians and political groups perceived as amenable or friendly to Russian influence and discredit those seen as hostile**. In Europe, Western intelligence agencies have, for example, reported Russian support for parties and organizations that undermine NATO and EU cohesion or advance Russian economic and political interests (Foster, 2016). In France, then-candidate Emmanuel Macron, noted for his opposition to many of Russia’s policies, suffered a major cyberattack that threatened to derail his candidacy. In contrast, his main rival, known for her pro-Russian views, was invited to the Kremlin and received extensive positive coverage by Russian media outlets.

14. A study by the Center for European Policy Analysis found that *Sputnik*, a Russian media outlet, granted “disproportionate coverage to protest, anti-establishment and pro-Russian members of the European Parliament” and did so in a deceptive fashion that “fit the [station’s] wider narrative of a corrupt, decadent and Russophobic West” (Nimmo, 2016). Movements that exacerbated internal tensions, threatened the cohesion of the EU and attacked NATO expansion tended to receive support from the Russian state. Movements that supported the opposite tended to be attacked or vilified.

15. Lastly, Russian meddling tries to **foment chaos and uncertainty in Western countries**. In July 2016, RT and *Sputnik* News published false stories about a US airbase in Incirlik, Turkey being overrun by extremists (Sputnik News, 2016). Observers reported intense activity by pro-Russian bot networks and social media aggregators that amplified the story and spread conspiracies about the imminent capture of nuclear missiles by terrorists (Fox, 2017). In January 2016, Russian-speaking communities in Germany were consumed by rumors that the government had covered up the rape of a girl by migrants. Russian media outlets and later also Russia’s Foreign Ministry spread the story, which insinuated that the official version of events was not to be trusted (Rutenberg, 2017).

16. Alina Polyakova of the Atlantic Council argues that the goal of such stories and of Russian meddling more broadly is to “manufacture some sort of political paralysis while at the same time raising the level of pro-Russian voices” to “destabilize politics and sow chaos” (Luhn, 2017). Individuals are induced to distrust their governments and mainstream media outlets in favor of conspiracies and rumors. The line between fact and fiction becomes blurred, making it easier for false or deceptive narratives to enter the public discourse (Fox, 2017). This confusion can be used to undermine the fabric of a society. It can also be used to support narratives within Russia about an impending global calamity that necessitates strong domestic leadership (Weisburd, Watts, and Berger, 2016).

17. In short, Russian misinformation and disinformation seek to accomplish multiple, interrelated goals to undermine the West and promote the interests of Russia’s leaders. They allow Russia to spread narratives that can influence, to its advantage, the way individuals, both at home and abroad, interact with political systems. Without resorting to direct military confrontation or substantial investments, Russian leaders thus seek to shape international affairs in their favor.

III. WHAT WE KNOW: RECENT RUSSIAN MEDDLING IN ALLIED COUNTRIES

18. Attribution in cyber space is notoriously difficult. This fact is especially true for information operations, which seek to create an environment of doubt, mistrust and confusion. Targets often prefer to conceal or downplay security breaches rather than face the embarrassment of public exposure. Social media platforms used to spread false or misleading narratives tend to be secretive with their data. The government agencies charged with investigating these incidents traditionally operate discreetly. Moreover, many of the components involved in information operations, including hacks, misreporting and bot networks, are just as available to private citizens as they are to state actors.

19. As such, it is difficult to discuss Russian interference without caveats. Although the Russian government is widely believed to have sponsored operations to discredit and destabilize liberal democracies, the extent and specifics of these operations remain unclear in many instances. In general, few government or parliamentary documents provide detailed, substantiated accounts of influence operations across the Alliance. Consequently, this section relies, in part, on public reporting and government statements to better understand allegations of Russian election and referendum interference in the United States, the United Kingdom, France, Germany, Spain and the Netherlands. These cases are illustrative because they involved a high number of credible reports alleging Russian cyber meddling and/or active steps initiated by governments and parliaments to prepare for any foreign meddling.

20. To keep this report concise, it focuses on cases of election and referendum meddling in Allied countries only. However, many of the patterns have been very similar in other countries, notably the former Yugoslav Republic of Macedonia[1], Georgia, Moldova, Montenegro (before it joined the Alliance), Sweden and Ukraine. Indeed, Russia first tested its cyber and information capabilities to influence domestic politics in NATO partner countries, especially in Georgia and Ukraine. Allies have already identified many lessons and best practices from their partners' experiences, as the Committee heard at the 2018 Spring Session. Going forward, the Alliance should continue to learn from partners, but also contribute to their resilience against such operations.

A. THE UNITED STATES

21. The US Presidential election of 2016 presents the most high-profile case of Russian meddling in elections. Four principal efforts were pursued: theft of information; selective dissemination of information; a propaganda campaign; and efforts to hack into voting systems across the country (Van de Velde, 2017).

22. Several key executive branch, Congressional and expert assessments have already been released publicly, but the investigations into Russian interference remain on-going. At the executive and Congressional levels, notable documents include:

- the January 2017 US Intelligence Community Assessment produced by the CIA, NSA, and FBI;
- the March 2018 House Permanent Select Committee on Intelligence Report adopted by the Majority Party;
- the March 2018 Minority Views on the House Permanent Select Committee on Intelligence Report; and
- the July 2018 Senate Select Committee on Intelligence's initial findings on the 2017 Intelligence Community Assessment.

23. What has become abundantly clear from all official and expert investigations is that Russia interfered with and sought to undermine public faith in the US democratic process. Although Russia

[1] Turkey recognises the Republic of Macedonia with its constitutional name.

and, previously, the Soviet Union have frequently attacked liberal democracies and sought to influence the outcomes of specific elections in the United States, Russia's actions in 2016 represented a significant escalation in activity, scope and directness.

24. Overt intrusions into public and private organizations as well as propaganda and disinformation enabled the Russian campaign. As reported in the January 2017 Intelligence Community Assessment, Russian intelligence officials targeted the personal and professional email accounts of officials associated with both parties (Office of the Director of National Intelligence, 2017). Clinton campaign chairman John Podesta had his email compromised after he mistakenly clicked on a spear-phishing email (Osnos, Remnick, and Yaffa, 2017). In his January 2017 testimony before the US Senate Select Committee on Intelligence, the then-director of the FBI, Mr James Comey, similarly claimed that Russian intelligence targeted and gained "limited access" to the Republican National Committee by compromising old email accounts and state-level Republican party organizations (Senate Select Intelligence Committee, 2017). However, according to the January 2017 Intelligence Community Assessment, Russia "did not conduct a comparable disclosure campaign" (Office of the Director of National Intelligence, 2017). Think tanks, lobbying groups, and other politically relevant individuals were also targeted as early as March 2016 (Office of the Director of National Intelligence, 2017).

25. Using this illicitly collected information, Russian officials launched a propaganda and misinformation campaign that relied on state-funded media, third-party intermediaries and paid trolls. Throughout the campaign, the fictitious DCLeaks and Guccifer 2.0, as well as WikiLeaks, contacted journalists and published emails, private phone numbers, campaign documents and other documents. Deputy Attorney General Rod Rosenstein made clear that DCLeaks and Guccifer 2.0 "were created and controlled by the Russian GRU [the Russian Main Intelligence Directorate]" (De La Garza 2018). These publications generated negative campaign coverage from established trendsetting news outlets, such as The New York Times (Watts and Rothschild, 2017).

26. Further, these events were extensively reported by Russian media outlets, including English-language outlets such as RT and *Sputnik*. RT, formerly known as Russia Today, is an international cable and satellite television network modelled after Western 24-hour news networks like CNN and the BBC. *Sputnik*, a government-run news commentary website and radio broadcast service, models itself after brash internet news sites like Buzzfeed. Both organizations are widely accused of serving as vehicles of Russian propaganda and amplifying extreme voices in their host countries (Rutenberg, 2017). Indeed, in 2017, the US Department of Justice required RT America to register under the Foreign Agent Registration Act. During the election, these sites used information disclosures to bolster their narrative about the failings of Western liberal democracy.

