NATO PARLIAMENTARY ASSEMBLY

COMMITTEE
ON THE CIVIL DIMENSION OF
SECURITY (CDS)

COUNTERING RUSSIA'S HYBRID THREATS: AN UPDATE

Special Report

by Lord JOPLING (United Kingdom)
Special Rapporteur

166 CDS 18 E fin | Original: English | 1st October 2018

TABLE OF CONTENTS

I. INTRODUCTION

1. Although it is not a new term, “hybrid warfare”[1] became a buzzword in the international political discourse following Russia’s invasion in Ukraine and its illegal annexation of Crimea in 2014. Hybrid warfare can be defined as “the use of asymmetrical tactics to probe for and exploit weaknesses via non-military means (such as political, informational, and economic intimidation and manipulation) [that] are backed by the threat of conventional and unconventional military means”[2]. In NATO’s context, “hybrid warfare” entails a campaign against an Ally or the Alliance by means that are not expected to trigger Article 5 of the Washington Treaty, which enshrines the principle of collective defence.

2. The current security environment in Europe and North America is filled with hybrid activity. This special report will focus specifically on the Kremlin’s use of hybrid tactics because Moscow’s hybrid toolbox is arguably the most sophisticated, resourceful, comprehensive and concerted. It also focuses on Russia because Russia’s 2014 military doctrine clearly identifies NATO as its primary threat. Russia’s hybrid warfare primarily targets the Euro-Atlantic community and the countries in the “grey zone” between NATO/EU and Russia.

3. Western experts agree that, while Russia is a declining power and greater challenges are likely looming over the horizon, in the short-term, Russia poses the most serious threat to the international order. In fact, Russia’s decline might be an incentive for the Russian president, Vladimir Putin, to use available means to revise the post-Cold War settlement sooner rather than later (Foreign Affairs, 2017). Hybrid methods can give significant advantages to the “weaker side” (Saarelainen, 2017). For example, they exploit the problem of attribution, wherein attacks can be difficult to trace back to the government of a specific country. These tactics are also aided by globalisation. Power dynamics are no longer based on just material means and increasingly focus on the ability to influence others’ beliefs, attitudes and expectations – an ability that has been boosted enormously by new technology and the interconnectedness of the Information Age (Smith, 2017).

4. Moscow’s use of hybrid techniques is neither random nor spontaneous. It is a manifestation of a well-thought out, well-funded and coordinated strategy. Recent findings of the US intelligence agencies, which link two very different types of hybrid methods – interference in the US elections and the use of Russian mercenaries in Syria – to the same pro-Kremlin oligarch, Mr Yevgeny Prigozhin[3], are a case in point.

5. The awareness of Russia’s disruptive activities in the West has grown considerably since the invasion in Georgia in 2008, and even more so since the illegal occupation and annexation of Crimea in 2014. In her speech in November 2017, the British Prime Minister, Theresa May, directly accused the Kremlin of trying to "undermine free societies" and "sow discord in the West" by mounting a sustained campaign of cyber espionage and disruption on governments and Parliaments across Europe. In a rare joint statement issued on 15 March 2018, leaders of the United Kingdom, France, Germany and the United States condemned the Salisbury chemical weapon attack as an assault on British sovereignty, “highly likely” committed by Russia. In August 2018, the United States introduced new sanctions on Russia over the Salisbury attack that would prevent Russia from obtaining sensitive electronic components and other dual-use technologies from the United States. Twenty-eight NATO Allies and partners expelled over 150 Russian officials from their territories, in

[1] The term “hybrid warfare” has been in use since at least 2005. It was subsequently used in reference to the strategy used by the Hezbollah in the 2006 Lebanon War.

[2] As defined in the 2015 NATO PA Defence and Security Committee General Report *Hybrid Warfare: NATO’s New Strategic Challenge?* [166 DSC 15 E bis].

[3] Mr Prigozhin, known as “Putin’s cook”, built his restaurant and catering empire largely owing to state contracts and his proximity to President Putin. The New York Times writes that – according to Mr Prigozhin’s critics, including opposition politicians, journalists and activists, as well as the United States Treasury and the special counsel to the US Department of Justice, Robert S. Mueller III – Mr Prigozhin is the Kremlin’s go-to oligarch for various covert missions.

a show of solidarity with the United Kingdom. NATO condemned the first use of a nerve agent on NATO territory, and reduced the maximum size of the Russian Mission to NATO by a third, thus sending a clear message to Russia that there are consequences for its unacceptable and dangerous pattern of behaviour.

6. This report aims at further improving awareness of Russia's hybrid activities, including political interference, low-level use of force, espionage, crime and corruption, disinformation and propaganda, cyberattacks, economic pressure and sanctions-busting, as well as showing how several techniques reinforce and complement each other. The report will examine the counter-measures adopted by the Euro-Atlantic community and offer thoughts on additional means of response to enhance resilience and defend our populations against these complex threats.

II. HYBRID TECHNIQUES IN THE KREMLIN'S PLAYBOOK

A. THE ORIGINS AND THE FRAMEWORK

7. Moscow's use of hybrid warfare dates back to the Soviet era when the concepts of "active measures"[4], "*maskirovka*"[5] and "reflexive control"[6] were developed. Hybrid methods were revived in Russia in the 2000s due to the renewed identification of the West as its strategic adversary, exemplified by Mr Putin's speech at the 2007 Munich Security Conference. Hybrid warfare was also adopted in response to the stark disparity between Russian and Western conventional military and technological capabilities and "soft power", and as a response to advances in information and communications technology, which have allowed for the emergence of new avenues for targeting the societies and political systems of potential adversaries.

8. Moscow's intention to use hybrid methods is articulated in several documents, the most recent being the 2014 Military Doctrine, the 2015 National Security Strategy and the 2015 Information Security Doctrine. These documents advocate the development of an effective means to influence public opinion abroad and, where necessary, a Russian resort to "non-traditional" methods. In his oft-cited article outlining the principles of hybrid warfare, Russia's chief of general staff, Valery Gerasimov, pointed out, *inter alia*, that "[t]he information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy" (NATO StratCom, 2015). In February 2017, the Russian defence minister, Sergei Shoigu, publicly announced the creation of information operations forces "for counter-propaganda purposes." Russia also streamlined the decision-making process in hybrid warfare by setting up the National Defence Management Centre (NTsUO) in 2014. This body coordinates the activities of military structures, but also of security and civilian agencies such as the Federal Security Service (FSB), the Federal Protective Service (FSO), the Foreign Intelligence Service (SVR), the Ministry of Interior and the State Atomic Energy Corporation, Rosatom. The NTsUO is seen to have "an incredibly expansive list of oversight, monitoring, and decision-making functions for state defence." According to Russia expert Roger McDermott, the NTsUO represents a step "toward conducting more integrated security operations in the future." The body is designed to give Russia the edge over NATO in taking decisions in a shorter time-frame. At the same time, other hybrid techniques in Russia's arsenal are intended to sow discord among and within NATO Allies in order to slow down NATO decision-making (Thornton, 2016).

[4] Subversive political influence operations, ranging from media manipulation to targeting political opponents.

[5] Camouflaging military activities for the purpose of denial and deception. An example is the concealment of offensive weapons transported to Cuba prior to the 1962 Cuban Crisis.

[6] Feeding an opponent selected information to prompt him to make knee-jerk decisions that are favourable to the Kremlin. Timothy L. Thomas, a prominent expert on Soviet "reflexive control", provided an example of how Soviet leaders paraded fake missiles and planted fake documents for Western intelligence to conclude that Soviet nuclear power was more formidable than it actually was.

9. Moscow justifies its use of hybrid methods by portraying itself as a victim of the West's "information aggression." Sergei Naryshkin, Russia's foreign intelligence service chief, accused the United States and its allies, particularly the United Kingdom, Poland, the Baltic States and Sweden, of waging a covert hybrid war against countries in the Commonwealth of Independent States (CIS). Mr Naryshkin further accused the West of trying to drive a wedge between CIS countries and of obstructing Eurasian integration. Mr Naryshkin also accused the West of interfering in the "democratic processes" of sovereign members of the CIS (Belsat, 2017).

