ISSUE

CHAILLOT PAPER Nº 148 — October 2018

Hacks, leaks and disruptions

Russian cyber strategies

EDITED BY
Nicu Popescu and Stanislav Secrieru

WITH CONTRIBUTIONS FROM
Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, Jarno Limnell, Patryk Pawlak, Piret Pernik, Thomas Reinhold, Anatoly Reshetnikov, Andrei Soldatov and Jean-Baptiste Jeangène Vilmer

Chaillot Papers

European Union
Institute for
Security Studies

European
Union
Institute for
Security Studies

HACKS, LEAKS AND DISRUPTIONS

RUSSIAN CYBER STRATEGIES

Edited by Nicu Popescu and Stanislav Secrieru

CHAILLOT PAPERS *October 2018*

148

Disclaimer

The views expressed in this *Chaillot Paper* are solely those of the authors and do not necessarily reflect the views of the Institute or of the European Union.

European Union
Institute for Security Studies
Paris

Director: Gustav Lindstrom

© EU Institute for Security Studies, 2018.
Reproduction is authorised, provided prior
permission is sought from the Institute and the
source is acknowledged, save where otherwise stated.

Contents

Executive summary 5

Introduction: Russia's cyber prowess – where, how and what for? 9
Nicu Popescu and Stanislav Secrieru

Russia's cyber posture

1 **Russia's approach to cyber: the best defence is a good offence** 15
Andrei Soldatov and Irina Borogan

2 **Russia's trolling complex at home and abroad** 25
Xymena Kurowska and Anatoly Reshetnikov

3 **Spotting the bear: credible attribution and Russian operations in cyberspace** 33
Sven Herpig and Thomas Reinhold

4 **Russia's cyber diplomacy** 43
Elena Chernenko

Case studies of Russian cyberattacks

5 **The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine** 53
Piret Pernik

6 **Russian cyber activities in the EU** 65
Jarno Limnell

7 **Lessons from the Macron leaks** 75
Jean-Baptiste Jeangène Vilmer

8 **The next front: the Western Balkans** 85
Oscar Jonsson

EU and NATO approaches to cyber threats

9 **NATO's responses to cyberattacks** 95
Siim Alatalu

10 **Protecting and defending Europe's cyberspace** 103
Patryk Pawlak

Conclusion: Russia – from digital outlier to great cyberpower 115
Nicu Popescu and Stanislav Secrieru

Annex

Abbreviations 123

Notes on the contributors 125

Executive summary

Russia's increasingly hostile activities in the cybersphere have lent new urgency to the cybersecurity debate in the West. However, how Russia thinks about cyberspace and exactly what Russia gets up to in this realm is for the most part shrouded in opacity. This *Chaillot Paper* traces the evolution of Russia's coercive and diplomatic approaches in the cyber field, examines in detail the instances of cyberattacks that Russia is believed to have conducted in Europe, and explores how states and organisations (in particular the EU and NATO) are adapting to the growing number of cyber intrusions and operations orchestrated by Russia.

The Russian cyber challenge is not new. The first known cyberattacks initiated by Moscow against the US military date from 1986 at least. At the time, the Soviet Union, working in collaboration with the East German secret services, acted through West German cyber proxies. Realising the value and the low cost of remotely-conducted cyber intrusions, Moscow sought to overcome its 'cyber-laggard' status already in the 1990s, and despite the economic crisis afflicting the country at that time began to develop a sophisticated arsenal of cyber espionage tools.

The roots of Russia's global cyber power lie in its expertise in intelligence gathering as well as in Russian domestic politics. From the early 2000s Russia invested in cyber capabilities to combat Chechen online information campaigns as well as to monitor, disrupt or crack down on the online activism of various Russian opposition groups and independent media. This is when snooping and (dis)information campaigns were coordinated in a systematic way for the first time; trolls and bots were deployed; and the patterns of cooperation between the Russian state and proxy cyber-activists, or 'patriotic hackers', as Vladimir Putin once called them, started to develop. This *modus operandi* was created domestically, but from the late 2000s and early 2010s started to be applied internationally as well.

In parallel with numerous hostile acts in cyberspace Russia has been active since the early 2000s in multilateral and regional forums on cybersecurity issues, aspiring to become a norm-setter in this domain. Moscow's initiatives on the multilateral level have not paid off however. The diverging understanding of what cybersecurity means for Russia and the West partially explains why Moscow's norm-setting attempts have failed so far. Whereas Russia sees information security and state control of the internet as a priority, Western countries are primarily concerned with the security of personal data and defence of their critical infrastructure.

Russia's cyber diplomacy has gone hand-in-hand with increasingly assertive behaviour in cyberspace. Quite a number of countries have ended up on the receiving end of Russian cyberattacks, some of them designed to sabotage physical infrastructure (e.g. Georgia, Estonia, Ukraine, Montenegro), and some designed to feed into information campaigns during election periods or at times of heightened diplomatic tensions with Russia (e.g. the US, France, the UK.) International organisations have also been targeted, including the World Anti-Doping Agency (WADA) and more recently the Organisation for the Prohibition of Chemical Weapons (OPCW).

And yet all this begs the question: how do we know that Russia is the culprit? While it is true that covering your tracks and conducting false flag operations in the cybersphere is easier than undertaking military false flag operations in the real world, and therefore that Moscow might have been 'framed' by adversaries, plenty of indicators point to Russia nonetheless. To begin with, some attacks are so sophisticated and persistent that they are obviously not the work of criminal hackers in search of a quick cyber buck: it is clear that major actors, primarily states, are behind them. This premise often reduces the list of suspects to a rather short one. Moreover, cyber forensics and counter-intelligence activities make it possible to detect bits of code reused in various signature attacks, track hacking groups and establish more precisely the circle of perpetrators. In addition, language, geolocation, details pertaining to the actual times when the hackers were active online, or the stratagem of drawing attackers to 'honey pots' and 'beacons' (systems and information deliberately planted in order to monitor and track them or even hack them back), have all been used to trace specific cyber intrusions and attacks back to government-affiliated hackers. That is how meticulous cyber forensic investigations relying on the tools described above helped to identify Russia's two most capable hacking teams: APT28 and APT29.

Russia's cyberattacks have elicited a variety of responses. There have been instances when Western intelligence hacked the Russian hackers themselves, watching in real time how they conducted attacks. In Russia senior intelligence officials working on cyber were arrested for alleged cooperation with Western intelligence agencies. There have been pre-emptive responses to anticipated Russian hacks as well. The French handling of the 'Macron leaks' demonstrates how cyberattacks and disinformation operations were successfully deflected by feeding fake documents to the hackers containing deliberately far-fetched and ridiculous information designed to undermine the credibility of the leaks when they subsequently dumped the information online. This pre-emptive response also envisioned engaging the mainstream media to limit the publicity given to the results of criminal hacking activity in cases where there were no major public interests at stake; and 'naming and shaming' media outlets that propagate leaks such as Sputnik and RT.