27. These activities were exacerbated by a coordinated campaign on social media platforms to highlight these disclosures, spread false stories and delegitimize the US government. On Facebook, officials have uncovered at least 120 fake Russian-backed accounts that spread messages seen by 29 million US citizens (Solon and Siddiqui, 2017). These pages include attempts to organize 129 offline, real-world events that were seen by 338,300 people in the United States (Volz and Ingram, 2018). It is unclear how many of these events were attended and how many people participated (Seetharaman, 2017). As of January 2018, Twitter had identified at least 50,258 Russian bot accounts that posted information related to the US election.

28. On both Facebook and Twitter, Russian accounts allegedly spread messages thought to be disruptive to US civil society or beneficial to Russian goals. This disruption effort included stealing identities and posing as fake US citizens, operating social media pages and other internet-based media targeted at a US audience and amplifying the views of real but divisive US citizens (Department of Justice, 2018). Messages sought to exploit and enrage both sides of controversial issues, including gun rights, immigration, LGBT rights and police use of force (Lecher, 2017). They also sought to directly influence the outcome of the 2016 US presidential election. This "firehose of falsehood," as RAND Corporation researchers describe it, produced high volumes of

misinformation over many different channels to demoralize and divide the public (Paul and Matthews, 2016).

29. In addition to these attacks, US officials claim that Russia targeted some voter databases during the 2016 election. On 22 September 2017, the US Department of Homeland Security informed 21 states that Russia had attempted to access state voter databases (Borchers, 2017). The Senate Intelligence Committee assessed that "[i]n a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter registration data; however, they did not appear to be in a position to manipulate individual votes or aggregate vote totals" (Burr et al., 2018). Though these databases can contain the usernames and passwords of election officials or the names, dates of birth, gender, driver's licenses, and partial Social Security numbers of voters, it is unclear what the hackers planned to do with this information.

30. The 2018 US midterm elections took place in the interval between the writing of this report and its discussion at the 2018 NATO PA Annual Session. These elections were widely expected to be a target for Russia and possibly other foreign governments attempting to influence US politics. Indeed, a few instances of meddling had already emerged at the time of writing. In July and August 2018, Facebook, Twitter, and Microsoft announced the removal of accounts. On 31 July 2018, Facebook removed 32 pages and accounts from Facebook and Instagram without attributing responsibility on who stood behind the attempt to influence the midterm elections (Roose, 2018). An additional 652 group pages and accounts were removed by Facebook and 284 accounts by Twitter on 22 August (Lapowsky, 2018). Both Russian and Iranian accounts were included in this group, which also highlights the broader threat of foreign meddling coming from countries beyond Russia (Solon, 2018). The Microsoft Corporation also deleted and seized accounts reportedly created by the GRU, which were targeting the Hudson Institute and the International Republican Institute – both prominent conservative think tanks. Over the past two years, Microsoft has furthermore shut down 84 fake websites over allegations of using phishing emails to gain access to networks (Dwoskin and Timberg, 2018). Spear-phishing attacks on US members of or candidates for Congress appear to have continued since the 2016 elections, which has prompted individual political campaigns to hire expensive cyber and information experts on staff.

31. In response to signs of continued attempts at interference, the US executive branch and Congress have taken active steps to secure the midterm elections. Since January 2017, over 60 bills related to election security have been introduced in the US Congress. In the 2018 omnibus spending bill, the US Congress included USD 380 million in funding for the Help America Vote Act (HAVA). Efforts to institute clear sanction mechanisms against election interference have also been advocated. Senators Marco Rubio and Chris Van Hollen have championed the bipartisan Defending Elections from Threats by Establishing Redlines Act (Deter Act) as one avenue to dissuade foreign interference in the midterms. In September 2018, President Donald Trump signed an executive order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election. In a joint statement, Senators Rubio and Van Hollen expressed their hope to go further on mandatory sanctions for those who might attack the US electoral systems (Van Hollen and Rubio, 2018).

B. THE UNITED KINGDOM

32. After reports of Russian interference in the US presidential election emerged, members of the British public expressed concerns about potential Russian meddling in the United Kingdom's 2016 EU membership referendum and its 2017 general elections. On 8 June 2017, the day of the United Kingdom's general election, the British Government Communications Headquarters (GCHQ) warned British energy companies that their systems might have been compromised by "advanced state-sponsored hostile threat actors." However, it is not known if this incident was related to the elections. Indeed, there were no known hackings or intrusions during the referendum and general elections campaigns (Williams-Grut, 2017). The government states that "to date, [it] has not seen evidence of successful interference in UK elections" (Roberts and Nokes, 2017).

33. Russia's influence in public discourse is unclear. While Prime Minister Theresa May accuses Russia of "planting fake stories" to "undermine free societies" and "sow discord in the West", attempts to study Russia's influence in the United Kingdom have revealed different estimates (BBC News, 2017). Oxford University, for example, found 105 Twitter accounts, tweeting 16,000 times, were linked to Russia. Overall, only 0.6% of tweets with the Brexit hashtag were linked to Russian news sources. Using a list of profile names provided to the US Congress, Edinburgh University found that 419 Russian Twitter accounts tweeted about both the US presidential election and the EU referendum (Booth et al., 2017). The Guardian newspaper found that these accounts were cited more than 80 times by the British press (Hern et al., 2017). A third study by City University of London found 13,500 bot accounts tweeting about the referendum. These bots operated as a "supervised network of zombie agents" and were deactivated or removed by Twitter shortly after polling closed. Bots "tweeted mainly messages supporting the Leave campaign", but researchers did not find evidence of widespread fake news and did not attempt to identify the owner of this network (City Press Office, 2017). Meanwhile, Swansea University and Berkeley University claim to have found 156,252 Russian accounts that mentioned Brexit in the days before the referendum (Reuters, 2017). The disparities in these estimates are the result of differing methodologies and Twitter's refusal to share much of its data with researchers.

34. These and other reports have triggered official investigations. In October 2017, the House of Commons Digital, Culture, Media and Sport Committee began a wide-ranging inquiry linked to Russia during the Brexit referendum and the 2017 general election. In November 2017, the Intelligence and Security Committee announced that it would investigate issues around Russian activity against the United Kingdom (Intelligence and Security Committee of Parliament, 2017). A separate investigation on digital campaigning by the Electoral Commission is also underway (Posner, 2017).

35. In July 2018, the Digital, Culture, Media and Sport Committee released an interim report on disinformation and fake news (UK House of Commons Digital, Culture, Media and Sport Committee, 2018). The Committee acknowledged the role that Russia has played in manipulating popular sentiment during referenda and national elections in Europe and the United States. The Committee offered suggestions on how to make tech companies more responsible for disinformation and fake news being spread on social media platforms. Additionally, the Committee called for a broader investigation into the scale of the problem in order to offer recommendations for actions.

36. Since June 2018, the actions of two prominent Brexit campaigners have drawn increasing scrutiny in the United Kingdom. Andy Wigmore, spokesman for the Leave.EU campaign, and Arron Banks, a major financial backer for Brexit, have faced criticism for their contacts with the Russian embassy in the run-up to the Brexit referendum, including an alleged exchange of confidential legal documents with officials at the Russian embassy and discussions about business deals (Cadwalladr and Jukes, 2018; UK House of Commons Digital, Culture, Media and Sport Committee). According to the Digital, Culture, Media and Sport Committee, the UK National Crime Agency is still investigating the matter at the time of writing.