10. As prominent Russia expert Mark Galeotti puts it, the Kremlin's focus on hybrid techniques "reflects the parsimonious opportunism of a weak but ruthless Russia trying to play a great power game without a great power's resources" (Calabresi, 2017). In the following chapters, this report will provide a brief overview of Russia's hybrid techniques.

B. POLITICAL INTERFERENCE

11. While Moscow has long been suspected of interfering in the politics of its so-called "near abroad", there is mounting evidence of its efforts to influence political developments in established Western democracies though a combination of cyberattacks, leaks of stolen data, the use of internet bots[7] and trolls[8], disinformation and support for fringe political parties[9]. According to Estonia's Foreign Intelligence Service, Russia is cultivating a network of "influence agents" – politicians, journalists, diplomats or business people who are pushing Russia's agenda in Western Europe. The Special Rapporteur wishes to list some of the facts and statements that, taken in their entirety, suggest a deliberate policy by Moscow to meddle in recent elections and referenda in the West. These interventions tend to back political parties, candidates or referendum proposals that oppose the established system (Galeotti, 2017). The Rapporteur wishes to stress that Russian meddling in no way implies that Moscow's interference was the decisive factor in the outcome of the concerned elections and referenda.

12. The most salient example of the Kremlin's interference was its attempt to influence the presidential election in the **United States** in 2016. In January 2017, the US intelligence community published a report stating that: "[Mr] Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton." The report also assessed "with high confidence that Russian military intelligence [released] US victim data obtained in cyber operations publicly and in exclusive to media outlets and relayed material to WikiLeaks." The report also notes that "these activities demonstrated a significant escalation in the directness, level of activity, and scope of effort compared to previous operations." Department of Homeland Security (DHS) officials admitted that the Russians targeted the voter registration rolls of 21 US states, managing to penetrate "an exceptionally small number of them." The DHS was able to determine that "the scanning and probing of voter registration databases was coming from the Russian government'' (McFadden, Arkin & Monahan, 2018).

13. Individuals associated with the Russian government stole and published thousands of emails of US politicians and bought Facebook ads, while Russia-backed bots and trolls posted false stories on social media and in the comments section of articles. During the presidential election, the Russians ran over 3,000 adverts on Facebook and Instagram to promote 120 Facebook pages in a campaign that reached 126 million US citizens (House of Commons, July 2018).

14. Senior Trump Administration officials, including the then-secretary of state, Rex Tillerson, and the US ambassador to the UN, Nikki Haley, branded Russia's alleged meddling in the presidential

[7] Software applications designed to generate messages (e.g. tweets) automatically.

[8] People who post controversial, provocative, inflammatory or off-topic messages online.

[9] The techniques used by the Kremlin to target Western electoral processes are explored in detail by the NATO PA Science and Technology Committee's 2018 report *Russian Meddling in Elections and Referenda in the Alliance* [181 STC 18 E fin].

election an act of "hybrid warfare" and accused Russia of trying to “sow chaos” in elections across the world.

15. The **UK** Parliament is investigating Russian interference in the Brexit vote. Damian Collins, chair of the parliamentary Digital, Culture, Media, and Sport Committee, noted that the first batch of data received from social media companies show that pro-Kremlin accounts were trying to “influence political debate in the UK and also to incite hatred and turn communities against each other”, while admitting that the evidence collected “could just be the tip of the iceberg” (Burgess, 2017). A report by British company 89up.org found that the Kremlin state media, RT and *Sputnik* pumped out at least 261 articles with a clear anti-EU bias, while pro-Kremlin trolls and bots ensured the broad dissemination of these articles in social media (Euronews, 2018). Another study by British experts found that more than 156,000 Russia-based Twitter accounts mentioned #Brexit in original posts or retweets – predominantly supporting “Leave” – in the days surrounding the vote. These posts were seen hundreds of millions of times (BBC, November 2017).

16. Similar incidents took place in the **French** presidential election, most notably with the eight-gigabyte leak of thousands of Macron campaign documents – several reported to be falsified or fabricated – shortly before the poll. While the French chief of cybersecurity states there is insufficient information to establish this attack came from Russia, the cybersecurity company Trend Micro stated the attack had patterns that were very similar to suspected Russian meddling in the United States (Willsher & Henley, 2017). The director of the US National Security Agency (NSA), Michael Rogers, similarly stated that his agency pinned at least some electoral interference in the French election on Moscow. The NSA warned French cybersecurity officials ahead of the presidential runoff that Russian hackers may have compromised certain elements of the election (Greenberg, 2017). A Russian bank has helped finance the campaign of far-right leader Marine Le Pen, though the party denies allegations of impropriety (Shekhovtsov, 2015).

17. Allegations of possible Russian interference have also reached **Spain** whose latest National Security Strategy includes the threat of misinformation campaigns. While Russia is not specifically mentioned in the document, Spanish officials have been open about Moscow’s interference in the Catalan independence referendum. The Spanish defence and foreign ministers stated that many of the profiles that spread fake news came from Russian territory. Reportedly, pro-Kremlin Twitter accounts, including bots, and Russian state media, such as Channel One, *Vesti*, and *Izvestia*, circulated fake or inflammatory anti-Spanish content. Notably, however, RT (formerly Russia Today) seems to have provided a more balanced coverage of the Catalan referendum, possibly because some in the Russian leadership might have thought that going too aggressively against Madrid could be counter-productive (Rettman, 2017).

18. The General Intelligence and Security Service (AIVD) of the **Netherlands**, also reported that, in the context of the Dutch parliamentary elections, “Russia [was] not afraid of using Cold War methods to obtain political influence.” In an annual report, the AIVD claimed that Russia tried to influence the election by spreading fake news, but that it failed in “substantially influencing” the election process.

19. Russia continues to nurture links with anti-establishment political parties in the West, particularly among far-right parties. Alternative for **Germany** (AfD), which came third in the 2017 German parliamentary elections with 12.6% of the vote, is remarkably popular among the country’s Russian-speaking population. According to the AfD’s own estimates, Russian speakers make up as much as a third of its voters. AfD leaders have travelled to Russia and met with officials from Mr Putin’s United Russia party and other representatives of the Kremlin. AfD’s electoral success is partly explained by rising anti-immigrant sentiments in German society. Pro-Kremlin trolls and bots are known to have bolstered these sentiments. In one notable case, Russian outlets disseminated the fake story of a Russian-German girl, Lisa, who was allegedly raped by migrants (Shuster, 2017).

20. **Greece** also accuses Moscow of bribery and meddling in its internal affairs. In July 2018, four Russian diplomats were banned from Greece after evidence revealed Moscow was trying to sabotage the naming deal between Athens and Skopje, which would pave the way towards an eventual NATO membership for the former Yugoslav Republic of Macedonia[10]. Reports have revealed that Russian agents – citizens and officials – have attempted to bribe senior Greek intelligence and military officers as well as to fund far-right groups. This situation mirrors Russia's apparent willingness to influence politics in the Western Balkans and to undermine EU and NATO aspirations in the region. Experts warn that the year 2018 marks the "launch of a renewed Russian campaign in the Balkans" (Galeotti, 2018).

21. One of the key findings of the **Lithuanian** state security department's 2018 annual report was that Russian intelligence and security services were particularly interested in the upcoming Lithuanian presidential elections in 2019.

22. Russia has a dedicated policy to reach out to and support Russian-speaking communities abroad, particularly in the countries of the former Soviet Union. Moscow estimates some 17 million such "**compatriots**" live in its neighbourhood. The three major instruments that support compatriots are the government agency *Rossotrudnichestvo*, which receives USD 95.5 million in funding from the state budget; the *Russkiy Mir* Foundation, which receives USD 15 million; and the Gorcharkov Foundation for Public Diplomacy, which receives USD 2 million (Kuhrt & Feklyunina, 2017). While the official goals of these organisations appear to be legitimate (e.g. promoting Russia's culture, language and worldview), the activities of these groups can have political consequences, by using Russian-speaking minorities to pressure their governments to abandon sanctions against Russia, for example.