All of the above has significant implications for Russia. The country is undoubtedly one of the world's great cyber powers. It has extremely sophisticated capabilities, and has integrated cyber tools in its foreign and security policy much more extensively than have other international players. But it must be remembered that Russia has achieved this in a context in which many international actors traditionally had something of a *laissez-faire* approach to cybersecurity, and certainly under-invested in cyber defence as a whole, and against cyber threats emanating from Russia specifically. Russia has inadvertently changed this state of affairs, possibly to its own detriment. Russian state cyber actors, but also private companies operating in the cybersecurity field, are now routinely treated with suspicion. The high-profile publicity that Russia has received in recent years as a result of its cyber operations has also spurred NATO and the EU to invest much more intensively in cybersecurity, which is likely to result in an escalation of defensive cyber activities *vis-à-vis* Russia. It has also led the US and many European states to adopt more assertive cyber strategies. Therefore it may be inferred that Russia's strategic 'cyber holiday' is now over, and that we have entered a new, much more contested phase of cyber geopolitics where the great cyber powers will henceforth adopt a more aggressive, 'gloves-off' approach.

Introduction: Russia’s cyber prowess – where, how and what for?

Nicu Popescu and Stanislav Secrieru

On 10 September 1986, Cliff Stoll, a systems administrator at the Lawrence Berkeley National Laboratory in California, called Chuck McNatt at the computer centre of the Anniston Army Depot in Alabama to inform him that a hacker called ‘Hunter’ was breaking into his computer systems. The hacker wanted to extract information from the US Army Redstone Rocket test site on US missile tests related to President Ronald Reagan’s flagship Strategic Defence Initiative, nicknamed ‘Star Wars’. This was one of the first known cyber espionage operations engineered by Moscow, in cooperation with East Germany, against the US military.

The hunt for ‘Hunter’ started as a quest to find out who (or what accounting error) generated a 75-cent shortfall, for 9 seconds of phone use, in the Laboratory receipts for computer use by other departments. Lax security practices at the time even in the military establishment meant that computer systems and networks were easy targets for hackers. Users of computers in the inner sanctum of the US military often simply used the word ‘password’ as their password. The CIA, FBI and NSA had not really dealt with hacking before. Intelligence officials were keen to be informed by Stoll, but it was unclear under what department’s jurisdiction such hacking activities fell. US intelligence finally got their act together, and three years later, in 1989, tracked the hackers down and in cooperation with the West German authorities arrested five culprits in and around Hanover. Among them was Hanover University physics student Markus Hess who had teamed up with several other hackers to collect sensitive information which was later sold to the KGB in exchange for $54,000 and quantities of cocaine. The hackers managed to attack 450 US military computers, and supplied the KGB with thousands of pages of printouts of US classified documents, passwords for US military computers, and details of the hackers’ own methods and techniques: how to break into specific (Vax) computers, which networks to use, as well as information on how military networks operated.[1]

---

[1] Clifford Stoll, *The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Pocket Books, 1989,) 267-366; John Markoff, “West Germans Raid Spy Ring That Violated U.S. Computers”, *New York Times*, March 3, 1989, https://www.nytimes.com/1989/03/03/world/west-germans-raid-spy-ring-that-violated-us-computers.html; Testimony on Hacking by Cliff Stoll, C-Span, May 15, 1989, https://www.c-span.org/video/?c4594226/epic-testimony-hacking-cliff-stoll-1989

This case represented a breakthrough in two important ways. On the one hand, it ushered in a new era of cheaper, safer and easier espionage, in which the Soviets turned US technological superiority into a vulnerability. On the other hand, this episode was remarkable for culminating in successful attribution and subsequent arrests. The investigators tracked the hackers by setting up a 'honeypot' – thousands of pages of fake documents featuring SDI (Strategic Defence Initiative) in their title were used as a bait to lure the hackers to spend more time online, thereby allowing law-enforcement agencies to track the hackers and ultimately catch them 'red-handed'.

Since then passwords have become more complex, cyber has become a mainstream concern, while cyber operations masterminded by Moscow are forcing businesses, militaries, politicians and diplomats in Europe and North America to scratch their heads in search of effective counter-strategies and responses. This *Chaillot Paper* seeks to shed some light on the less salient aspects of the current debate on the cyber threats faced by the European Union and its member states.

Russia is not the only source of cyber threats with which Europe has to contend. There are plenty of other malicious (state and non-state) cyber actors, such as China, Iran, North Korea, organised crime syndicates and terrorist groups active in the cyber domain. The US, Israel and many European states are also highly active in cyberspace, a realm which has become crucial to ensure national security. All of the above players have their own specialisations, niche capabilities and motives, and each deserves to be examined in their own right. But this *Chaillot Paper* will only focus on Russia, partly because it constitutes an interesting case of a major power where the cyber component is well integrated in domestic politics as well as in the country's foreign and security policies. Moreover Russia uses a whole panoply of cyber activities – espionage, cyber surveillance, 'simple' and sophisticated hacking operations, magnified through pro-active social media and diplomatic campaigns – to advance its interests as part of a larger 'hybrid warfare' strategy. This makes Russia more of a priority for European political leaders and publics than other cyber players.

The challenge for Europe is certainly twofold. On the one hand it is vital to understand what is going on at the technical level, but it is also necessary to be able to decipher the political thinking and the strategies behind cyber developments in Russia, as well as to gauge to what extent Russia's use of cyber tools in its foreign and security policy has been successful. This paper seeks to provide relevant insights by addressing several clusters of questions. One such cluster concerns Russia itself: what is the role of cyber in Russian domestic politics and what is the relationship between cyber activities conducted at home and abroad? How is Russian cyber diplomacy evolving? How different is Russia from other cyber powers? Is Russia in any way distinctive or unique as a cyber actor on the global stage? How do we know for sure if Russia is behind certain attacks? And is credible attribution possible at all?

The second cluster of questions deals with the numerous cyberattacks in Europe that have been attributed to Russia. How has use of cyberattacks evolved from the cases of Estonia and Georgia to Ukraine, France and the Western Balkans? How aggressive or, on the contrary, self-restrained has Russia been? The third cluster of questions concerns what lessons EU member states have learned, and in particular how the EU and NATO have been responding to these cyber challenges on the diplomatic, informational, political and security fronts.

Russia’s cyber posture

CHAPTER 1

Russia’s approach to cyber: the best defence is a good offence

Andrei Soldatov and Irina Borogan

In the centre of Moscow, on the corner of Lubyanka Square and Myasnitsky Street, stands a rather forbidding-looking building that was once the KGB’s computing centre. Today it houses the Information Security Centre of the Federal Security Service (FSB). The centre, which is the chief cyber branch of the Russian security service, was initially responsible for protecting computer networks and tracking down hackers, but in recent years its remit has been greatly expanded. Its activities now go beyond just protecting the government’s IT networks but also encompass closely monitoring the internet and the media as well as operations overseas. This reflects how far the thinking of the Russian secret services and the Kremlin’s approach to cyber in domestic and foreign policy has evolved since 2000. This chapter will first show how cyber tools were developed to address national security threats and to contain and constrain the opposition. The analysis then explores how the very tactics developed for tackling domestic problems migrated into Russia’s foreign policy toolbox. It will look in particular at how Russia’s penchant for cyber warfare spilled over into US-Russia relations. The concluding part of the chapter will examine the costs of Russia’s cyberwarfare and anticipate future developments in this domain.