C. FRANCE

37. During the 2017 French presidential election, then-candidate Emmanuel Macron and his party reported that they had suffered cyberattacks and false reports on social media. In February 2017, Mr Macron's digital campaign reported: "thousands of attempted attacks [against Mr Macron's] servers [from] tens of thousands of computers […] at the same time" (Beardsley, 2017). Macron campaign officials faced phishing attacks that exposed their networks to external actors (Hacquebord, 2017). On social media, Mr Macron was the subject of several fake stories (Chrisafis, 2018). The source of these attacks remains unclear.

38. Most prominently, Mr Macron was the target of a major coordinated leak designed to damage his candidacy. On 5 May 2017, 36 hours before the French run-off election, a 9-gigabyte file appeared on internet forums and open-source sharing sites (Greenberg, 2017a). The document purported to contain Macron campaign emails, documents, accounting files, contracts and other information meant to embarrass the campaign. According to the Macron campaign, the file also contained "numerous false documents intended to sow doubt and disinformation" (Greenberg, 2017a). The release appeared strategically designed to exploit French laws prohibiting campaign coverage less than 48 hours before the election. Despite a press ban on the publishing of the content, the leak quickly spread over social media (Dearden, 2017). As in the US presidential election, the file and related hashtags were amplified by bots, far-right activists and WikiLeaks (Volz, 2017).

39. Most French cybersecurity experts have declined to attribute this incident to Russia officially. After the election, the French government's chief of cybersecurity claimed that there was insufficient proof to attribute such an attack (Associated Press, 2017). Other French sources have commented on the amateurism of the attack compared to most state-sponsored cyberattacks. Indeed, the Macron team prevented several attacks by inundating the attackers with fake accounts to slow down and discredit the intrusion (Challenges, 2017).

40. However, experts outside France have suggested Russia as a likely perpetrator. Then US NSA Director Michael Rogers stated that the United States "had become aware of Russian activity" in the French election and that US officials told their French counterparts about this (Greenberg, 2017b). In April 2017, a private cybersecurity firm, Trend Micro, reported that the attack on Mr Macron bore characteristics similar to the attack against the US Democratic National Committee (Hacquebord, 2017).

41. Like other Allies, France has taken active steps to address cyber and information operations. One notable recent action was the July 2018 adoption of a law on the manipulation of information during the election period. The so-called fake-news law permits courts to rule whether articles published up to three months before an election are credible or should be taken down. It allows candidates to sue for the removal of fake news stories and forces social media platforms such as Facebook and Twitter to disclose the funding for sponsored content (Young, 2018).

D. GERMANY

42. Germany has faced several threats allegedly connected to Russia. In May 2015, Russian hackers sent phishing emails to members of the German government, including the office of the chancellor. The emails installed a Trojan virus on the computers of MPs and staff members who clicked on it. Over the next three weeks, the hackers scoured the German Parliament's network and collected 16 gigabytes of data (Beuth, Biermann, Klingst, and Stark, 2017). Notably, the hackers relied on human error, targeting the Parliament near a national holiday when the IT department was closed. In 2016, meanwhile, Russian media outlets circulated a false story about an alleged rape to delegitimize the German government (Meister, 2016). After protests by Russian-speaking Germans, the incident earned a rebuke by German officials, who accused Moscow of "political propaganda" (Witte, 2017). Between March and April 2017, a private cybersecurity firm also

identified unsuccessful attempts by Russia to infiltrate organizations aligned with Germany's two largest political parties (Barker, 2017). In March 2018, the German government confirmed reports that its government-run intranet, used to securely exchange information between different ministries and government offices, had been breached by a Russian hacking group. The attack appeared to focus on the Foreign Ministry and was being treated as "an ongoing process, an ongoing attack" (Oltermann, 2018).

43. In the 2017 German federal elections, however, Russian meddling appeared to be absent. While Russian media outlets promoted a high volume of stories that fostered negative views of Europe and Germany's leadership, stolen files from the German Parliament failed to surface. Researchers at the London School of Economics, meanwhile, reported a "coordinated Russian-language [bot] Twitter network", but their algorithms suggest that these networks were smaller than those deployed in other countries (Applebaum et al., 2017). Researchers with Oxford University found that 15% of Twitter traffic associated with "Alternative for Germany" – a party with pro-Russian views – had automated attributes, while major political parties averaged between 7.3 and 9.4% (Neudert et al., 2017). There is no public evidence to suggest Russia's involvement in this bot activity, nor do most observers think bot activity substantially influenced the election.

E. SPAIN

44. Spain claims that Russian meddling exacerbated tensions surrounding the 2017 Catalonia referendum (Emmott, 2017). In November 2017, Spanish ministers claimed that content related to Catalonia was sent from "Russian territory" and "other locations", such as Venezuela (Alandete, 2017a). These claims were supported by a researcher at the Elcano Royal Institute, a Spanish think tank. In a report on the Catalonian referendum, the researcher reported that trolls and bots disseminated true and false messages on Facebook and Twitter with the goal of provoking outrage toward the Spanish government. The messages characterized Spain as violent and undemocratic and reinforced images of Western instability (Milosevich-Juaristi, 2017).

45. Observers have supported some of these claims. In one study carried out by a researcher at George Washington University, the author found that stories by Russian outlets, such as RT and *Sputnik*, were circulated far more frequently than stories by other global outlets and ten times as frequently stories by as Spanish media counterparts (Alandete, 2017b). "Zombie accounts" spread pro-secessionist and anti-Spanish messages online (Alandete, 2017a). Meanwhile, *El Pais*, a major Spanish newspaper, found that tweets by Julian Assange and Edward Snowden in support of Catalonian secession were likely amplified by bot activity, with more than 60 retweets occurring every minute, and attributed this bot activity to Russia (Alandete, 2017c). The Atlantic Council's Digital Forensic Research Lab found evidence to support claims that Russian propaganda had influenced the debate around Catalonia. Notably, researchers found that Assange's tweets received "extra amplification'' from pro-Russian bots (Nimmo, 2017).

F. THE NETHERLANDS

46. Concerned by the meddling in the US Presidential elections in 2016, the Netherlands took active steps to prepare for potential Russian interference in the Dutch general elections in March 2017, including through active outreach to US officials by former NATO PA President and then-Minister of Foreign Affairs Bert Koenders (Brattberg and Maurer, 2018). However, Russian interference had already entered Dutch politics on two previous occasions. In October 2015, a group of Russian hackers involved in several other major hacks reportedly breached the Dutch Safety Board in the period leading up to and after the release of its report on the 2014 downing of flight MH17 over eastern Ukraine. In the run-up to the April 2016 referendum on the EU-Ukraine Association Agreement, Russian interference in the debate was seen as well, for example through agents passing themselves off as Ukrainians to influence local political debates.

47. To secure public trust in elections, the Netherlands had already banned the use of electronic voting in 2007 (Brattberg and Maurer, 2018). Before the March 2017 election, the government further strengthened election infrastructure by forbidding the electronic counting of ballots and the use of USB flash drives and email by election officials (Chan, 2017). Additionally, the government raised awareness of past Russian interference in foreign elections while also informing the Dutch public about disinformation and fake news. Furthermore, social media companies instituted a fact-checking function for Dutch newspaper articles (Brattberg and Maurer, 2018). Ultimately, the General Intelligence and Security Service concluded that Russia was not able to "substantially influence" the 2017 Dutch elections beyond the spreading of fake news. Independent experts argue that the fact the elections were carried out "without any noteworthy interference" could either be explained by "active preparations or an apparent lack of Russian effort at interference", possibly because the Russian government did not want to draw further ire in the Netherlands.