23. Political interference and its actual impact are difficult to measure and prove. Whether it is funding from a Russian bank or cyberattacks by groups traced to Russian territory, it is often difficult to establish a clear and direct link between these actions and the Russian state.

24. In most cases, the Kremlin's interference does not create new societal cleavages or negative trends, it merely tries to reinforce them. The rise of anti-establishment political forces is an old trend. However, the pro-Russian attitudes of the Western far-right – examples of which are mentioned in paragraphs 16 and 19 of this report – are a recent phenomenon, which coincides with Moscow noticing these parties and providing support to them (Polyakova, 2016). Exaggerating the impact of Russian meddling could, in fact, be counterproductive as it could make the Kremlin more important than it really is. However, it should not be downplayed either and further steps to protect political systems in the free world are urgently needed.

C. KINETIC OPERATIONS

25. The term "hybrid warfare" does not refer solely to non-kinetic operations. Experts note that, as part of its hybrid tactics, Russia has employed "a full spectrum of activities, ranging from incitement of violence, kidnapping, and attempted assassination to infiltration and covert action combined with military efforts" (Kramer & Speranza, 2017). The most obvious example of a kinetic operation is the use of professional soldiers without military insignia, likely Russian Special Forces, in the occupation of Crimea and Donbas. These soldiers have since been referred to as "polite men" or "little green men." While the origin of these troops has never been doubted, the absence of insignia allowed President Putin, at least formally and temporarily, to distance the Russian state from these forces and mitigate international reaction. Evidence of Russian military presence in Donbas is abundant, but, due to the lack of formal attribution of these forces, Russia continues to present itself as a third party in the conflict.

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

26. The degree of plausible deniability varies by context. While the occupation of Crimea was a poorly disguised Russian Special Forces operation, local ownership of the “rebellion” in Donbas was more significant, allowing Mr Putin to downplay the involvement of the Russian state to a mere participation of Russian “volunteers” who took a “leave of absence” from serving in the Russian military. In Syria, Russia’s continuing military involvement after the formal withdrawal of Russian forces is even more shadowy. It has relied on a private paramilitary company, the Wagner Group, which was also active in Ukraine in early 2014 and is, according to media and US intelligence reports, associated with a Russian oligarch, Yevgeny Prigozhin. Since September 2015, the Wagner Group has played a major role in the Syrian government’s reconquest of its territory, operating as an undeclared branch of the Russian military alongside official Russian forces (Hauer, 2018). The clash between these trained Russian mercenaries and US forces in Syria resulted in the deaths of about 100 Russian mercenaries. Such a direct clash between Russian and US soldiers is unprecedented in recent history and could have resulted in a dangerous escalation. However, Mr Putin was able to deny any links between the Russian state and these mercenaries.

27. The presence of private Russian military contractors has also been reported in some African and Arab countries, including the Central African Republic (CAR)[11], Sudan or Libya. Companies like the Wagner Group allow Moscow “to enter a foreign (…) environment with minimal risk, and to exploit both political and economic opportunities there” while offering the Kremlin plausible deniability on its involvement (Hauer, 2018).

28. A particularly alarming development is Moscow’s apparent readiness to target its perceived enemies on foreign soil, including with weapons of mass destruction. The collateral damage of the chemical attack on Mr Skripal and his daughter in March 2018 in Salisbury caused the death of a civilian British woman and sent her husband to the hospital. The UK investigation identified two Russian citizens – who travelled to the United Kingdom under the names of Alexander Petrov and Ruslan Boshirov – as primary suspects and linked them to the Russian foreign military intelligence agency (GRU). Independent investigations, including by the prominent independent research organisation Bellingcat, have supported this conclusion. The Russians have claimed that these two individuals travelled to London from Moscow for a two- or three-day visit in order to see Salisbury cathedral. They conveniently neglected to refer to the identification of traces of the *Novichok* nerve agent in their London hotel bedroom. More recent investigations have identified one of the two suspects as a much-decorated GRU colonel, Anatoly Chepiga.

29. Other low-level uses of force by Russia include repeated incursions into NATO airspace[12], alleged involvement in the anti-NATO coup attempt in Montenegro in October 2016 and targeted actions such as the kidnapping of an Estonian officer in September 2014.

30. Russia also engages in regular large-scale exercises, such as *Zapad* and *Kavkaz*, designed to demonstrate Russia’s offensive abilities in eastern Europe for intimidation purposes and – in the cases of Georgia in 2008 and Ukraine in 2014 – to mask invasion. When conducting these exercises, Russia regularly evades its commitments under the Vienna Document to exchange information about its exercises and notify other member states. The scope of these exercises is usually substantially larger than officially declared by Moscow. *Zapad 2017*, for instance, reportedly involved 60,000 to 70,000 troops instead of the officially announced 12,700.

[11] Three independent Russian journalists were killed in the CAR while investigating the Wagner Group’s activities there.

[12] One of the most recent incursions occurred on 12 March 2018 over the Estonian island of Vaindloo. According to NATO’s military command, the behaviour of Russian aircraft during such incursions is unprofessional rather than hostile. However, this behaviour could lead to serious incidents, such as the shooting down of a Russian fighter jet over Turkish territory in 2017. The European Leadership Network’s study of 39 encounters between Russian and NATO air and naval forces concluded that these "highly disturbing" violations of national airspace had caused several incidents where an open conflict or the loss of life was narrowly avoided.

D. DISINFORMATION AND PROPAGANDA

31. This Committee's 2015 report *The Battle for the Hearts and Minds* [164 CDSDG 15 E bis] and 2017 report *The Social Media Revolution* [158 CDSDG 17 E bis] explored Russia's disinformation and propaganda machine in detail. These reports show that Russian mainstream media are not merely biased but have been "weaponised" and turned into the Kremlin's foreign policy tool. Margarita Simonyan – the chief editor of RT, which, along with *Sputnik*, is Moscow's flagship foreign language channel to influence international public opinion – claims RT is needed "for about the same reason as why the country needs a Defense Ministry" and that RT is capable of "conducting information war against the whole Western world," using "the information weapon" (EUvsDisinfo, January 2018).

32. Russian state-controlled media fail to meet minimal journalistic requirements: they are not independent and receive weekly instructions from the Kremlin (EUvsDisinfo, September 2017). More importantly, they lack scruples and ethical boundaries, blatantly falsifying evidence and reporting outright lies. Examples of this unethical "reporting" are extensively presented in the abovementioned NATO PA reports. The French president, Emmanuel Macron, has banished Russia's RT and *Sputnik* representatives from his media pool, arguing that they are not journalists but agents of influence.

33. In 2017, Russia's full-scale disinformation campaign continued. EU counter-propaganda experts, in their annual overview, mentioned examples of spectacular claims from pro-Kremlin mouthpieces, such as the imminent threat of civil war in Sweden, a US plane dropping a nuclear bomb over Lithuania, or a report that rape cases in Sweden had risen by a thousand percent (in fact a rise of 1,4% since 2015). Ukraine has remained a target of many of these stories, with Ukrainians often described as fascists and oppressors and Ukraine portrayed as an artificial country and a failed state (EUvsDisinfo, December 2017).

34. While exploiting the diverse and free Western media landscape, Russian state media promote a unified message and narrative. Unlike in Soviet times, this narrative has a less solid ideological base and appeals to a wide range of people with anti-Western, anti-liberal and anti-globalist views. Anti-Americanism is a key element of the narrative, designed to drive a wedge between the United States and Europe. This narrative embraces virtually all fringe ideas that contradict the mainstream Western worldview. An example of an initiative in this area is the new media venture "USA Really. Wake Up Americans" that was launched by the "Internet Research Agency", a Russian troll factory that was indicted for meddling in the 2016 US elections and, according to numerous media investigations, is linked to Yevgeny Prigozhin (EUvsDisinfo, April 2018). This venture, created to combat the "growing political censorship imposed by the United States", mainly targets anti-establishment audiences. Active on social media, it mostly spreads anti-US views and focuses on socially and politically divisive issues.