The roots of Russian cyber policy

In 2000, when the brutal military campaign that would become known as the second Chechen war was in full swing, not only the army and secret services, but also the Russian population at large, needed to be convinced why this time the outcome would be different from the first Chechen War, which ended disastrously for the Kremlin when Moscow was forced to withdraw its troops from the rebellious republic. In short, they wanted to hear from the recently installed Russian president, Vladimir Putin, what went wrong then and how it could be fixed.

Vladimir Putin readily offered his explanation, which shifted the blame for military defeat onto the shoulders of independent journalists, thereby betraying deep mistrust of and antagonism towards a free media. The reason, he asserted, was that in the mid-1990s liberal Russian journalists and their foreign counterparts had undermined the war effort.[1] The media and other independent sources of information on the conflict therefore needed to be brought under tighter control. This became a key precondition for winning the second Chechen war.[2]

Thus, the Kremlin developed a new view of the nature of information – and decided to treat it as a weapon.[3] In a rare moment of frankness, Sergei Ivanov, the head of Russia's Security Council who would later become the minister of defence, declared that 'one must admit the obvious fact that along with the real fighting [in Chechnya] there is a virtual war underway, a media war [...].'[4] And the Kremlin was determined not to be a passive observer in this information conflict.

The problem was addressed at all levels. At the operational level, the war was rebranded as a 'counterterrorism operation' and the rules regarding media coverage of 'counter-terrorist activities' were tightened.[5] The accreditation rules for local journalists were made more stringent in violation of existing legislation, while access to Chechnya for foreign journalists was severely curtailed. In less than two years, most Russian media outlets were forced to fall in with the government line – those who did not were subjected to sackings, hostile takeovers and criminal investigations.[6] The seizure of the NTV channel which led to a purge of management and an exodus of reporters is the most glaring example of the Kremlin's campaign to subdue the still-independent press in the early 2000s.[7] On the conceptual level, in 2000 Vladimir Putin signed the Information Security Doctrine, the first policy document of its kind. It itemised an unusually broad list of threats, ranging from the 'degradation of spiritual values', to the 'weakening of the spiritual, moral and creative potential of the Russian population', as well as the 'manipulation of information (disinformation, concealment or misrepresentation).'[8] It also identified one major source of threat as 'the desire of some countries to dominate and encroach on the interests of Russia in the global information space.'[9]

---

[1] See Putin's interview to the First Channel in 2000. Available on YouTube: https://www.youtube.com/watch?v=ptOEMK5uYQQ

[2] "Russia's Media War Over Chechnya," *BBC*, November 19, 1999, http://news.bbc.co.uk/2/hi/world/monitoring/528620.stm

[3] See, for instance, the article "Information as a Weapon" published by a pro-Kremlin military expert Alexander Khramchikhin in *Nezavisimaya Gazeta*, February 13, 2015.

[4] David Hoffman, "In Chechnya, Russia Is Also Fighting a Propaganda War," *Washington Post*, January 25, 2000, https://www.washingtonpost.com/archive/politics/2000/01/25/in-chechnya-russia-is-also-fighting-a-propaganda-war/905c6e0a-1eca-4516-ad84-40a2dcf0ddbe/?noredirect=on&utm_term=.fb36b5ce75af

[5] Laura Belin, "Russian Media Policy in the first and second Chechen campaigns," Paper presented at the 52nd conference of the Political Studies Association, Aberdeen, Scotland, 5-8 April 2002, https://www.infoamerica.org/documentos_pdf/rusia.pdf

[6] Ibid.

[7] Yevgeny Kiselyov, "The Seizure of NTV 10 Years On," *Moscow Times*, April 20, 2011, https://themoscowtimes.com/articles/the-seizure-of-ntv-10-years-on-6453

[8] Russian presidential decree no. 1895, "Doktrina informationnoi bezopasnosti Rossiiskoi Federatsii" [Doctrine of Russian Information Security], September 9, 2000, http://base.garant.ru/182535/

[9] Ibid.

These were the rules of engagement as designated by the Kremlin: content generated by journalists and media outlets not under the state authorities' control could present a threat to the national security of Russia – meaning the political stability of the regime. This included the internet from the very beginning – as early as in 1999 the Russian foreign ministry helped to draft a resolution for the UN General Assembly that warned that information disseminated on the internet could be misused for 'criminal or terrorist purposes' and could undermine 'the security of States.'[10]

In the Kremlin's discourse about the internet, the terms 'information security', 'information wars', and 'information warfare' became pervasive. According to one academic researcher, 'in December 2013 the keyword "information warfare against Russia" in Russian generated more than 700,000 posts in Google and more than 4,000 videos in YouTube.'[11] The discourse has been matched by some institutional reshuffling. The cyber intelligence department of the FSB was renamed the 'Information Security Centre' (ISC) in 2002 – prior to that it was known as the Directorate of Computer and Information Security (UKIB).

Use of such language ('information security/warfare' etc) started a global rift between Russian and Western cyber government experts: while the Russians insisted on talking about information warfare, meaning state control of media content, Western experts wanted to talk only about cyberwarfare, which is mostly about protecting a nation's critical digital networks.[12]

In the early 2000s, the main players established themselves globally in the cyber arena. In Russia, those were the Russian secret services – the FSB's Information Security Centre and the Russian electronic intelligence agency, known as the Federal Agency for Government Communications and information (FAPSI) until it was largely absorbed by the FSB in 2003. The generals who ran FAPSI/FSB defined the rules – they wrote the Information Security Doctrine as they dominated the information security branch of Russia's Security Council. In the US, the first document of this kind (much narrower in its scope than its Russian counterpart), entitled 'National Policy on Telecommunications and Automated Information Systems Security' (NSDD-145), was drafted by officials in the Defence Department.[13] However, the Russian military, which experienced a sharp drop in budget allocations in the 1990s and a corresponding decline in prestige, did not have much say in cyber affairs until 2013 when the ministry of defence announced plans to create its 'cyber troops',[14] probably one of the lessons drawn from Russia's war with Georgia in 2008.

---

[10] United Nations General Assembly, "Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security," January 4, 1999, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R

[11] Ieva Berzina, "The Narrative of 'Information Warfare against Russia' in Russian Academic Discourse", *Journal of Political Marketing*, 17, no. 2 (2018): 162.

[12] Pasha Sharikov, "Understanding the Russian Approach to Information Security," *ELN,* January 16, 2018, https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/

[13] Fred Kaplan, *Dark Territory. The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 1-20.

[14] "V Minoborone RF sozdali voiska informatsionnih operatsii" [Russia's Ministry of Defense set up information troops], *Interfax*, February 22, 2017, http://www.interfax.ru/russia/551054

Internationally, the Kremlin's approach was defined by the FSB generals at the Security Council (the group led by Vladislav Sherstyuk)[15] and the foreign ministry's Department for New Challenges and Threats (headed by the Kremlin's special envoy on cybersecurity, Andrey Krutskikh). Intellectual support was provided by Moscow State University's Information Security Institute, a think tank founded and led by Sherstyuk.