IV. POLICY RESPONSES AND THE WAY FORWARD

48. In almost all reported cases of suspected Russian meddling, a familiar pattern has emerged. First, political parties or government institutions report unauthorized intrusions into their networks. Emails are compromised. Personal data is stolen. These intrusions are then followed by significant, indiscriminate leaks, circulated on social media and magnified by bots, trolls and other accounts. Finally, these leaks are reported on by traditional, trendsetting press outlets that publicize the most sensational revelations. Meanwhile, outlets sympathetic to or controlled by the Russian government publish false or misleading stories that encourage polarized debates and conspiratorial thinking. The result is a bubble of confusion, wherein large amounts of leaked and false information give the impression of a scandal (Toucas, 2017).

49. As detailed in previous sections, there is little doubt that Russian leadership has exploited freedom of speech and of the press to delegitimize democratic institutions in NATO member states. Nor is there any doubt that Russia's involvement in such operations will continue in the immediate future.

50. The following sections detail a few policy responses to Russian meddling. These recommendations should not be understood as comprehensive or exhaustive as the situation is still developing and much of the surrounding analysis remains outside the public view. Rather, these sections reflect on promising practices by NATO members, approaches recommended by experts and other points commonly broached as part of the discussion on Russian interference (see for example: Fly, Rosenberger and Salvo, 2018 or Salvo and Beaulieu, 2018). Specific solutions will vary from state to state and from target to target. For clarity, policy responses are categorized into four sub-topics: policies that affect election infrastructure; policies that affect information systems; policies that affect social and mass media; and other possible measures.

A. ELECTION INFRASTRUCTURE

51. To date, there are no known cases of hackers altering vote totals in any election. However, there are indications of Russian interest in election infrastructure, such as voter registration systems, voting machines, tally servers and election-night reporting. Member states of the Alliance should therefore carefully analyses the potential threat. In the United States, for example, senior intelligence officials claimed to have "substantial evidence" that Russian-backed hackers gained access to, but did not alter, state websites and voter registration systems in seven states during the 2016 presidential election.

52. To discourage attacks on these systems, the US Department of Homeland Security designated election systems as "critical infrastructure" on 6 January 2017 in order to enhance communication between the federal government and election officials while unlocking additional funding for election security (Newman, 2017). Two bipartisan bills, the Secure Elections Act and the Protecting the

American Process for Election Results (PAPER) Act, have been proposed in the US Congress to enhance these efforts by eliminating paperless electronic voting machines, providing additional funding and assistance to election bodies, and mandating post-election security audits (Stewart, 2018). At the sub-national level, individual states have taken precautions such as the pre-election testing and certification of voting systems as well as requiring ballot reconciliations and audits (National Conference of State Legislatures, 2018).

53. Building on lessons learnt and best practices, your Rapporteur would, in particular, encourage fellow Committee members to explore taking the following steps through their national parliaments and governments:

- conduct regular risk assessments of election infrastructure and remedy any identified gaps or vulnerabilities;
- institutionalize pre-election preparations against election interference;
- mandate post-election security audits;
- provide adequate funding and assistance to election bodies; and
- designate election infrastructure as critical infrastructure.

B. INFORMATION SYSTEMS

54. More common are hacks that compromise the security of humiliating confidential information. As a researcher at the Center for Strategic and International Studies reports, “dumping authentic private information in the public domain is key for an attacker to gain credibility and build an audience they intend to manipulate” (Toucas, 2017). Authentic information serves as a hook for a larger misinformation campaign.

55. Governments can stop or deter some attacks by encouraging vulnerable organizations to adopt traditional cybersecurity measures. For example, most experts believe that organizations should have information technology departments with organization-wide visibility and access. They should be staffed with trained and professional employees who can purchase the necessary hardware and software without prohibitive delays. Meanwhile, all employees and managers should be aware of the threats that they face and how they might avoid unnecessary exposure through proper cyber hygiene. Workers should know to avoid clicking links or downloading content from unknown sources. They should know not to share passwords and personally identifiable information. Also, they should be aware that information posted on social media might be used against them. If individuals suspect a cyberattack, they should know who to contact.

56. Additionally, organizations should have clear and actionable protocols to expedite a response in the event of an intrusion and ought to know when it is appropriate to notify the relevant law enforcement or intelligence agencies. In the United States, for example, staffers at the Democratic National Committee were slow to engage the FBI about alleged Russian intrusions into their network (Lipton et al., 2016). In Germany, parliamentarians rejected cybersecurity assistance from the Federal Office for Information Security because they were concerned “the agency could seek to spy on them” (Beuth et al., 2017).

57. Independent of Russia’s activities, there is growing awareness of the need to develop robust cybersecurity capabilities. In 2016, the EU adopted the Network and Information Systems (NIS) directive, the first piece of EU-wide legislation on cybersecurity. The directive requires member states to develop incident response teams and a national authority competent in the area (Cybersecurity and Digital Privacy Unit, 2017). EU member states should promptly transpose the directive into national law if they have not done so already. In addition to various laws at the state level, the United States federal government passed the 2015 Cybersecurity Information Sharing Act to allow intelligence agencies to share information about cybersecurity threats with technology and manufacturing companies (Karp, 2016). At the same time, several NATO member states have

created military cyber commands to specifically counteract unwanted intrusions. France created such an organization in December 2017, following the presidential election, and similar institutions exist in the United States and Germany (Gramer, 2017). All NATO member states have developed a cybersecurity strategy in some form, though such strategies must be regularly updated to remain relevant (NATO Cooperative Cyber Defence Centre of Excellence, 2018).

58. Several national governments have also implemented laws and regulations that make organizations liable for breaches. The French National Commission on Informatics and Liberty (CNIL) is a cybersecurity regulatory body empowered to inspect corporate networks and enforce national data protection laws. In 2015, it conducted 550 inspections and fined at least one company EUR 50,000 for inadequate security measures (Raul et al., 2016). The United Kingdom, despite its anticipated exit from the EU, expects to implement the NIS Directive into its national law and, following public consultation in January 2018, confirmed that it would fine organizations up to GBP 17 million (EUR 20 million) for failing to cooperate with cybersecurity authorities, to report an incident or to implement appropriate security measures.

59. Internationally, there have been several sustained multilateral efforts to counter Russia's cyberattacks and information operations. In July 2014, the Alliance established the NATO Strategic Communications Centre of Excellence in Riga, Latvia, to research and identify information warfare.

60. The Cyber Defence Policy and an accompanying action plan, approved by all members at the NATO Wales Summit in September 2014, reaffirmed the Alliance's position that international law applied in cyber space and that Article 5 could be invoked in response to a cyberattack. The meeting also launched the NATO-Industry Cyber Partnership to strengthen NATO's relationship with the private sector and achieve specific cybersecurity objectives (Maldre, 2016). At the 2016 NATO Summit in Warsaw, cyber space was recognized as a domain of operations for NATO. Cybersecurity and defense played a significant role at the 2018 Brussels Summit as well. Among other actions, Allies agreed on a way to integrate sovereign cyber effects into Alliance operations and missions and decided to establish a Cyberspace Operations Centre in Belgium to provide situational awareness and coordinate NATO operational activity. Your Rapporteur welcomes these next steps in NATO's cyber defense policies. However, your Rapporteur argues that NATO must become quicker in analyzing cyber threats and better in responding in a coordinated, multidisciplinary way if it becomes necessary. Your Rapporteur also encourages further efforts, as parliamentarians in your respective member states, to ensure individual plans of action, lines of authority, and lines of coordination at the national, regional and local levels.

61. Enhanced coordination on cybersecurity and defense was identified as one of seven urgent needs for NATO-EU cooperation. The July 2018 Joint Declaration on EU-NATO Cooperation noted the intensifying work between the two organizations on hybrid threats, including cyberattacks. The fact that NATO and the EU are both participants in the Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland is a boon in this regard. If circumstances permit, the EU could also be invited to join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Moreover, the Digital and Social Media Playbook created by the NATO Science and Technology Organization provides a continually-updated assessment tool to help officials understand the goals and methods of cyber adversaries (NATO PA, 2017).