35. As noted, new breakthroughs in information and communications technology, including the growth of social media, has allowed Moscow to propel its disinformation and propaganda to a new level. Multiple reports show how pro-Russian trolls and bots spread fake news and socially divisive contents in Western societies. NATO's Strategic Communications Centre of Excellence reports that two-thirds of Twitter users who write in Russian about NATO presence in eastern Europe are bot accounts. Online channels are used in other ways, such as creating the illusion of a chemical leak through mass tweeting to generate panic in the US state of Louisiana or having the employees of Russian "troll factories" create false websites (Chen, 2015). Russia also imitates the official websites of Western institutions, for example replicating the website of the European Centre of Excellence for Countering Hybrid Threats, adding a pro-Russian twist. The Centre's website address, which is https://www.hybridcoe.fi/, has been imitated with the web address http://hybridcoe.ru/, giving it a professional and legitimate look, while adding anti-NATO and anti-EU content.

36. It must be noted that the Kremlin's disinformation machine could acquire even more efficient tools in the future. The development of artificial intelligence algorithms called Generative Adversarial Networks (GANs) offers the possibility of easily doctoring sound and video and thus create visual contents that could, for instance, convincingly depict a Western leader making a pro-Russian statement or a statement intended to prompt panic and confusion among Western audiences (The Economist, 2017).

E. CYBER AND ELECTRONIC WARFARE

37. Russia uses cyber weapons to carry out hybrid operations such as election meddling, espionage and disinformation campaigns. However, a cyberattack could also be a category of hybrid warfare in its own right. In 2017, multiple large-scale cyberattacks targeting critical infrastructure had serious real-world consequences. The WannaCry ransomware attack[13], attributed to North Korea, crippled health services in the United Kingdom and other Allied countries. The NotPetya ransomware attack, attributed to Russian hackers by the United Kingdom and other Allies, targeted the Ukrainian tax system but spread to businesses across the country and beyond. Corporate losses from this attack are estimated to be in the hundreds of millions of US dollars. In November 2017, the head of the British National Cyber Security Centre (NCSC), Ciaran Martin, warned that Russian hackers had targeted the British energy, telecommunications and media sectors. Russia is also accused of attacks on the German Parliament in 2015 and the German Foreign Ministry in 2017, as well as the crippling of a French TV broadcasting network (TV5Monde) in 2016. Earlier this year, the BSI – Germany's Federal Office for Information Security – accused the Russian government of carrying out a large-scale cyberattack on German energy providers. Ahead of the US midterm elections, Microsoft declared it had seized fake websites created by hackers linked to Russian military intelligence. These websites were replicating the websites of the Hudson Institute and the International Republican Institute but were in fact redirecting users to web pages created to steal passwords and other credentials (Sanger & Frenkel, 2018).

38. An interesting case demonstrating the link between Russian hackers, Russian "soft power" agents and the Russian state concerns the dispute around the potential separation of the Ukrainian Orthodox Church from the Moscow Patriarchate. Religious and state officials in Russia have been working hand in hand to prevent the split, as it would certainly diminish Russia's influence in Ukraine. As the split has been tentatively approved by the Ecumenical Patriarch Bartholomew I of Constantinople[14], it was revealed that Russian hackers had targeted senior Orthodox Christian figures including top aides to Patriarch Bartholomew I. Reportedly, the same Russian hacker group, Fancy Bear, was associated with the US Democratic National Committee email hacks in 2016 (Satter, 2018).

39. Russia is also suspected of carrying out electronic warfare (EW) attacks. The former commander of United States Army Europe, Lieutenant General Ben Hodges, notes that Russia has developed "a significant electronic warfare capability" over the past three years. On the eve of the *Zapad 2017* exercise, the mobile communications network in western Latvia was jammed, apparently by a Kaliningrad-based communications jammer aimed towards Sweden. A NATO official claimed the incident demonstrates Russia's ability to intercept or jam civilian networks "within a significant radius and with relative ease" (Gelzis & Emmott, 2017). Norway's public broadcaster announced that, during *Zapad 2017*, civilian aircraft operating in East Finnmark, Norway, reported a loss of their GPS signal. Measurements showed the disturbance came from the east. A report by the International Centre for Defence and Security found that further EW capability development by Russia would pose a serious challenge to NATO's eastern flank. Russia uses advanced surveillance techniques, such as drones and covert antennas, to pull data from smartphones used by NATO troops in the Baltic States and Poland (Grove, Barnes & Hinshaw, 2017).

[13] Ransomware attacks lock victims' computers and/or threaten to release captured data, demanding payment.

[14] Considered "first among equals" in the Orthodox Christian Church.

40. While the problem of attribution in cyberspace is acute, most cyberattacks of this scale have been traced to Russia—often to groups of hackers called Cosy Bear, also known as APT29, and Fancy Bear, also known as APT28[15]. The NCSC has accused Russia of using cyberattacks "to undermine the international system." According to a 2017 British House of Commons Intelligence and Security Committee report, the escalation of Russian cyber activities shows Russia is no longer concerned about remaining covert and is adopting a more brazen approach.

F. OTHER TYPES OF HYBRID THREATS

41. While most countries engage in some form of **espionage** and intelligence gathering, the activities of Russian spies seem disproportionate compared to the country's global weight. US intelligence experts warn that the conflict between the US intelligence community and Russian special services is intensifying in ways that could destabilise the bilateral relationship and the broader world order (Beebe, 2017). The US government claims that the number of Russian spies in the United States has considerably increased in the past 15 years (Schmidle, 2017). The United States also suspects that the Moscow-based Kaspersky Lab has used its popular antivirus software to spy on the United States and blunt US intelligence activities. Another example of Russian espionage in the United States is the case of Maria Butina, a Russian woman charged with "working to infiltrate the National Rifle Association (NRA) and influence US politics" (Swaine, 2018). The investigation has revealed her ties to Kremlin-backed banks and Russian oligarchs under US sanctions.

42. Meanwhile, the British secret intelligence service (MI6) has reclassified Russia as a "tier one" threat alongside Islamist terrorism. For comparison, Russia was not even mentioned in the British National Security Council's annual strategic defence and security review in 2010. British experts further assess that Russia employs between 705,000 and 940,000 people across its security agencies. In comparison, the British security agencies put together employ about 16,500 people. Officials also assess that Russian security and intelligence budgets have grown annually by 15-20%, with spending mainly going to operations (Edwards, 2017). Non-NATO neighbours like Sweden have also reported that espionage has increased since Russia's annexation of Crimea (Ringstrom, 2015).

43. Russia experts such as Mark Galeotti, who addressed this Committee at the 2017 NATO PA annual session in Bucharest, detect links between the Kremlin and Russian-origin **criminal groups** operating in Europe. They claim to have evidence that the Kremlin uses these groups as sources of "black cash", cyber attackers, traffickers of people and goods and even targeted assassinations by offering access to the networks of Russian intelligence. Local criminal groups have reportedly assisted Russia's invasion of Crimea and Donbas (Galeotti, 2017). In May 2018, a report by the British Parliament's foreign affairs Committee entitled "Moscow's Gold: Russian Corruption in the U.K." said that London is being used as a "base for the corrupt assets" of individuals linked to the Kremlin. The authors of the report asserted that these financial activities are "clearly linked to a wider Russian strategy" and are a threat to UK national security. The report called for a "coherent and pro-active strategy on Russia, (…) that clearly links together the diplomatic, military and financial tools that the U.K. can use to counter Russian state aggression." The proposed concrete measures include establishing a register of ownership for foreign companies that wish to own property in the United Kingdom, thereby exposing those who "purchase UK property through offshore shell companies, disguising their identities and the potentially corrupt sources of their funding" (House of Commons, 2018a).