However, as things unfolded, it became clear that these state actors presented only the official façade of the Kremlin's approach to cyber issues. When in the early 2000s the Kremlin was busy clamping down on the media, the Russian secret services were faced with a formidable challenge: pro-Chechen separatist and islamist websites were still functioning. Chechens maintained servers outside Russia and, despite the Kremlin's best efforts, some Western governments refused to shut the sites down.[16] Then, in January 2002, a popular Chechen website affiliated with rebels (www.kavkaz.org) was closed down. It had been attacked by hackers, students in the Siberian city of Tomsk. The local branch of the FSB, the Russian secret police, enthusiastically supported the students' actions, defending them as the legitimate 'expression of their position as citizens, one worthy of respect'.[17]

Outsourcing cyber warfare

The attack heralded a new approach. The Kremlin began to outsource hacking operations and cyberattacks to a network of informal actors – activists, criminal groups and possibly even legitimate cyber tech firms. Resorting to this tactic allowed Russia to create plausible deniability and lower the costs (including in reputational terms) and risks entailed by controversial overseas operations.[18] Sometimes these actors have been aided and abetted by the secret services – as was clearly the case when the hidden videos and phone conversations of Russian opposition leaders were leaked and widely circulated by informal groups between 2010 and 2016.[19] In other cases, government support was much more difficult to detect (at least in the short term) as the Kremlin managed to hide all possible traces which might connect perpetrators with the Russian state. That was the case of the infamous attack on Estonian websites in 2007. On 27 April of that year, Russian hackers attacked the websites of the Estonian government, parliament, banks, ministries, newspapers, and broadcasters (for more on this, see chapter 5 in this volume on 'The early days of cyberattacks', pp. 53-64). Estonian foreign minister Urmas Paet accused the Kremlin of having orchestrated the cyberattacks.[20] But Estonia failed to present proof of the Russian government's involvement, and in September 2007 the country's defence minister admitted that did not have sufficient evidence to link the attacks to the Russian government.[21] However, two years later the plausible deniability cover was blown. In May 2009, Konstantin Goloskokov, one of the activists of the pro-Kremlin Nashi movement (which received state funds), admitted to the *Financial Times* that he was behind the series of cyberattacks on Estonia in 2007.[22] It is not clear why he confessed, but his interview represents circumstantial evidence that via Nashi (which also in 2007 conducted a harassment campaign against the UK's ambassador in Moscow until it was called off by Russian officials[23]) the Kremlin was indeed behind the cyber assault on Estonia.

---

[15] Vladislav Sherstyuk, originally a KGB officer who by the 1990s had become head of the obscure and powerful Third Department of the Federal Agency for Government Communications and information (FAPSI), in charge of spying on foreign telecommunications; in 1998, he was appointed director of FAPSI, and in the 2000s he moved to the Security Council.

[16] "Chechen Rebel Website Reopens," *BBC*, October 8, 2004, http://news.bbc.co.uk/2/hi/europe/3727266.stm

[17] Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: Public Affairs, 2010), 231.

[18] "Russia Denies U.S. and UK Allegations of Global Cyber Attack," *Moscow Times*, April 17, 2018, https://themoscowtimes.com/news/russia-denies-us-and-uk-allegations-of-global-cyber-attack-61195

[19] "Kremlin Accused of Opposition Phone Call Leaks," *BBC*, December 20, 2011, https://www.bbc.com/news/av/world-europe-16279131/kremlin-accused-of-opposition-phone-call-leaks; "Navalny's Private E-Mails Leaked," *Moscow Times*, October 27, 2001, https://themoscowtimes.com/news/navalnys-private-e-mails-leaked-10439; "Mikhail Klikushin, Former Russian Prime Minister Caught on Camera Having Sex With Opposition Leader," *Observer*, May 4, 2016, http://observer.com/2016/04/former-russian-prime-minister-caught-on-camera-having-sex-with-opposition-leader/

The apparent low costs/low risks of such operations paid off. The cyberattacks in Estonia worked, the operation was not costly and Russia was able to claim (for two years at least) plausible deniability.

The success of Russia's cyber warfare strategy is due to two main factors. First, these days Russia's coercive foreign policy includes an aggressive cyber component: examples include denial-of-service attacks on neighbouring countries as a punishment for actions regarded as running counter to Russian interests;[24] the leak of an intercepted phone conversation between Victoria Nuland, the Assistant Secretary of State for European and Eurasian Affairs, and the US ambassador to Ukraine, which then provoked tensions between the US and Europe during the Maidan protests in Kyiv;[25] trolling international media to promote Russia's view on the conflict in Ukraine;[26] the hacking of a power plant in Ukraine in 2015;[27] and alleged meddling in the US election in 2016.[28]

---

[20] "Russia Accused of 'Attack on EU'," *BBC*, May 2, 2007, http://news.bbc.co.uk/2/hi/europe/6614273.stm

[21] Adrian Blomfield, "Russia Accused over Estonian 'Cyber-Terrorism'", *The Telegraph*, May 17, 2007, https://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html

[22] Charles Clover, "Kremlin-backed Group behind Estonia Cyber Blitz," *Financial Times*, March 12, 2009, https://www.ft.com/content/57536d5a-0ddc-11de-8ea3-0000779fd2ac

[23] Luke Harding, "Pro-Kremlin Group Told to Stop Harassing British Ambassador", *The Guardian*, January 18, 2007, https://www.theguardian.com/world/2007/jan/18/russia.lukeharding

[24] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia; John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html

[25] "Ukraine Crisis: Transcript of Leaked Nuland-Pyatt Call," *BBC*, February 7, 2014, https://www.bbc.com/news/world-europe-26079957; "Angela Merkel Fumes at US Diplomat's Curse of EU", *The Telegraph*, February 7, 2014, https://www.telegraph.co.uk/news/worldnews/europe/germany/10624361/Angela-Merkel-fumes-at-US-diplomats-curse-of-EU.html

[26] Lucy Fisher, "Russian Leaks Reveal Spin on MH17 Disaster," *The Times*, April 19, 2018., https://www.thetimes.co.uk/article/russian-leaks-reveal-spin-on-mh17-disaster-0xgpl0tj0. See for more examples: StopFake.org

[27] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[28] "US Punishes 19 Russians over Vote Meddling and Cyber-attacks," *BBC*, March 15, 2018, https://www.bbc.com/news/world-us-canada-43419809

Second, the growing prominence of the cyber component inevitably began to blur the line between domestic and external policy and led to institutional overlaps. Back in the days of the Soviet Union there was a clear demarcation between actors carrying out disinformation operations inside and outside the country: disinformation campaigns conducted beyond Soviet borders were run by the Active Measures Department of the First Chief Directorate of the KGB and Agency Press News (APN), which never conducted operations inside the country.

This changed in the late 2000s and early 2010s when the same informal networks were tasked with attacking the Kremlin's critics both inside the country and outside. Fancy Bear, a group behind a cyberattack on the US Democratic National Committee (DNC) during the presidential election, was caught targeting Russian independent journalists in September 2016; while the Internet Research Agency in St. Petersburg, a troll farm with links to the Kremlin, engaged in trolling operations in Europe and the US, was tasked with a disinformation campaign after the assassination of prominent Russian opposition politician Boris Nemtsov in Moscow, in the vicinity of the Kremlin, in 2015.[29]

This approach has at least two ramifications. On the one hand, overlap between domestic and external operations ignites competition between institutions which possess cyber capabilities. Each tries to prove to the Kremlin that it is more useful than the others and thus to secure greater access to the Kremlin's levers of power and patronage, but also increased funding and privileges.[30] On the other hand, it seems that the Kremlin tends to treat every domestic or international crisis in terms of threats to internal political stability – regardless of whether the crisis constitutes a danger to the regime in Moscow or not.