C. SOCIAL AND MASS MEDIA

62. While more robust cybersecurity measures can reduce risk, they cannot eliminate it entirely. Technical and human errors are certain to create vulnerabilities for even the most diligent organizations (Inglis, 2017). Furthermore, while access to private information can aid a disinformation campaign, it is not necessary to wage it. Misleading or fabricated stories can thrive even in the absence of hacks and leaks through social and mass media.

63. There are primarily two responses to misinformation on social media: one that emphasizes the **responsibilities of technology and media companies** and the other emphasizing the **responsibilities of governments**. Regarding the first approach, legislators and journalists have increased scrutiny of how media companies operate, especially in the wake of the Cambridge Analytica scandal. Following one briefing, US Senator Mark Warner described the efforts of one social media company as "show[ing] an enormous lack of understanding […] of how serious this issue is, the threat it poses to democratic institutions, and [begging] many more questions than they offered" (Fandos and Shane, 2017). British parliamentarians have similarly described corporate efforts to probe the issue as the "bare minimum" (Shaban, 2018). Third-party experts, meanwhile, have reported aggressive efforts by Facebook and Twitter to scrub data related to Russian interference from their platforms, preventing independent assessments (Timberg and Dwoskin, 2017). Even within the companies, business officials "acknowledge now that they missed what should have been obvious signs of people misusing the platform" (Thompson and Vogelstein, 2018).

64. In response to concerted public criticism, these companies have made some changes to address the misuse of their sites by malicious actors. In April 2017, Facebook published "Information Operations and Facebook" that outlined how a foreign adversary might exploit the platform to manipulate public opinion. In the same month, it suspended 30,000 fake accounts that had been created to influence the 2017 French presidential election (Weedon et al., 2017). In November 2017, Google announced it would "de-rank" RT and *Sputnik*—a process wherein a site is de-emphasized in search results—for their role in spreading disinformation (BBC News, 2017). Twitter identified and suspended 3,814 accounts linked to Russia's interference operation. These accounts, in total, had approximately 2.7 million followers. The platform also announced that it would counteract highly automated bot accounts through a number of detection tools based on public and non-public account data and activity characteristics (Edgett, 2018). Other websites and apps have received far less scrutiny. However, there is evidence of Russian disinformation campaigns on, for example, Reddit, a social media and news aggregation website, or Instagram, a photo-sharing mobile app (DiResta, 2018). This issue should be followed up vigorously. Companies should continue to harness the promise of emerging technologies by refining their approach to disinformation, using artificial intelligence and big data analytics in particular.

65. Other efforts have focused on fact-checking and informing users of false content. In November 2017, Facebook announced a new portal that allowed users to determine if they liked or followed any accounts linked to Russian propaganda (Yurieff, 2017). In January 2018, the company announced changes to its news feed algorithm and, in October 2017, it announced plans to hire more ad reviewers (Vogelstein, 2018). Prior to the 2017 German parliamentary elections, Facebook began labelling false stories and alerting users to hoaxes (Stelter, 2017). A similar but more vigorous effort took place before Italy's 2018 parliamentary elections, wherein Facebook partnered with fact-checking organizations to alert users who shared false information about the fact-checker's findings (Serhan, 2018). A number of independent fact-checking groups have also sprung up from civil society, including StopFake, the Atlantic Council's Digital Forensic Research Lab, the German Marshall Fund of the United States, Hamilton 68 or the Baltic "elves" (Fried and Polyakova, 2018).

66. Traditional media companies, meanwhile, have taken steps to educate the public on possible misinformation. In France, eight news organizations, including *Agence France-Press*, *L'Express* and *Le Monde*, joined forces with Facebook and Google to identify false stories circulating on social media (Barzic et al., 2017). *Le Monde*, meanwhile, established its own fact-checking site, *Les Décodeurs*, to help users determine the trustworthiness of a specific website (Albeanu, 2017). These new ventures build upon past and current fact-checking efforts, which have been a staple of Western newsrooms since the beginning of the 21st century. Per one estimate, there are at least 34 permanent fact-checking groups active across 20 different European countries (Graves and Cherubini, 2016). Meanwhile, journalists report that newsrooms are having conversations "about [their] paper's standards for using material of questionable sourcing" and the potential motives behind a source (Peters, 2017).

67. Some lawmakers have found these efforts are necessary but not sufficient. Efforts have also increased to regulate social media activity or make companies liable for illegal content in other ways. In the United States, a bipartisan group of lawmakers proposed legislation to ban foreign-paid social media political advertizing and make political advertizing on social media more transparent overall by putting it under the same regulatory regime as broadcast TV and radio (Kelly and Warner, 2017). Officials across NATO member states have also shown increasing interest in holding social media companies liable for failing to counteract illegal activity facilitated through their platform (Rozenshtein, 2017). The German Parliament approved a new law that requires social media platforms to take down "obviously illegal" material within 24 hours of being notified and makes them liable for up to EUR 50 million in fines if they fail to do so. French President Emmanuel Macron has expressed a strong interest in giving media regulators extra powers to "fight any destabilization attempt by any television channels controlled or influenced by foreign states" and regulating untruths on social media (BBC News, 2018). This led to the bill on information manipulation in pre-election periods (see above). The EU also runs Europol's Internet Referral Unit which, per a July 2016 report, assessed and referred for removal over 11,000 messages related to terrorist content. Ninety-one percent of this content was removed (Europol, 2016). Though the group puts its focus on extremist content, its activities could serve as a model for other efforts.

68. The second approach to misinformation puts the onus on governments by emphasizing their responsibility to keep the public informed. Russian meddling exacerbates existing fissures in society, but it does not create them. A misinformation campaign cannot take root if no domestic audience is willing to accept the divisive and conspiratorial messages that Russian actors amplify. Thus, this approach emphasizes the responsibility of democracies to establish sources of authority and ensure that debates across the political spectrum operate using the same set of shared facts.

69. Many of these efforts focus on government task forces that target disinformation. The EU, for example, operates the East Stratcom Task Force, a team of diplomats tasked with exposing Russia's online information through its website, EU vs Disinfo, and a network of over 400 experts, journalists, and think tanks. The European Commission also published a Communication on Fake News and Online Misinformation, for release in 2018, setting out the challenges and outlining key principles and objectives that should guide actions and specific measures the Commission seeks to take (European Commission, 2018). In support of its work on the document, an EU high-level group published a detailed report, formulating a number of recommendations for a multidimensional approach to online disinformation (High-Level Group on Fake News and Online Disinformation, 2018). The Czech Republic opened its Centre Against Terrorism and Hybrid Threats to counter disinformation, hoaxes, foreign propaganda, and extremist messaging within its borders (Colborne, 2017). In December 2016, the US Congress expanded the mission of the State Department's Global Engagement Center, originally envisaged to counter terrorist propaganda, to include countering state-sponsored propaganda and disinformation. However, despite lawmakers reallocating USD 120 million from the Department of Defense's budget, it appears the Center has yet to access or spend any money. In January 2018, the British government announced plans to create a new national security unit tasked with "combatting disinformation by state actors and others", but it remains unclear how this unit will operate and what its mandate will be (Walker, 2018). The German Interior Ministry similarly proposed the creation of a Center of Defense against Disinformation to identify misinformation and educate the public on its dangers (Deutsche Welle, 2016). In the run-up to the 2018 parliamentary elections, the Italian government had an online portal that allowed people to report false content online (Serhan, 2018). On a smaller scale, parliaments themselves can play a role in countering misinformation by holding hearings and releasing reports that reveal false narratives and the actors behind them.