44. Russia has a long history of using its **energy** resources as a foreign policy tool[16]. It is important to stress that Europe's energy vulnerability has diminished considerably. This is due to the following factors: 1) diversification of supply through additional infrastructure, such as new Liquefied Natural Gas (LNG) terminals in Poland and Lithuania; 2) the development of shale oil and gas reserves in the United States; 3) the EU's steps towards an integrated energy market through the Third Energy

[15] The cybersecurity firm CrowdStrike associated Cosy Bear with the FSB and Fancy Bear with the GRU.

[16] This issue is discussed in detail by the Assembly's Economics and Security Committee's 2018 report *The Energy Security Challenge in Central and Eastern Europe* [070 ESC 18 E].

Package, which forces Gazprom to sell its stakes in European transmission networks; and 4) the “green revolution” in energy, especially the advances in renewable energy and energy efficiency (Russia’s 2017 Economic Security Strategy identified the development of green technology as a threat to its economic security).

45. Nevertheless, Russia retains significant leverage over Europe’s energy market. Russia’s gas supplies to Europe are growing and almost 40% of Europe’s gas imports come from Russia. The EU is currently discussing the controversial Nord Stream 2 project, a new pipeline connecting Germany and Russia while bypassing countries like Ukraine and Poland. Opponents of the pipeline argue that the project undermines the energy solidarity envisioned by the European Energy Union initiative. The Baltic States have taken important steps to reduce energy dependence on Russia, but their electricity markets remain synchronised with the Moscow-controlled electricity network BRELL. The Baltic states are concerned that Moscow will try to sabotage their desynchronisation plans. Lithuania is also highly concerned by the Russian company *Rosatom*’s non-transparent construction of a nuclear power plant in Belarus, 50 kilometres from the Lithuanian capital, Vilnius. Europe’s energy sector, as a whole, needs to improve its cybersecurity resilience from hostile foreign actors (Grigas, 2017).

46. A recent report by the Asan Institute for Policy Studies provides information indicating that Russia has been engaging in **sanctions-busting** as a foreign policy tool. More specifically, circumventing the UN sanctions on North Korea, Russia is believed to have supplied 622,878 tons of undeclared refined oil to this country between 2015 and 2017, which represents around one third of North Korea’s total refined oil imports during the same period (Asan, 2018).

47. Some experts, including British Chief of the Defence Staff Air Chief Marshal Sir Stuart Peach, British MP Rishi Sunak and former NATO Supreme Allied Commander Admiral James Stavridis, warn that the Russian navy could potentially pose a threat to the **undersea cables** that carry 97% of global communications and USD 10 trillion of financial transfers every day. There are no alternatives to these cables. Modern economies and societies depend crucially on this undersea infrastructure, which lacks basic defences (Murphy, Hoffman & Schaub, 2016). Russian submarine activity in the northern Atlantic has increased significantly in recent years, and these submarines have been “aggressively operating” near undersea cables. Russia is significantly expanding its naval capacity, including Yantar class intelligence ships and auxiliary submarines, both of which are specifically able to disrupt undersea cable infrastructure. Sir Stuart Peach claims the United Kingdom and its NATO Allies are ill-prepared to deal with the prospect of such an attack (BBC, December 2017). In June 2018, the United States imposed sanctions on the Russian government’s underwater capabilities, which reportedly helped the Kremlin tap undersea communications cables used by Western countries.

48. Generally speaking, Russia’s hybrid activities pose a threat to the **maritime** environment. Ports and commercial and military vessels are easy targets for sabotage, navigational spoofing and cyberattacks (Kremidas-Courtney, 2018). Considering the vessels’ high reliance on cyber-enabling capabilities, cyberattacks can cause important damage.

III. RESPONDING TO HYBRID THREATS

A. NATO

49. As noted, hybrid attacks present a challenge to the Alliance as they are generally not expected to trigger Article 5 of the Washington Treaty. In the hybrid era, the emphasis falls on Articles 3, which outlines collaboration and mutual assistance short of collective defence, and 4, which obligates consultations when the security of an Ally is threatened. At its summit in Warsaw in 2016, NATO adopted a strategy on the Alliance’s role in countering hybrid warfare. It was reaffirmed that the primary responsibility to respond to hybrid threats rests with the targeted nation. NATO, however, is

prepared to assist an Ally at any stage of a hybrid campaign. The Allied leaders also announced that Allies would be prepared to counter hybrid warfare as part of collective defence and that the North Atlantic Council could decide[17] to invoke Article 5 of the Washington Treaty. Collective action depends on a unified assessment of the threat, a determination that Russia's hybrid tactics aim to prevent.

50. In the wake of Russia's aggression in Ukraine, NATO drafted a Readiness Action Plan (RAP) that tripled the size of the NATO Response Force (NRF) and introduced a Very High Readiness Joint Task Force (VJTF) capable of being deployed within days as a deterrent force. To ensure the efficiency of the VJTF, NATO set up the NATO Force Integration Units (NFIU) in eastern and central Europe. One notable step by NATO was the deployment of four battalions in the Baltic states and Poland, which considerably escalated the cost of potential aggression against these Allies[18].

51. To be fully effective, these military responses must be complemented by efforts to achieve national resilience in areas such as continuity of government, critical government services and cyber networks, energy, food and water supplies and the ability to deal effectively with uncontrolled movement of people. In 2017, NATO produced an Alliance-wide assessment of national resilience which generated an overview of the state of civil preparedness. This identified areas where further efforts are required to enhance resilience.

52. NATO has also improved intelligence cooperation among Allies by establishing a new Joint Intelligence and Security Division (JISD). To reflect the growing need to take a holistic approach, a new branch for hybrid analysis was created within the JISD with a mandate to analyse the full spectrum of hybrid actions by drawing from military and civilian, classified and open sources. Many aspects of hybrid warfare – such as countering disinformation, cyber threats and energy security – are also covered by NATO's Public Diplomacy Division and Emerging Security Challenges Division. NATO has also launched a platform of cooperation with Ukraine specifically dedicated to bringing together experts on hybrid threats.

53. Several NATO-certified or NATO-supported centres of excellence – including the Strategic Communications Centre in Riga, the Cyber Defence Centre in Tallinn, the Energy Security Centre in Vilnius and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)[19] – provide the threat analysis and draft policy recommendations.

54. Since the massive 2007 cyberattack against Estonia by Russian hackers, NATO has made great strides in developing its cyber defence capabilities. The 2016 Warsaw Summit identified cyberspace as the fifth "domain of operations in which NATO must defend itself." In February 2017, NATO Allies endorsed an action plan that put cyber defence at the core of NATO's collective defence and promoted NATO's cooperation with the industry. Every year for 10 years, NATO has organised a cyber exercise week that involves NATO member states and allies reacting to simulations of cyberattacks that mirror real threats. Through the Cyber Defence Pledge, NATO members have committed to prioritising enhancements to the defences of their national networks – which is of critical importance, given the fact that the Alliance's cyber security is inhibited by the capabilities of its weakest member. NATO has shored up the defence of its own networks[20].

[17] All NATO decisions are made by consensus, after discussion and consultation among member countries.

[18] For more details on NATO's Enhanced Forward Presence (EFP), see this year's general report of the NATO PA Defence and Security Committee entitled *Reinforcing NATO's Deterrence in the East* [168 DSC 18 E].

[19] Hybrid CoE is a joint project of NATO, the EU and several NATO/EU member states, inaugurated in October 2017.

[20] In 2016, NATO had to ward off about 500 cyberattacks each month.

55. NATO is also increasingly cooperating with the EU on cyber defence: the two organisations have increased information exchange and participated in joint exercises. They have also agreed to cooperate in incident response and crisis management.

B. EUROPEAN UNION

56. With its considerable resources and soft power, the EU is a key player in building Europe's resilience to hybrid threats, particularly disinformation and cyberattacks. The 2016 EU-NATO Joint Declaration lists more than 40 specific areas of cooperation and as many as ten of those relate to strengthening cooperation on hybrid threats. However, EU-NATO cooperation is limited to the international staff of the two organisations and does not involve member states.