As a result Russian cyber foreign policy is largely responsive to crises (e.g. the furore over the removal of the Bronze Soldier statue in Tallinn in 2007) as well as to emerging opportunities (e.g., the Brexit referendum), thus essentially tactical rather than strategic. However, cyber tools are not applied indiscriminately to every crisis or opportunity that arises. Thus, these tactics also make the Kremlin's moves less predictable as it is hard to anticipate when or where it will strike and which combination of cyber tools it will employ. This is hardly a new strategy, however.

---

[29] "Interview s eks-sotrudnikom 'fabriki trollei' v Sankt-Petersburge" [Interview with former employee at troll-farm in Saint Petersburg], *DojdiTV*, October 14, 2017, https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/; Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike blog*, June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

[30] For more see Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: Public Affairs, 2010).

From Cold War to cyber war

The temptation to think that the lessons of the Cold War are applicable to cyber has been popular since the mid-2000s. Government experts of the early 2000s, in Russia as well as the West, believed that the internet could be treated as just another battlefield, where the rules of engagement could be clearly defined.[31]

Since 2013, Russia, the United States and Europe have been busy putting together a set of international rules called cyber CBMs, or 'confidence-building measures.' The person who developed the cyber CBMs concept was Michele Markoff, an experienced American diplomat who had spent half her career in strategic nuclear arms control negotiations. In 1998 she began to specialise in cyber diplomacy and subsequently became a key figure at the Office of Cyber Affairs in the State Department.

The career of her Russian counterpart, Andrey Krutskikh, had followed a similar trajectory—from nuclear arms control to cyber. In the 2010s Markoff and Krutskikh represented their respective countries at most of the talks between Russia and the United States on cyberspace.[32]

Markoff believed that the internet needed to be governed by a set of measures similar to those established to prevent a nuclear war. These controls, in her view, could prevent a cyber conflict from escalating. In June 2013 she secured the US-Russia bilateral agreement on confidence-building in cyberspace.[33] As part of the agreement the White House and the Kremlin established a Direct Communications Line that connects the US Cybersecurity Coordinator and the deputy head of the Russian Security Council and could be used 'should there be a need to directly manage a crisis situation arising from an ICT [information and communications technology] security incident.' It was the digital era's equivalent of the Cold War red telephone that connected the presidents of the Soviet Union and the United States in emergencies. The new hotline was even integrated into the existing infrastructure of the Nuclear Risk Reduction Center, located in the Harry S. Truman Building, the headquarters of the US State Department.

It was from there at the end of September that Michael Daniel, the Obama administration's Cybersecurity Policy Coordinator, passed a message to Sergei Buravlyov, deputy secretary of the Russian Security Council and Colonel General of the FSB. 'This was the first time it was used since it was established', according to Daniel,[34] whose mission was 'to communicate the US government's serious concerns about the Russian information operation to attempt to influence the election.' He declined to comment on how his Russian counterpart received the message, but it was obviously not a diplomatic success. In October 2016 another batch of emails damaging to one of the US presidential contenders was leaked to the press.[35]

---

[31] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 273.

[32] "Amerikanskii Gosdep podtverdil vstrechu po kiberbezopasnosti s Rossiei" [US State Department confirmed meeting on cyber security], *Rosbalt*, February 7, 2017, http://www.rosbalt.ru/world/2017/02/07/1589659.html

[33] "Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security," The White House, June 17, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

[34] Authors' interview with Michael Daniel, by phone, May 2017.

This illustrates how a modern cyber conflict is simply not comparable with a conventional armed or nuclear conflict. When there is a missile launch or preparation for a missile launch, it is impossible for the government to deny responsibility. However, all kinds of informal actors who are not easily detected can launch cyberattacks. Early on the Kremlin realised this and has exploited the opportunity to the full.

The costs of cyberwar

One of the unforeseen consequences of Russia's aggressive cyber tactics, combined with its continued denial of any role or involvement in cyberattacks, has been the complete loss of trust in Russia among the Western cyber expert community and Western governments.[36] The new climate of mistrust has affected Russian government institutions, including the foreign ministry and law enforcement agencies, the secret services,[37] as well as Russian private cybersecurity companies, among which Kaspersky Lab is the most visible example. Kaspersky Lab is facing reputational and financial damage as the company has failed to explain its opaque relationship with the Russian secret services.[38] This also creates an environment where Russia is seen as a prime suspect in every cyberattack conducted in the West, with the result that the strategy of plausible deniability no longer works for Russia – although on the plus side (from Moscow's point of view) this reinforces the perception of Russia as a pugnacious and aggressive foreign policy actor.

Russia was the first suspect when the opening ceremony of the Winter Olympic Games in PyeongChang was disrupted by a cyberattack in February. The cyberattacks disabled internet access and broadcast systems, shut down the PyeongChang 2018 website and prevented spectators from printing out their tickets. Cyber experts swiftly concluded that the hackers aimed to disrupt the Olympics and destroy a lot of data on servers rather than steal information using malware dubbed the 'Olympic Destroyer'. While most security experts were quite cautious about attributing responsibility for the attack to a particular country or government, pundits and commentators pointed the finger at Russia as the most likely culprit. Clearly, Russia can no longer hide behind the mask of plausible deniability as now when cyberattacks occur it is invariably designated as the prime suspect.

---

[35] Amelia Heathman, "Aliens and Arms Deals: the Wikileaks 'October Surprise' Data Dumps Have Begun", *Wired*, October 12, 2016, https://www.wired.co.uk/article/wikileaks-plans-target-us-election

[36] Nikki Haley, "We Can't Trust Russia", *CNN*, July 9, 2017, https://www.youtube.com/watch?v=tRaU07vgh-c

[37] Mark Landler and Gardiner Harris, "In Retaliation, U.S. Orders Russia to Close Consulate in San Francisco", *New York Times*, August 31, 2017, https://www.nytimes.com/2017/08/31/us/politics/russia-consulate-close-retaliation.html

[38] Dustin Volz, "Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software", *Reuters*, December 12, 2017, https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4

Looking ahead

Apparently, 'a low cost-low risk' strategy of using proxies in overseas operations proved to less low cost and deniable than was imagined at the outset. Russia overused plausible deniability to such an extent that the Kremlin is now suspected of being behind any major cyberattack that takes place in the West. But it does not look like the Kremlin has an alternative strategy to fall back on. Moreover, it lacks incentives to find one. On the one hand, the direct costs are not yet very prohibitive,[39] while cyberattacks are still considered to be a useful foreign policy tool which helps to keep immediate neighbours under pressure.

On the other hand, Russia's increased assertiveness in cyberspace has led other great powers with wider bandwidth to reassess their vulnerabilities and beef up national cyber defence infrastructures. If Russia wants to remain in the top league of the world's great cyber powers, it will have to keep pace with others in what looks like a new cyber race. Clearly the Kremlin fully intends to invest in, develop and test new cyber intrusion methods, and thus to preserve its capacity to surprise and harm its opponents in cyberspace and beyond whenever it deems necessary.