70. As two experts from the Atlantic Council underline, "[w]inning the information war will require a whole-of-society approach" (Fried and Polyakova, 2018). Other efforts thus focus on civil society and the promotion of civic education and media literacy. In Italy, for example, the Ministry of Education unveiled a new curriculum with courses intended to teach Italian students how to identify false news stories and understand how social networks can be manipulated (Horowitz, 2017). In the

United States, several schools have adopted programs to help students understand how false narratives are created and how to identify them (Rosenwald, 2017). Since 2015, all French primary and secondary schools teach a course on moral and civic education. While primarily motivated by concerns over countering violent extremism, the course could serve as a useful forum to discuss misinformation campaigns. Similar programs exist in other Allied states. Though it is not yet clear how these programs will affect current public debates, several recent studies suggest that they help citizens better engage in the political process (Figueroa, 2017).

71. A related approach focuses on strengthening research on cyber and information operations and developing technological tools to deal with them. One EU high-level group, for example, proposes “a network of independent European Centres for (academic) research on disinformation” and urges the European Commission to consider an independent Centre of Excellence (High-Level Group on Fake News and Online Disinformation, 2018). A RAND Corporation scholar has also promoted the idea of a multidisciplinary Center for Cognitive Security (Waltzman, 2017).

D. OTHER APPROACHES

72. Russia uses information warfare because it appears to cause significant disruption at a low cost. As such, democracies could choose to discourage influence operations by imposing real consequences. For one, democracies should pursue actions through their court systems in cases of election interference, as the US Department of Justice has done in its February and July 2018 indictments of several Russian citizens and companies. Another potentially important instrument is sanctions. All NATO members instituted sanctions against the Russian Federation in the wake of the illegal annexation of Crimea in 2014. These sanctions must remain in place until conditions change. However, only one NATO member has implemented sanctions in response to election meddling. In the summer of 2017, the US Congress, in a near-unanimous, bipartisan vote, tasked the White House with imposing additional sanctions on Russia, in part because of its interference in the 2016 elections. In March 2018, after a substantial delay, the White House enacted part of these statutorily mandated sanctions. The US administration targeted five entities and 19 individuals, including the Internet Research Agency and individuals identified by the ongoing special counsel investigation as participants in Russia’s election meddling campaign. Your Rapporteur welcomes these first steps and acknowledges increased enactment of sanctions in recent months but notes that they fall short of the full range of sanctions authorized by Congress. Moreover, your Rapporteur would strongly argue that further sanctions should be discussed at the national and collective levels in response to additional evidence of Russian meddling in democratic processes.

73. Democracies can and should project national and multinational unity when faced with influence operations. Russian interference exploits and tries to exacerbate polarization within a society. Successful interference relies on political actors taking advantage of misinformation for short-term gain, for example by exploiting leaks for political gain. To prevent any future incidence, interference must thus be rebutted firmly and swiftly in a spirit of unity. Political leaders must be able to admit that Russian interference is demonstrably taking place when necessary. Political rivals must work together to condemn it with one voice via clear messages and actionable policies. By developing norms and procedures that discourage exploitation of misinformation, political systems can improve their resilience and deter future information warfare. The will of the people expressed through their votes in elections and referenda must be protected forcefully.

IV. CONCLUSIONS

74. In February 2018, US National Security Agency Director Dan Coats testified before lawmakers in the US Senate Intelligence Committee. As part of his assessment of the worldwide threats facing the United States and its allies, Mr Coats reported that: "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople and other means of influence to try to exacerbate social and political fissures in the United States […] There should be no doubt that Russia perceives its past efforts as successful and views the 2018 US midterms as a potential target for Russian influence operations" (Senate Select Intelligence Committee, 2018).

75. As Mr Coats' testimony indicates and this report shows, the problem of Russian election interference is not going away. If anything, recent events suggest that it will be a more significant part of Russia's toolkit than ever before. With a budget amounting to a few million US dollars, Russian forces can sow distrust and mayhem, build support for friendly politicians, and undermine enemies. While some steps have been taken to counter Russian meddling by means of cyber and information operations, Russia itself has faced few consequences for its interference. Many alleged targets of Russia's activities remain mired in internal debates that undermine any collective response.

76. To prevent further erosion of liberal democratic principles, NATO member states will need to take concerted efforts to strengthen their electoral processes. This need will become increasingly pressing, as evidence mounts that other countries, including China and Iran, have employed tactics similar to Russia's. Some of those efforts are detailed in previous sections, but member states will need to examine the pressures and circumstances affecting their country and develop a response accordingly. Russia adapts its operations to its targets and, thus, responses will need to be adapted as well. Your Rapporteur must underline, however, that individual and collective responses must be rooted in our common values, including individual liberty, human rights, democracy and the rule of law. These values can be exploited by an adversary, but they can also be our greatest asymmetric advantage. If we do not uphold these values, we undermine the democratic processes that we wish to safeguard and lose any advantage they provide.

77. As policymakers and agenda-setters, legislators play a particularly large role in this process. Consequently, lawmakers will need to foster dialog within their countries about how to rebut and respond to allegations of interference. They will need to work with their colleagues in other parties to ensure that credible allegations are believed by their constituents and civil society at large. They will need to ensure that allegations are investigated in a fair and impartial manner. While your Rapporteur recognizes the difficulty of these tasks, she hopes that this report can inform discussions and help member states recognize the threat posed by these operations. Indeed, your Rapporteur appreciates the input on the first draft of the report during the Spring Session from members of the Committee – and from associate members who have often suffered from Russia's cyber and information operations. In particular, your Rapporteur welcomed input on the lessons they and their governments have drawn from cases where their countries were subjected to information warfare – what worked well and what did not. The input was invaluable in preparing the concrete policy recommendations in this final report as well as in the proposed resolution for the NATO Secretary General and Allied governments and parliaments.

79. As the STC's work over the last few years clearly shows, threats in the cyber and information space are becoming absolutely critical. Before the terrorist attacks of 11 September 2001, the United States suffered from a failure of imagination. The Alliance – whether individually or collectively – must not suffer such a failure again. However, as Mr Coats has recently argued, "here we are nearly two decades later, and I'm here to say the warning lights are blinking red again" (Coats, 2018). The Committee and the NATO Parliamentary Assembly cannot relent and must continue to keep a sharp eye on cyber and information threats. Your Rapporteur stands ready to support this work in any way possible.

BIBLIOGRAPHY

Alandete, David, "How the Russian Meddling Machine Won the Online Battle of the Illegal Referendum", *El Pais*, 13 November 2017a,

Alandete, David, "Russian Meddling Machine Sets Sights on Catalonia", *El Pais*, 28 September 2017b

Alandete, David, "Russian Network Used Venezuelan Accounts to Deepen Catalan crisis", *El Pais*, 11 November 2017c

Albeanu, Catalina, "3 Fact-Checking Initiatives at Le Monde as the Newsroom Gears Up for the French Election", *Journalism.co.uk*, 28 March 2017

Applebaum, Anne; Pomerantsev, Peter; Smith, Melanie; and Colliver, Chloe, "'Make Germany Great Again': Kremlin, Alt-Right, and International Influences in the 2017 German Elections", *London School of Economics*, 2017

Associated Press, "The Latest: France Says No Trace of Russian Hacking Macron", *Associated Press*, 1 June 2017

Barker, Tyson, "Germany Strengthens Its Cyber Defense", *Foreign Affairs*, 26 May 2017

Barzic, Gwenaelle; Kar-Gupta, Sudip; Heavens, Andrew; and Lough, Richard, "Facebook, Google Join Drive Against Fake News in France", *Reuters*, 6 February 2017

BBC News, "Emmanuel Macron: French President Announces 'Fake News' Law", *BBC News*, 3 January 2018