57. In April 2016, the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy adopted a Joint Communication on countering hybrid threats. The framework defines the EU's assistance to member states in building their resilience against hybrid threats while recognising that the primary responsibility for countering these threats lies with member states. To improve situational awareness through sharing of intelligence analysis, the EU has established the Hybrid Fusion Cell.

58. As a response to Russia's disinformation campaigns, the EU created the East StratCom Task Force, also referred to as EU "myth-busters". The team of a dozen nationally-seconded diplomats exposes Russia's online disinformation daily. After repeated calls from the European Parliament, the taskforce has finally been granted a separate budget of just over 1 million euros a year. The Rapporteur is convinced that the amount remains inadequate, given the scope of the challenge and the EU's vast financial capabilities.

59. While the EU's recently established Permanent Structured Cooperation on Defence (PESCO) focuses mainly on hard security investments, one of the 17 collaborative defence projects—led by Lithuania and involving nine EU members – led to the establishment of rotational EU Cyber Rapid Response Teams. In December 2017, the EU established a permanent Computer Emergency Response Team (CERT-EU) covering all EU institutions, bodies and agencies. The EU allocated EUR 50 million to develop a cybersecurity competence network connecting private and public entities – including research centres, university programmes, and industry partners – to best tackle the EU's cybersecurity challenges and strengthen individual member state capacities.

C. NATIONAL LEVEL

60. Many NATO and EU member states and aspirant countries have revisited their national security policies in response to Russia's hybrid activities. While it is impossible to provide a comprehensive overview of these efforts within the limits of this report, the Rapporteur would like to highlight several important national initiatives.

61. Regarding **political interference**, the United States launched an investigation into Moscow's interference in its 2016 presidential election, led by US Special Counsel and former FBI Director Robert Mueller. The investigation has indicted 32 people and three Russian entities. The US Department of Justice has also indicted 12 Russian GRU intelligence officers for hacking Democratic Party representatives using spear phishing emails and malicious software. The 12 officers are also charged with releasing sensitive documents and stealing the data of half a million voters. This is the first US official indictment charging the Russian government with intending to influence the outcome of the 2016 election. Moscow denies any involvement and denounces a "conspiracy".

62. Considering mounting evidence of Russia's ongoing efforts to interfere in the upcoming 2018 US midterm elections – including attempts to hack US senators and the creation of fake official websites – a bipartisan group of senators introduced a bill to impose new sanctions on Russia for

meddling in US elections. These sanctions would mostly target the Russian sovereign debt, its energy projects and corrupted oligarchs.

63. Forewarned by events in the United States and informed by US intelligence services, French political forces managed to prepare for impending interference in their presidential election campaign. Then-candidate Emmanuel Macron's team hired cyber experts who suggested setting up decoy email accounts and prepared a communication strategy to deal with potential leakages.

64. German security services successfully minimised foreign interference in the 2017 elections by looking for vulnerabilities in networks. Unusually, the head of Germany's domestic intelligence agency went public to warn citizens about disinformation campaigns and cyberattacks from Russia (EUvsDisinfo, 2016). The British government helped protect its political system by tracking the major perpetrators of these attacks, providing politicians with professional expertise on communications security and working with media and think tanks to promote open discourse that counteracted propaganda. In the run-up to the Swedish elections in September 2018, authorities trained local election workers to spot and resist foreign influence, while Swedish political parties enhanced their email security systems. The Swedish Prime Minister announced the creation of a new agency responsible for bolstering the "psychological defence" of the Swedish public by "identifying, analysing, and responding" to "external influence" campaigns (Rettman, 2018).

65. As previously discussed, NATO's frontline states are concerned about **kinetic threats**, such as armed groups without military insignia. In addition to relying on NATO's support, these countries have an all-society approach to defence. Lithuania, for instance, reintroduced conscription and published a 75-page manual, entitled “Guide to Active Resistance”, for distribution in schools and libraries. It includes tips on civil disobedience in case of foreign invasion. Similarly, the US Army has drafted a new strategy for 2025 to 2040. It focuses on enemies that have not declared themselves as combatants in a context where the lines between war and peace are blurred. To meet these foes, the US Army is expected to move toward smaller, “semi-independent” and much more versatile formations able to fight in every domain of warfare simultaneously (Tucker, 2017).

66. Regarding **disinformation**, Germany has taken strict measures to limit hate speech and fake news on social media, imposing heavy fines (up to EUR 50 million) for companies – from Facebook to Google – that do not remove posts that incite hate or violence. In France, legislation has been proposed that would allow the Superior Council of the Audiovisual (CSA), a media watchdog, to take down contents, close user accounts and block websites in order to protect French democracy from fake news during elections. The proposed law would also establish responsibilities for the media to cooperate with the state and be transparent about their sponsored content.

67. NATO Allies in central and eastern Europe have taken aggressive steps to counter Russia's disinformation. Estonia recently increased the budget of its strategic communications department – responsible for countering propaganda – more than 13-fold. The Czech Republic has set up a Centre against Terrorism and Hybrid Threats in its Ministry of Interior to combat propaganda. The Centre uses a Twitter feed to debunk false stories. Lithuania hosts the US-funded Radio Liberty, which broadcasts to Russian and Belarusian audiences in their native languages.

68. In terms of **cyber**, a notable development has been the announcement by the United Kingdom of the creation of a new offensive cyber force of up to 2,000 personnel, which represents a near four-fold increase in manpower focused on offensive cyber operations (Haynes, 2018).

69. Sweden and Finland, non-NATO partners, are increasingly targeted by Russian hybrid activities. Both nations emphasise an educational approach to misinformation instead of restricting access to it. Both countries launched programmes to teach children to differentiate between real and fake sources as early as primary school. These tips are presented in entertaining formats, including in one of Sweden's most famous cartoon strips. Finnish Foreign Ministry officials claim that media

literacy education has helped Finns turn away from fake news and propaganda sites and led to the closure of the Finnish-language bureau of *Sputnik* due to low readership (Standish, 2017).

D. MEDIA AND CIVIL SOCIETY

70. Efforts to tackle hybrid threats are not confined to the government, but have proliferated among civil, academic and media organisations. The most prominent civic and academic initiatives to expose pro-Kremlin falsehoods include StopFake.org (an initiative by Ukrainian journalists and students), the Digital Forensic Research Lab (an effort by the US-based Atlantic Council think tank) and the Baltic "elves" (volunteer internet users in the Baltic states taking on pro-Kremlin trolls).

71. Traditional media have set up numerous fact-checking mechanisms, including the BBC's *Reality Check* and *Le Monde*'s 'Les Décodeurs'. Leading German and Swedish newspapers teamed up to prevent foreign information meddling during the election period. Recently, all major Lithuanian news outlets, the Baltic "elves" and Lithuania's Military Strategic Communications unit launched a joint initiative called *Demaskuok.lt* ("Debunk.lt") aimed at monitoring and debunking disinformation before it spreads in the country. The partners are using advanced algorithms and artificial intelligence to scan thousands of news articles in Russian and Lithuanian in order to detect potential fake news and disinformation. The initiative has generated considerable interest in NATO and EU circles.

72. Social media and technology giants, such as Facebook, Microsoft, Twitter and YouTube, mainly focus on removing terrorist-related contents. However, Facebook has cooperated to an extent with US authorities in the investigation of Russian meddling in US elections, and it unveiled new transparency guidelines related to advertising. In the same vein, Twitter has launched a battle against fake and suspicious accounts. The goal is to tackle the flow of disinformation on the platform and "better protect users from manipulation and abuse" Del Harvey, Twitter's vice president, said. More than 70 million accounts were suspended in May and June and it continues. Most of these accounts are Russian and similar to fake accounts used to interfere in the 2016 US election. The company also announced "major changes to the algorithms it uses to police bad behaviour" (Timberg & Dwoskin, 2018).