---

39. According to US Special Counsel Robert Mueller's investigation, GRU agents spent around $95.000 to hack computers in the US and to release the information obtained in this way, while a Russian troll farm spent $1.25 million monthly on ad campaigns. See: "Mueller Indictment against 12 Russian Spies for DNC Hack", *VOX*, July 13, 2018, https://www.vox.com/2018/7/13/17568806/mueller-russia-intelligence-indictment-full-text; "Russia Spent $1.25 million per Month on Ads, Acted Like an Ad Agency", *AdAge*, February 16, 2018, http://adage.com/article/digital/russia-spent-1-25m-ads-acted-agency-mueller/312424/

CHAPTER 2

Russia’s trolling complex at home and abroad

Xymena Kurowska and Anatoly Reshetnikov

Political trolling in Russia has reached massive proportions, as evidenced by both investigative journalism revealing the existence of ‘troll factories’[1] and ‘big data’ analysis of trolling activity on the internet.[2] Russian ‘trolls’ have also been officially charged with Kremlin-orchestrated hacking and interference in other countries’ affairs, most notably elections.[3] But what is the philosophy behind trolling, and what is its effect on political communication? This chapter looks at both the internal and external dimensions of Russia’s trolling complex. Within Russia, trolls’ activities serve to neutralise dissident voices on the internet and thereby reduce the potential for anti-regime political mobilisation. Moscow deploys trolls abroad as part of a disruptive and subversive strategy, undermining the liberal order to its advantage.

The philosophy behind the trolling complex

In 2014, in the midst of the war in the Donbass, when the Russian defence minister Sergey Shoygu was asked whether Russian troops had been deployed in the southeast of Ukraine, he replied cryptically: ‘It is very difficult to look for a black cat in a dark room, especially if it is not there. All the more stupid to look for it there if this cat is clever, brave and polite.’[4] The insinuation is that it makes no sense to ask about the existence of the putative cat. If the black cat is there – which, in fact, it is – the cat is clever enough to make its presence undetectable, and hence immune from liability.

---

[1] Alexey Kovalev, “Russia’s Infamous ‘Troll Factory’ Is Now Posing as a Media Empire,” *Moscow Times,* March 24, 2017, https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534; Dmitry Volchek and Daisy Sindelar, “One Professional Russian Troll Tells All,” *RFE/RL*, March 25, 2015, https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html.

[2] Oliver Roeder, “What You Found In 3 Million Russian Troll Tweets,” *FiveThirtyEight*, August 8, 2018, https://fivethirtyeight.com/features/what-you-found-in-3-million-russian-troll-tweets/.

[3] “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

[4] *Lenta.ru*, April 17, 2014, https://lenta.ru/news/2014/04/17/shoygu/; *Novaya Gazeta*, December 14, 2017, https://www.novayagazeta.ru/articles/2017/12/14/74914-ministr-prevyshe-vsego.

This anecdote reflects the perverse logic behind trolling. In the popular discourse in today's Russia, the adjective 'polite' is often used as an ironic allusion to the Russian military presence in the Crimea. Russian soldiers in the Crimea have been described both as 'little green men', referring to their camouflage, and as 'polite people' in an effort to portray them as peaceful and non-interfering in local people's lives.[5] In this context, Shoygu's reply simultaneously denies and confirms the presence of Russian troops in the southeast of Ukraine. Evasiveness, prevarication and maintaining ambiguity about the truth is a common political tactic in contemporary Russia, one which is consolidated by political trolling. In lieu of classical propaganda geared to convince and manufacture consent,[6] the government's strategy is to manufacture cynicism that stimulates disengagement. Cynicism is a weapon in this context: political trolling seeks to undermine, or suspend, the normative foundations of key areas and principles of liberal governance (such as, for example, elections, democracy, the right to self-determination), by invoking those principles rhetorically, but also ridiculing and deriding their content in actual practice. The writer Peter Pomeratsev's formulation, '[n]othing is true and everything is possible,'[7] aptly describes the cynicism underpinning Russia's trolling complex.

Pro-Kremlin trolling customises for regime purposes activities which used to be the domain of private actors. Originally trolling is a recreational activity carried out by relatively privileged private individuals that self-organise.[8] Pro-Kremlin trolls tend to be precarious workers who are commissioned to perform specific tasks and whose incentive is therefore not self-expression but the need to earn a living. The classic trolling premise of 'doing it for the lulz', that is, for the digital *schadenfreude* produced by pranks and insults, is adapted to further the political purposes of a regime, which is antithetical to the original trolling 'ethos'. The method is to re-appropriate the liberal values of the freedom of speech and civic engagement to create a semblance of citizenry action. In other words, pro-Kremlin trolling relies on citizens' critical faculties to get them engaged in a debate. However, they quickly become alienated as they realise that their engagement proves futile in an internet environment characterised by absurd fabrications, red herrings designed to confuse and mislead, politically-charged attacks and even taunts and insults. Dissident voices appear to be yet another mirage which discourages political mobilisation before it can materialise.

---

[5] Roland Oliphant, "Ukraine Crisis: 'Polite People' Leading the Silent Invasion of the Crimea," *The Telegraph*, March 2, 2014, https://www.telegraph.co.uk/news/worldnews/europe/ukraine/10670547/Ukraine-crisis-Polite-people-leading-the-silent-invasion-of-the-Crimea.html

[6] Edward Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media* (New York: Pantheon Books, 2002).

[7] Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (London: Public Affairs, 2015).

[8] On trolling see e.g. Gabriella Coleman, Hacker, *Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London & New York: Verso, 2015); Wendy Phillips, *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture* (Cambridge, MA & London: MIT Press, 2015).

Techno-authoritarianism: 'neutrollisation' in domestic politics

Russia uses this approach both at home and abroad. Of course, there are undoubtedly millions of genuine Russia-based supporters of the current regime who disseminate their views in the Russian blogosphere. But trolls do not fall into this category – and they are also quite numerous.

We know this because trolling and bot accounts have their identifiable specificities. Bots are easy to pin down and quantify through network analysis because a bot is a software application which runs automated and structurally repetitive tasks at a high rate.[9] One study estimates that from February 2014 to December 2015, during a particularly intense period in Russian politics, the activity of bots among accounts actively tweeting about Russian politics exceeded 50%.[10] NATO's Strategic Communications Centre of Excellence (NATO Stratcom COE) assesses that between February and April 2018 only 7% of active users who post in Russian were recognisable as humans or institutions and the remaining 93% were news accounts, bots, hybrid, or anonymous.[11] Trolling accounts maintained by humans are more difficult to identify and need to be examined for patterns that diverge from regular users' behaviour: the absence of personal details, photos, links to other social networks, mentions of relatives and friends, etc.[12] Thematically, a typical troll account usually consists of a stream of non-personal and ludicrous content punctuated with frequent political posts. It is usually investigative journalists and former trolls that help with such identifications, as the authors of this chapter explain in a previously published study of this subject.[13]

Most organised pro-Kremlin trolls work for the Internet Research Agency LLC, commonly known as a 'troll factory'. The agency was founded in the summer of 2013 in Ol'gino in St Petersburg in the aftermath of two developments: the emergence of social media as a platform for political mobilisation during the Arab Spring, and the nationwide wave of anti-regime protests that took place in Russia between 2011 and 2013. The protests were organised by civil society actors and in particular by the so-called 'non-systemic' opposition.[14] The scale of anti-regime mobilisation in those years was the highest since the 1990s. The protest movement resulted in a series of programmatic documents, among them the 'Manifesto of Free Russia' published online by Boris Nemtsov, which called for radical political change.[15] The government liberalised party legislation and reinstated the direct election of governors as a concession (although, regarding the latter, they also introduced municipal and presidential filters which *de facto* meant that the federal government retained a lot of control over regional politics). Since then, however, as evidenced by surveys conducted by the Levada Center, the share of Russian citizens that are willing to participate in protests driven by political demands has been slowly decreasing (save for a brief hike in potential participation in the spring and summer of 2017).[16] This registered decline was most certainly a result of a complex combination of factors, and the authors do not seek to claim here that institutionalised political trolling was the most important of those. Yet, as becomes obvious from a closer look at the actual practice of pro-Kremlin trolling activities, their main aim was unequivocal: to neutralise potential social mobilisation at its origin.