BBC News, "Theresa May Accuses Vladimir Putin of Election Meddling", *BBC* News, 14 November 2017

Beardsley, Eleanor, "France Warns Russia to Stay Out Of Its Presidential Election", *National Public Radio*, 21 February 2017

Beaulieu, Britanny and Keil, Steven, *Russia as Spoiler: Projecting Division in Transatlantic Societies*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018

Beuth, Patrick; Biermann, Kai; Klingst, Martin; and Stark, Holger, "Merkel and the Fancy Bear", *Zeit Online*, 12 May 2017

Booth, Robert; Weaver, Matthew; Hern, Alex; and Walker, Shaun, "Russia Used Hundreds Of Fake Accounts to Tweet about Brexit, Data Shows", *The Guardian*, 14 November 2017

Borchers, Callum, "What We Know about the 21 States Targeted by Russian Hackers", *Washington Post*, 23 September 2017

Brattberg, Erik and Maurer, Tim, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, 2018

Burr, Warner et al., *Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security*, Senate Intelligence Committee, 2018

Cadwalladr, Carole and Jukes, Peter, "Leave.EU Faces New Questions over Contacts with Russia", *The Guardian*, 16 June 2018

Challenges, "Cyberattaques contre l'équipe Macron: le point sur la situation", 5 October 2017

Chan, Sewell, "Fearful of Hacking, Dutch Will Count Ballots by Hands", *The New York Times*, 1 February 2017

Chrisafis, Angelique, "Emmanuel Macron Promises Ban on Fake News During Elections", The Guardian, 3 January 2018

City Press Office, "13,500-Strong Twitter Bot Army Disappeared Shortly after EU Referendum, research reveals", *City, University of London*, 20 October 2017

Coats, Dan, *Transcript: Dan Coats Warns the Lights Are 'Blinking Red' On Russian Cyberattacks*, NPR, 18 July 2018

Cole, Harry "Dressing Down: Web Firms Facebook and Google 'Should Be Legally to Blame for Fake News', MPs Warn", 28 July 2018

Colborne, Michael, "The Brief Life, and Looming Death, of Europe's 'SWAT Team for Truth'", *Foreign Policy*, 20 September 2017

Corera, Gordon, "Russia 'Will Target US Mid-Term Elections' Says CIA Chief", *BBC News*, 29 January 2018

Cybersecurity and Digital Privacy Unit, The Directive on Security of Network and Information Systems (NIS Directive), European Commission, 19 September 2017

Dearden, Lizzie, "Emmanuel Macron Email Leaks 'Linked to Russian-Backed Hackers Who Attacked Democratic National Committee'", *The Independent*, 6 May 2017
De La Garza, Alejandro, "Here's What Deputy Attorney General Rod Rosenstein Said About Indicting Russian Intelligence Officers for Election Hacking", *Time*, 13 July 2018
Department of Justice, *United States of America v. Internet Research Agency…*, 16 February 2018
Deutsche Welle, "Germany Plans Creation of 'Center Of Defense' Against Fake News, Report Says", *Deutsche Welle*, 23 December 2016
Diamond, Larry, "Russia and the Threat to Liberal Democracy", *The Atlantic*, 9 December 2016
DiResta, Renee, *Statement for the Record from Renee DiResta*, US Senate Select Committee on Intelligence, 2018
Dwoskin, Elizabeth and Timberg, Craig, "Microsoft Says It Has Found a Russian Operation Targeting U.S. Political Institutions", *The Washington Post*, 21 August 2018
Edgett, Sean, *Sean Edgett's Answers to Questions for the Record*, Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, 19 January 2018
Emmott, Robin, "Spain Sees Russian Interference in Catalonia Separatist Vote", *Reuters*, 13 November 2017
European Commission, *Communication on Fake News and Online*, European Commission Communication, 2018
Europol, Europol Internet Referral Unit One Year On, *Europol*, 22 July 2016
Fandos, Nicholas and Shane, Scott, "Senator Berates Twitter Over 'Inadequate' Inquiry Into Russian Meddling", *New York Times*, 28 September 2017
Figueroa, Ariana, "Can Teaching Civics Save Democracy?", *National Public Radio*, 22 September 2017
Fly, Jamie, Rosenberger, Laura and Salvo, David, *Policy Blueprint for Countering Authoritarian in Democracies*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018
Foster, Peter, "Russia Accused of Clandestine Funding of European Parties as US Conducts Major Review of Vladimir Putin's Strategy", *The Telegraph*, 16 January 2016
Fox, Robert A., Statement Prepared for the U.S. Senate Select Committee on Intelligence hearing: Disinformation: A Primer In Russian Active Measures And Influence Campaigns', United States Senate Committee on Intelligence, 30 March 2017
Fried, Daniel and Polyakova, Alina, *Democratic Defense against Disinformation*, Atlantic Council, 2018
Gramer, Robbie, "Wary of Russian Cyber Threat, France Plans to Bolster its Army of 'Digital Soldiers'", *Foreign Policy*, 10 January 2017,
Graves, Lucas and Cherubini, Federica, *The Rise of Fact-Checking Sites in Europe*, Reuters Institute for the Study of Journalism, 2016
Greenberg, Andy, "Hackers Hit Macron With Huge Email Leak Ahead of French Election", *Wired*, 5 May 2017a
Greenberg, Andy, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'", *Wired*, 9 May 2017b
Hacquebord, Feike, *Two Years of Pawn Storm*, Trend Micro, 2017
Harris, Gardiner, "State Dept. Was Granted $120 Million to Fight Russian Meddling. It Has Spent $0.", *The New York Times*, 4 March 2018
Hern, Alex; Duncan, Pamela; and Bengtsson, Helena, "Russian 'Troll Army' Tweets Cited More than 80 Times in UK Media", *The Guardian*, 20 November 2017
High Level Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation*, Report of the High Level Group on Fake News and Online Disinformation, 2018
Horowitz, Jason, "In Italian Schools, Reading, Writing, and Recognizing Fake News", *New York Times*, 18 October 2017
Inglis, Chris, *Statement of Chris Inglis before the Senate Armed Services Committee*, US Senate, 27 April 2017
Intelligence and Security Committee of Parliament, *Press Release: 23 November 2017*, *Intelligence and Security Committee of Parliament*, 23 November 2017