73. However, there is a growing pressure on social media companies to do more. In May 2017, the Home Affairs Select Committee of the British Parliament published a report that criticised social media firms for being "shamefully far" from tackling illegal and dangerous content. The absence of national borders in the cyber space makes it difficult for national legislators to force meaningful change, given that there is no commercial incentive for companies to share information with lawmakers or allow them to scrutinise their contents.

IV. CONCLUSIONS AND RECOMMENDATIONS

74. Russia's use of hybrid tactics poses a clear challenge to the Euro-Atlantic community. While Russia is much weaker economically and culturally, it often seems to have the edge in hybrid warfare because it has a unified decision-making process and a clear anti-Western agenda. The Kremlin is also not bound by the same ethical constraints as many NATO members, as manifested, *inter alia*, by the rigging of the recent Russian presidential 'elections' in favour of the incumbent – to the extent of stuffing ballot boxes in front of the cameras, setting up "troll factories" and even targeting individuals with weapons of mass destruction on foreign soil. The Kremlin exploits the open media landscape in the free world while eradicating free speech domestically and turning its media channels into weapons of mass deception. It sponsors extreme political movements in the West while persecuting the opposition at home.

75. Russia's hybrid machine is innovative and difficult to predict. In most cases, the Kremlin exploits and aims to amplify cleavages that already exist in Western societies. Therefore, it is imperative to focus on building the overall resilience of a society and addressing domestic grievances, rather than on efforts to predict Russia's next move. Examples from Sweden and Finland

are particularly relevant in this regard. Hybrid defence efforts should primarily be oriented inwards, rather than outwards against a specific country. The Alliance should harness the powers of democracy, free speech, basic human rights and the rule of law in a more proactive way to counter the vulnerabilities of a hybrid threat.

76. That said, the Rapporteur would like to offer several concrete proposals to enhance the Euro-Atlantic community's response to the Kremlin's hybrid operations:

- The Allies should revise their education policies to ensure that schools promote genuine, fact-based debate and critical thinking. New generations – who are avid social media users – ought to be encouraged to come out of their virtual bubbles and recognise signs of trolls and bots. Conventional armed forces play a supporting role in hybrid warfare, but the existence of an educated, patriotic and resilient society is our first line of defence.

- An effective response to hybrid threats depends on seamless teamwork, across different areas. There is a need for better coherence and coordination within NATO, especially by pulling together the available civilian and military assets.

- There is a need to increase strategic awareness. Member states must be able to assess events on the ground quickly and unanimously to respond effectively to Russia's hybrid threats. This effort requires greater intelligence sharing, reinforcing links between domestic agencies and a renewed discussion of the role of Special Forces in coordinating military assistance among NATO member states and partners. Some commentators suggest creating a designated "East Hub" for NATO, akin to the "South Hub" in Naples, Italy. However, the Rapporteur believes priority should be given to making full use of existing structures, such as NATO's Joint Forces Command located in Brunssum, the Netherlands.

- NATO members that have not yet designated specific government units charged with countering fake news and hostile propaganda with facts round-the-clock ought to do so. Existing NATO and EU capabilities, such as NATO's Public Diplomacy Division and the EU's East Stratcom Task Force, should receive additional financial, technological and human assets in order to better provide credible responses to hybrid warfare as often as possible.

- While focusing on domestic resilience, restrictive measures – such as the removing fake news, imposing penalties for spreading hate speech and blacklisting and freezing the assets of the most active Russian disinformation warriors – should continue to be applied. Members should seriously consider targeting the Western assets of corrupt Russian elites.

- Electoral structures should be designated as strategic infrastructure. National security and cyber institutions should offer their assistance to political parties and candidates in protecting their data and networks.

- While cyber defence is growing in priority, more creative thinking and multilateral cooperation across the Alliance is needed to enhance the security of our networks and systems. The Allies should consider strengthening their retaliatory capabilities in cyberspace, allowing NATO to call upon Allies to use, where appropriate, their offensive cyber capabilities in support of NATO operations. The protection of undersea communication cables should be prioritised.

- While welcoming the progress made in deepening NATO-EU cooperation on countering hybrid threats, more can be done in this area. The Rapporteur recommends the two institutions consider establishing a joint Brussels-based platform for combating hybrid threats. The organisations should also consider creating small NATO-EU counter-hybrid teams tasked with information fusion and analysis to enhance situational awareness (European Parliament, 2017).

- It is imperative to continue efforts to diversify energy imports and promote energy efficiency, including by implementing the vision of the EU Energy Union.

- To limit the space for Russian hybrid warfare, the problem of “grey zones” in eastern Europe must be addressed. Leaving eastern European countries in limbo is an invitation for further Russian aggression and tensions with the West. Georgia, Ukraine and Moldova, as well as the Western Balkan countries, should be given a clear membership perspective both in NATO and the EU. Their accession should be based solely on their implementation of membership criteria.

77. The Rapporteur supports the view that NATO should mainstream its role in responding to hybrid threats in its strategic documents. For example, the former British foreign secretary, William Hague, recently urged the Allies to consider revising the Washington Treaty and introducing an Article 5B. The new article would make clear that hybrid attacks would trigger a collective response from the Alliance. While changing the Treaty, which has withstood the test of time, might not have wide support among the Allies, the Rapporteur is convinced that the Allied leaders should initiate the drafting of the Alliance’s new Strategic Concept to reflect new global security realities, including the rise of hybrid threats. As Mr Hague put it: “The updating of NATO […] would mean that the Western alliance, so accustomed to the black and white choice of peace or war, would at last be adapting to the new world so beloved of President Putin and displayed in his election victory—a world of permanent grey.”

78. In conclusion, the Rapporteur wishes to stress that the Kremlin appears determined to disrupt collective European decision-making and reduce the influence of the United States on the continent. In its attempts to weaken the Euro-Atlantic security community, Moscow challenges our collective vision of a Europe that is whole and at peace. It is a daunting challenge, but the Euro-Atlantic community has the capacity to counter it if it acts in the spirit of solidarity. The wide international reaction to the outrageous use of chemical warfare on UK soil demonstrates that the international community is becoming aggressively impatient in response to Russia’s hybrid tactics. As the British Prime Minister, Theresa May, put it in her remarks to Russian leaders: "We know what you are doing, and you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies and the commitment of Western nations to the alliances that bind us."

BIBLIOGRAPHY

Asan. (2018, July 31). The Rise of Phantom Traders: Russian Oil Exports to North Korea. Retrieved from The Asian Insitute for Policy Studies: http://en.asaninst.org/contents/the-rise-of-phantom-traders-russian-oil-exports-to-north-korea/

BBC. (2017, December 15). Russia a 'risk' to undersea cables, defence chief warns. http://www.bbc.com/news/uk-42362500

BBC. (2017, November 17). UK cyber-defence chief accuses Russia of hack attacks. http://www.bbc.com/news/technology-41997262

Beebe, G. (2017, October 31). Containing Our Intelligence War with Russia. Retrieved from The National Interest: http://nationalinterest.org/feature/containing-our-intelligence-war-russia-22985

Belsat. (2017, December 22). Russia's foreign intelligence chief accuses West of waging hybrid war. Retrieved from Belsat: http://belsat.eu/en/news/russia-s-foreign-intelligence-chief-accuses-west-of-waging-hybrid-war/

Burgess, M. (2017, November 10). Here's the first evidence Russia used Twitter to influence Brexit. Retrieved from Wired: http://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency

Calabresi, Massimo. "Inside Russia's Social Media War on America." Time, 18 May 2017. http://time.com/4783932/inside-russia-social-media-war-america/

Chen, Adrian, "The Agency", The New York Times Magazine, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Edwards, J. (2017, December 3). British security services are vastly outgunned by the Russian counterintelligence threat. Retrieved from Business Insider: http://uk.businessinsider.com/british-security-services-vs-russian-counterintelligence-threat-2017-12?r=UK&IR=T

European Parliament. (2017, March). Countering hybrid threats: EU-NATO cooperation. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

Euronews. (2018, February 12). New report concludes Russian social media interfered in UK's EU referendum. Retrieved from Euronews: http://www.euronews.com/2018/02/12/new-report-concludes-russian-social-media-interfered-in-uk-s-eu-referendum