---

[9] Lawrence Alexander, "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign", *Global Voices*, April 2, 2015, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/.

[10] Denis Stukal, Sergey Sanovich, Richard Bonneau and Joshua A. Tucker, "Detecting Bots on Russian Political Twitter", *Big Data 5*, no. 4 (December 2017), https://www.liebertpub.com/doi/full/10.1089/big.2017.0038.

[11] Robotrolling, 2018/2, https://www.stratcomcoe.org/robotrolling-20182-0.

[12] Andrey Soshnikov, "Stolitsa politicheskogo trolling" [The capital of political trolling], *Moy Rayon*, March 11, 2015, http://mr7.ru/articles/112478/.

[13] Xymena Kurowska and Anatoly Reshetnikov, "Neutrollization: Industrialised Trolling as a Pro-Kremlin Strategy of Desecuritization," *Security Dialogue*, 49, no. 5 (2018): 345-363.

[14] That is, one operating outside of the parliament, as the parliamentary opposition is widely believed to have been co-opted by the regime to perform a largely symbolic function.

A trolling frenzy in the aftermath of the assassination of Boris Nemtsov in February 2015 shows this mechanism in practice. Nemtsov was an important leader of the Russian ‘non-systemic’ opposition and his assassination could have damaged the Kremlin if the authorities were shown to have been implicated. In March 2015, *Novaya Gazeta* and *Moy Rayon* published four leaks containing lists of troll accounts with descriptions of their tasks in connection with the assassination of Nemtsov.[17] Trolls were tasked to: spread the view that the authorities did not stand to gain by the assassination and that it was a provocation aimed at creating the impression of the regime’s complicity; portray the opposition as capitalising on the death of their comrade, and thereby incite negative attitudes towards them; insinuate the involvement of Ukrainian individuals; and criticise Western politicians for using Nemtsov’s murder as an excuse to interfere in Russia’s internal affairs. Each post was to include some keywords to facilitate searchability: ‘opposition’, ‘Boris Nemtsov’, ‘assassination of Nemtsov’, ‘provocation’, ‘opposition in Russia’.[18] An empirical analysis[19] demonstrates the ‘flooding effect’ of the coordinated spread of pre-fabricated messages that the pro-Kremlin trolls subsequently generated. They used highly sensationalist and contradictory content to simulate a public forum that had the appearance of having been generated by ordinary citizens. Their aim was to sow discord and confusion by making it near impossible to separate truth from fiction and intervene in the discussion in a meaningful way.

The ambiguity of trolls who maintain the appearance of authenticity makes it particularly difficult to blow the whistle on a troll. A direct confrontation ends up ‘feeding the troll’, i.e. it sucks a user into an endless cycle of irony and ridicule that makes a meaningful exchange impossible. The effect is structural in that it prevents political mobilisation from taking off the ground. By using this tactic of neutralisation-by-trolling, or 'neutrollisation', the trolls' puppet masters (possibly affiliated with the Russian authorities) contaminate the internet, thereby undermining it as a space for political engagement and informed debate. Hence, the regime no longer needs to resort to outright coercion or censorship.

---

[15] Boris Nemtsov, “Manifest svobodnoy Rossii” [Manifesto of Free Russia], *Ekho Moskvy*, June 9, 2012, https://echo.msk.ru/blog/nemtsov_boris/897379-echo/.

[16] Levada Center, Survey on Protests, May 8, 2018, https://www.levada.ru/en/2018/05/08/protests-2/.

[17] Diana Khachatryan,“Kak stat’ troll’hanterom” [How to become a troll-hunter], *Novaya Gazeta*, March 10, 2015, https://www.novayagazeta.ru/articles/2015/03/10/63342-kak-stat-trollhanterom.

[18] Ibid.

[19] Kurowska and Reshetnikov, “Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization”, 355-57.

Out of 60% of the Russian population that use social media, around 80% occasionally encounter information that makes them angry, and around 15% regularly encounter content that is inimical to their views, annoying or objectionable.[20] The overwhelming majority of such users choose to ignore such information instead of blocking it, confronting the posters, or contacting the site administrator.[21] This may appear to be a sensible strategy. Yet such rudimentary statistics do not provide data about the source of such content, how and where in the social media sphere it has been encountered, and what is the history of handling such information by individual users. In other words, while non-engagement is the most frequent reaction to comments and statements posted by trolls, we need further analysis to understand whether this is an informed choice and to what extent this is an effect of 'neutrollisation'.

Trickster diplomacy

Russia applies these methods abroad, too. Pro-Kremlin trolls generate and cultivate a plethora of fake Twitter and Facebook accounts to engineer political disorientation and alienation on the internet outside of Russia.[22] This international strategy mirrors domestic practices of exploiting self-expression on social media. Russia cannot however deploy its 'neutrollisation' tactics on a global scale given its current relations with the West.

It therefore opts for the role of a playful trickster. A trickster can be defined as an actor who is fully embedded within dominant institutions but subverts them by adopting a cynical and derisive attitude towards them.[23] A trickster does not propose any sustainable alternative to the existing order. It acts instead from within it but undermines and corrupts the system.

The discourse on multipolarity – or of a polycentric world order in Russian diplomacy parlance – is an example of how Western normative grammar can be twisted in this way. Adopted from the neorealist theory of International Relations conceived in US

---

20. Levada Center, Survey on Social Media, May 8, 2018, https://www.levada.ru/en/2018/05/08/social-media/

21. Ibid.

22. Yevgeniya Kotlyar, "Pervoe videointervyu s eks-sotrudnikom amerikanskogo otdela 'fabriki trolley'" [First video-interview with a former employee of the American department of the 'troll factory'], *Dozhd'*,October 26 , 2017, https://tvrain.ru/teleshow/reportazh/oni_sdelali_video_kak_negr_zanimaetsja-448671/; Nicholas Fandos and Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts", *New York Times*, July 31, 2018, https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html.