Karp, Brad S., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, Harvard Law School Forum on Corporate Governance and Financial Regulation, 2016
Kelly, John W., *Briefing for the United States Senate Select Committee on Intelligence*, US Senate Select Committee on Intelligence, 1 August 2018
Kelly, Mary Louise and Warner, Mark, "What You Need To Know About The Honest Ads Act", *National Public Radio*, 19 October 2017
Lapowsky, Issie, "Iran Emerges as Latest Threat to Facebook and Twitter", *Wired*, 21 August 2018
Lecher, Colin, "Here Are the Russia-Linked Facebook Ads Released by Congress", *The Verge*, 1 November 2017
Lipton, Eric; Sanger, David E.; and Shane, Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", *New York Times*, 13 December 2016
Luhn, Alec, "From Russia, with Love", *Vice News*, 5 May 2017
Maldre, Patrik, *Moving Toward NATO Deterrence for the Cyber Deterrence for the Cyber Domain: Cyber Intelligence Brief No. 1*, Center for European Policy Analysis, May 2016
Maness, Ryan C. and Jaltner, Margarita, "There's More to Russia's Cyber Interference than the Mueller Probe Suggests", *The Washington Post*, 12 March 2018
McFadden, Cynthia; Arkin, William M.; Monahan, Kevin; and Dilanian, Ken, "U.S. Intel: Russia Compromised Seven States Prior to 2016 Election", *NBC News*, 28 February 2018
Meakins, Joss, "Why Russia is far less threatening than it seems", *Washington Post*, 8 March 2017
Meister, Stefan, "The 'Lisa Case': Germany as a Target Of Russian Disinformation", *NATO Review Magazine*, 2016
Milosevich-Juaristi, Mira, *The Combination': An Instrument in Russia's Information War in Catalonia*, Real Instituto Elcano, 20 November 2017
Minority Staff of the Committee on Foreign Relations of the United States Senate, *Putin's Asymmetric Assault on Democracy In Russia And Europe: Implications For U.S. National Security*, United States Senate, 2018
National Conference of State Legislatures, *Election Security: State Policies*, *National Conference of State Legislatures*, 13 February 2018
NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Security Strategy Documents*, NATO Cooperative Cyber Defence Centre of Excellence, 2018
NATO PA, "Countering Russia's Hybrid Threats: An Update [166 CDS 18 E fin]", report by Lord Jopling, November 2018
NATO PA, "Hybrid Warfare: NATO's New Strategic Challenge? [166 DSC 15 E BIS]", presented by Julio Miranda Calha (Portugal), 10 October 2015
NATO PA, "The Social Media Revolution: Political and Security Implications [158 CDSDG 17 E bis]", presented by Jane Cordy (Canada), 7 October 2017
Neudert, Lisa-Maria; Kollanyi, Bence; and Howard, Philip N., *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?*, Oxford University, 19 September 2017
Newman, Lily Hay, "Securing Elections Remain Surprisingly Controversial", Wired, 13 July 2017
Nimmo, Ben, *#ElectionWatch: Russia and Referendums in Catalonia?*, Atlantic Council, 2017
Nimmo, Ben, *Propaganda in a New Orbit: Information Warfare Initiative Paper No 2*, Center for European Policy Analysis, 2016
Office of the Director of National Intelligence, *Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution*, 2017
Oltermann, Philip, "German Government Intranet Under 'Ongoing Attack'", *The Guardian*, 1 March 2018
Osnos, Evan; Remnick, David; and Yaffa, Joshua, "Trump, Putin, and the New Cold War", *The New Yorker*, 6 March 2017
Paul, Christopher and Matthews, Miriam, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, RAND Corporation, 2016
Peters, Jonathan, *Putin, Politics, and the Press*, Columbia Journalism Review, 3 March 2017
Posner, Bob, *Responding to the Rise of Digital Campaigning*, *UK Electoral Commission blog*, 31 October 2017

Raul, Alan Charles; Smith, John; and Sulmeyer, Michael, *Touring the World of Cybersecurity Law*, RSA Conference 2016, 2016
Reuters, "Russian Twitter Accounts Promoted Brexit ahead of EU Referendum: Times Newspaper", 15 November 2017
Roberts, Liz Saville and Nokes, Caroline, Elections: Written question – 113484, Minister for the Cabinet Office, 2017
Roose, Kevin, "Facebook Grapples With a Maturing Adversary in Election Meddling", *TheNew York Times*, 1 August 2018
Rosenwald, Michael, *Making Media Literacy Great Again*, Columbia Journalism Review, 2017
Rozenshtein, Alan, *"It's the Beginning of the End of the Internet's Legal Immunity", Foreign Policy,* 13 November 2017
Rutenberg, Jim, "RT, Sputnik and Russia's New Theory of War", *New York Times*, 13 September 2017
Salvo, David and Beaulieu, Brittany, *NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018
Satter, Raphael; Donn, Jeff; and Day, Chad, "Inside Story: How Russians Hacked the Democrats' Emails", *U.S. News and World Report*, 4 November 2017
Seetharaman, Deepa, "Russian-Backed Facebook Accounts Staged Events Around Divisive Issues", *Wall Street Journal*, 30 October 2017
Senate Select Intelligence Committee, *"Global Threats and National Security"*, C-SPAN, 13 February 2018
Senate Select Intelligence Committee, "Russia's Role in Election-Year Hacking", *C-SPAN*, 10 January 2017
Serhan, Yasmeen, "Italy Scrambles to Fight Misinformation Ahead of Its Elections", *The Atlantic*, 24 February 2018
Shaban, Hamza, "Members of the U.K. Parliament Grill American Tech Giants over the Spread of Fake News", *Washington Post*, 8 February 2018
Solon, Olivia, "Facebook Removes 652 Fake Accounts and Pages Meant to Influence World Politics", *The* Guardian, 22 August 2018
Solon, Olivia and Siddiqui, Sabrina, "Russia-backed Facebook posts 'reached 126m Americans' during US election", *The Guardian*, 31 October 2017
Splidsboel Hansen, Flemming, *The Weaponization of Information: News from the Cognitive Domain*, DIIS, 14 December 2017
Sputnik News, "Thousands Yell 'Death to US' Near Turkey's Incirlik Base, Home to US Nukes", *Sputnik News*, 28 July 2016
Stelter, Brian, "Facebook to begin warning users of fake news before German election", CNN, 15 January 2017
Stewart, Emily, "Russian Election Interference is Far From Over. I Asked 9 Experts How to Stop It.", *Vox*, 19 February 2018,
Strobel, Warren and Walcott, John, "Top NSA official Says Telephone Surveillance Should Have Been Disclosed", *Reuters*, 22 March 2017
Thompson, Nicholas and Vogelstein, Fred, "Inside The Two Years That Shook Facebook—And The World", *Wired*, 12 February 2018
Timberg, Craig and Elizabeth Dwoskin, "Facebook Takes Down Data and Thousands Of Posts, Obscuring Reach OF Russian Disinformation", *Washington Post*, 12 October 2017
Toucas, Boris, *The Macron Leaks: The Defeat of Informational Warfare*, Center for Strategic & International Studies, 30 May 2017
UK House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report*, UK House of Commons Digital, Culture, Media and Sport Committee, 29 July 2018
Van de Velde, Jacqueline, *The Law of Cyber Interference in Elections*, SSRN, 2017
Van Hollen and Rubio, Van Hollen, Rubio Statement on Election Security Executive Order, 12 September 2018

Vogelstein, Fred, "Facebook Tweaks Newsfeed To Favor Content From Friends, Family", *Wired*, 11 January 2018
Volz, Dustin, "U.S. Far-Right Activists, WikiLeaks and Bots Help Amplify Macron Leaks: researchers", *Reuters*, 7 May 2017
Volz, Dustin and Ingram, David, "Facebook: Russian Agents Created 129 U.S. Election Events", *Reuters*, 25 January 2018
Walker, Peter, "New National Security Unit Set Up to Tackle Fake News in UK", *The Guardian*, 23 January 2018
Waltzman, Rand, *The Weaponization of Information: The Need for Cognitive Security,* RAND Corporation, 2017
Watts, Clint, *Cyber-Enabled Information Operations*, Statement Prepared for the US Senate Committee on Armed Services, 2017
Watts, Duncan J. and Rothschild, David M., *Don't Blame the Election on Fake News. Blame it on the Media*, Columbia Journalism Review, 2017
Weedon, Jen; Nuland, William; and Stamos, Alex, *Information Operations and Facebook*, Facebook, 2017
Weisburd, Andrew; Watts, Clint; and Berger, J.M., *Trolling for Trump: How Russia is Trying to Destroy our Democracy*, War on the Rocks, 6 November 2016
Williams-Grut, Oscar, "REPORT: Russia hacked UK energy companies on election day", *Business Insider*, 19 July 2017
Witte, Griff, "As Germans Prepare to Vote, a Mystery Grows: Where are the Russians?", *Washington Post*, 10 September 2017
Young, Zachary, "French Parliament Passes Law Against 'Fake News'," *Politico*, 4 July 2018
Yurieff, Kaya, "Facebook Will Show Users What Russian Propaganda They Liked or Followed", *CNN*, 22 November 2017
Zygar, Mikhail, "Why Putin Prefers Trump", *Politico*, 27 July 2016