EUvsDisinfo. (2016, December 16). A threat to democracy. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/a-threat-to-democracy/

EUvsDisinfo. (2017, September 11). Three things you should know about RT and Sputnik. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/three-things-you-should-know-about-rt-and-sputnik/

EUvsDisinfo. (2017, December 21). What didn't happen in 2017? Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/what-didnt-happen-in-2017/

EUvsDisinfo. (2018, January 15). Chief Editor: RT is like "a defence ministry". Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry/

EUvsDisinfo. (2018, April 16). "USA Really. Wake Up Americans". The story of Russia's new private propaganda outlet. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/usa-really-wake-up-americans-the-story-of-russias-new-private-propaganda-outlet/

Foreign Affairs. (2017, November 13). How Big a Challenge Is Russia? Retrieved from Foreign Affairs: https://www.foreignaffairs.com/ask-the-experts/2017-11-13/how-big-challenge-russia

Galeotti, Mark, "The Kremlin's Newest Hybrid Warfare Asset: Gangsters", Foreign Policy, 12 June 2017, http://foreignpolicy.com/2017/06/12/how-the-world-of-spies-became-a-gangsters-paradise-russia-cyberattack-hack/

Galeotti, Mark, "Do the Western Balkans face a coming Russian storm?", European Council on Foreign Relations, ECFR/250, April 2018, https://www.ecfr.eu/page/-/ECFR250_do_the_western_balkans_face_a_coming_russian_storm.pdf

Gelzis, G., & Emmott, R. (2017, October 5). Russia may have tested cyber warfare on Latvia, Western officials say. Retrieved from Reuters: https://www.reuters.com/article/us-russia-nato/russia-may-have-tested-cyber-warfare-on-latvia-western-officials-say-idUSKBN1CA142

Greenberg, A. (2017, September 5). The NSA confirms it: Russia hacked French election 'infrastructure'. Retrieved from Wired: https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Grigas, A. (2017, November). Is Russia's Energy Weapon Still Potent in the Era of Integrated Energy Markets? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-November-2017.pdf

Grove, T., Barnes, J., & Hinshaw, D. (2017, October 4). Russia Targets NATO Soldier Smartphones, Western Officials Say. Retrieved from Wall Street Journal: https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402?utm_content=buffer2da6c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Hauer, N. (2018, August 27). Russia's Favorite Mercenaries. Retrieved from The Atlantic: https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/

Haynes, D. (2018, September 21). Britain to create 2,000-strong cyber force to tackle Russia threat. Retrieved from SkyNews: https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

House of Commons. (2018b, July 29). Disinformation and 'fake news': Interim Report. Retrieved from Digital, Culture, Media and Sport Committee: UK - Disinformation and 'fake news': Interim Report

House of Commons. (2018a, May 21). Moscow's Gold: Russian Corruption in the UK. Retrieved from Foreign Affairs Committee: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/932/932.pdf

Kramer, F. D. & Speranza, L. M. (2017, May). Meeting the Russian Hybrid Challenge. Retrieved from Atlantic Council: https://euagenda.eu/upload/publications/untitled-92736-ea.pdf

Kremidas-Courtney, C. (2018, June 11). Countering Hybrid Threats in the Maritime Environment. Retrieved from CIMSEC: http://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/36553

Kuhrt, N., & Feklyunina, V. (2017). Assessing Russia's Power: A Report. Retrieved from King's College London and Newcastle University: https://www.bisa.ac.uk/files/working%20groups/Assessing_Russias_Power_Report_2017.pdf

McFadden, C., Arkin, W. M. & Monahan, K. (2018, February 7). Russians penetrated U.S. voter systems, top U.S. official says. Retrieved from NBC News: https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721?cid=db_npd_nn_fb_fbbot

Murphy, M., Hoffman, F. G. & Schaub, G. (2016, November). Hybrid Maritime Warfare and the Baltic Sea Region. Retrieved from Centre for Military Studies, University of Copenhagen: http://cms.polsci.ku.dk/publikationer/hybrid-maritim-krigsfoerelse/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf

NATO StratCom Centre of Excellence, "Countering propaganda: NATO spearheads use of behavioural change science", 12 May 2015, https://www.stratcomcoe.org/countering-propaganda-nato-spearheads-use-behavioural-change-science

Polyakova, Alina, "Why Europe Is Right to Fear Putin's Useful Idiots", Foreign Policy, 23 February 2016, http://foreignpolicy.com/2016/02/23/why-europe-is-right-to-fear-putins-useful-idiots/

Rettman, A. (2017, November 13). Spain joins call for EU action on propaganda. Retrieved from EU Observer: https://euobserver.com/foreign/139843

Rettman, A. (2018, January 15). Sweden raises alarm on election meddling. Retrieved from EU Observer: https://euobserver.com/foreign/140542

Ringstrom, Anna, "Sweden security forces fear Russian military operations", Reuters, 18 March 2015, https://www.reuters.com/article/us-sweden-espionnage-russia/sweden-security-forces-fear-russian-military-operations-idUSKBN0ME1H620150318

Saarelainen, M. (2017, September 4). Hybrid threats – what are we talking about? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/

Sanger, D. E., & Frenkel, S. (2018, August 21). New Russian Hacking Targeted Republican Groups, Microsoft Says. Retrieved from The New York Times: https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html

Satter, R. (2018. August 28). Ungodly espionage: Russian hackers targeted Orthodox clergy. Associated Press: https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8/Nothing-sacred:-Russian-spies-tried-hacking-Orthodox-clergy

Shekhovtsov, Anton, "Russia and Front National: Following the Money", The Interpreter, 3 May 2015, http://www.interpretermag.com/russia-and-front-national-following-the-money/

Schmidle, Nicholas, "The U.S. Has More to Lose Than Russia in Spy Expulsions", The New Yorker, 7 August 2017, https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions

Shuster, S. (2017, September 25). How Russian Voters Fueled the Rise of Germany's Far-Right. Retrieved from Time: http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/

Smith, H. (2017, October). In the era of hybrid threats: Power of the powerful or power of the "weak"? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2017/11/Strategic-Analysis-October-2017.pdf

Standish, R. (2017, October 12). Russia's Neighbors Respond to Putin's 'Hybrid War'. Retrieved from Foreign Policy: http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland/

Swaine, J. (2018, August 6). Maria Butina's alleged backer linked to Kremlin-financed bank and Putin associates. Retrieved from The Guardian: https://www.theguardian.com/world/2018/aug/06/maria-butina-charged-spying-putin-russia-kremlin

The Economist. (2017, July 1). Fake news: you ain't seen nothing yet. Retrieved from The Economist: https://www.economist.com/news/science-and-technology/21724370-generating-convincing-audio-and-video-fake-events-fake-news-you-aint-seen

Timberg, C., & Dwoskin, E. (2018, July 6). Twitter is sweeping out fake accounts like never before, putting user growth at risk. Retrieved from The Washington Post: https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?noredirect=on&utm_term=.e2d094395640

Thornton, R. (2016, October 27). Russian "Hybrid Warfare" and the National Defence Management Centre (NTsUO). Retrieved from After 'hybrid warfare', what next? http://tietokayttoon.fi/documents/10616/1266558/Understanding+and+respond-ing+to+contemporary+Russia/49bdb37f-11da-4b4a-8b0d-0e297af39abd?ver-sion=1.0

Tucker, P. (2017, October 9). How the US Army is Preparing to Fight Hybrid War in 2030. Retrieved from Defense One: http://www.defenseone.com/technology/2017/10/how-us-army-preparing-fight-hybrid-war-2030/141634/?oref=d-topstory&utm_source=Sailthru&utm_medium=email&utm_campaign=EBB+10.10.2017&utm_term=Editorial+-+Early+Bird+Brief

Willsher, Kim, and Henley, Jon, "Emmanuel Macron's campaign hacked on eve of French election", The Guardian, 6 May 2017, https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election