23. For more on the notion of the trickster as used in mythology, folklore, psychoanalysis and more recently in internet studies, see: https://en.wikipedia.org/wiki/Trickster

academic circles and framed as an alternative to US liberal hegemony,[24] Russia's narrative of a polycentric world projects an image of Russia as a guardian of the global order standing against the double standards applied by the West.[25] Such parodic re-appropriation is common when 'humanitarian intervention' is at stake.[26]

The alleged use of the Responsibility to Protect (R2P) doctrine to justify the intervention in Georgia in 2008 provides a perfect example of how Russia resorts to exactly such cynical tactics to bend and distort the meaning of a norm. Sergey Lavrov, the Russian foreign minister, never invoked the doctrine as such. He explicitly justified the intervention in terms of the responsibility to protect Russian citizens as stipulated in the Russian constitution, in contrast to the liberal notion of the right to protection of any individual regardless of citizenship. He also ironically alluded to R2P as 'the term which is very widely used in the UN when people see some trouble in Africa or in any remote part of other regions.'[27] In his turn, the Russian representative to the UN, Vitaly Churkin, referred to the R2P doctrine to claim that Georgia had failed to carry out its responsibility to protect its citizens in Abkhazia and South Ossetia. His accusation of double standards is worth quoting:

> 'Now it is clear why, for many months, Georgia rejected our urgent proposal that it sign a legally binding document on the non-use of force to settle the South Ossetian conflict … The President of Georgia said that demanding his signature on such a document was absurd, because Georgia does not use force against its own people. Now it appears that it does. How can we not recall the responsibility to protect that we hear so much about in the United Nations?'[28]

Conclusion

The most sinister aspect of 'neutrollisation' is that it ultimately exploits and undercuts national and global citizens' genuine desire for political engagement. But reacting to a troll only creates more chaos, meaning that confrontation is not a viable or effective option. Recognition is relatively straightforward, if not entirely effortless. 'The EU versus Disinformation' campaign[29] and the NATO Strategic Communications Centre of Excellence[30] initiative on educating the public on how to identify trolling is a crucial step forward in this respect. However, the moral panic over trolling and efforts to 'name and shame' Russia for its alleged trolling and hacking activities will likely backfire – because this is exactly the reaction that the trolls are looking for. Seasoned internet users know that the best strategy is to ignore trolls, that is, to consciously refuse to be 'neutrollised' by resisting the constant stream of innuendo and negative messages propagated by trolls. This is the educational function of anti-trolling campaigns. If a reaction is necessary, it should be as laconic and unemotional as possible to minimise the risk of 'feeding the troll' and engendering further provocations.

---

[24] Xymena Kurowska, "Multipolarity as Resistance to Liberal Norms: Russia's Position on Responsibility to Protect," *Conflict, Security & Development*, 14, no. 4 (2014): 489-508.

[25] Sergey Lavrov, "Foreign Minister Sergey Lavrov's Remarks at the 71st Session of the UN General Assembly," September 23, 2016, http://russiaun.ru/en/news/ga_71sl.

[26] Erna Burai, "Parody as Norm Contestation: Russian Normative Justifications in Georgia and Ukraine and their Implications for Global Norms," *Global Society* 30(1): 67–77.

[27] Sergey Lavrov, "Interview to BBC", Moscow, August 9, 2008. For analysis see Anatoly Reshetnikov, "Intervention as Virtue, Obligation and Moral Duty: The Meaning of Russia's Rhetoric on Responsibility During the Georgian and the Crimean Crises", *Russian Politics* 2, no. 2 (June 2017): 155–181.

[28] United Nations Security Council 5952nd meeting, s/pv.5952, New York, August 8, 2008, 5, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/PV.5952.

[29] https://euvsdisinfo.eu/

[30] https://www.stratcomcoe.org/

While relevant, such measures are not sufficient for handling Russia's 'trickster diplomacy' because if Russia engages in such diplomacy, it is a direct result of the existing configuration of the international order. Russia resorts to trolling primarily in response to its stigmatisation by the West and as part of its perceived mission to counter the hegemony of the West. Folk wisdom has it that to pacify a trickster one needs to channel its dexterity into solving common problems which transcend the trickster's grievances. In other words, to 'outsmart' it by making it part of the club. In the current strained climate of Russia-West relations, such an option would quickly be labelled as appeasement, legitimisation of aggression, and/or political naiveté. It would also risk undermining the unity of the Western bloc regarding sanctions against Russia, which is the ultimate goal of the Kremlin. For the time being, the West may therefore be stuck with the challenge of dealing with Russia's 'trickster diplomacy'.

CHAPTER 3

Spotting the bear: credible attribution and Russian operations in cyberspace

Sven Herpig and Thomas Reinhold

How do we know who is behind a cyberattack? What are the tools and techniques that could help to identify the hackers who have conducted a cyber-operation? And why is credible attribution in the case of cyberattacks carried out or masterminded by Russia so challenging? These are the questions which this chapter aims to address in detail. However, before examining the technical, intelligence and geopolitical aspects of attribution, this chapter will first explain what attribution is and why it is important in the domain of cybersecurity

Attribution: what it is and what for?

The term 'attribution' chiefly refers to a concept in international law that describes the process of identifying an attack or operation against a state. It is widely used in debates about the norms and rules of state behaviour and how they apply to cyberspace. Strictly speaking, attribution is usually used in the context of armed attacks and considered as one of the main legal requirements for the right of states to resort to force in self-defence under article 51 of the UN Charter. Any state action that refers to this article has to be justified by the credible identification of the origins of an attack. Only by supplying such evidence, are states deemed to have the 'inherent right of individual or collective self-defence' and can therefore take steps towards an appropriate response to stop these threats. Attribution is also used to convince the state's own government, public, and transnational partner organisations about the origin of a cyberattack. The threshold to convince these parties might be lower than the one required to trigger article 51.

In the case of national attribution policymakers and the executive have to be convinced about the origin of an attack in order to legitimise the use of offensive countermeasures. This form of assessment can rely on all technical, geopolitical and intelligence data that is available. Transnational attribution refers to convincing allies, bilaterally or as a whole (e. g. through NATO), about the validity of the attribution. This is essential in order to obtain political, diplomatic or other kinds of support from allies. It might not be possible to explicitly use or cite certain intelligence and technical data to convince them, as such data may be too highly classified. Naturally, this might limit the credibility of the attribution analysis. Then there is public attribution which refers to convincing the public with the attribution assessment. Having public backing in a democratic country allows the government to choose from a wider range of policy options. Credible public attribution enables the government to take certain steps, such as expelling diplomats or implementing economic sanctions, or at least facilitates such a response. Unlike in the case of transnational attribution (for which purpose allies might partially share sensitive information), most intelligence information and certain technical data cannot be shared with the public due to its classified and highly confidential nature. And this very limitation might undermine the credibility of public attribution.

Attributing a cyber operation

Technical aspects of attribution

From a technical point of view, measures for attribution need to be articulated in at least two dimensions. The first dimension distinguishes between those measures that can be established in the domestic IT systems and networks of a state ('inner scope measures') and those that need to exist or be built up in foreign IT systems ('outer scope measures'). The second dimension is composed of preventive and reactive measures. Preventive measures constantly observe, collect and store data that could be used to identify an attack that is detected or noticed at a later point in time. Reactive measures can be used to 'mark and track down an attacker' during an ongoing operation.

Inner and outer scope measures are both crucial to establishing credible attribution. Therefore, each state would need to have implemented its own set of data-gathering measures and/or allow defenders to trail attackers through their systems. This is clearly a challenge in the realm of international relations. Defining international standards for data-gathering measures, cooperation guidelines, information sharing and known communication channels would go a long way towards addressing this challenge and creating a common process to enable an international response. A first step towards such international cooperation has been made by the Budapest Convention on Cybercrime[1] which became effective in 2004. Its agreements however do not apply to norms of state behaviour like espionage or military cyber activities and its practical aspects still need additional and more simplified cooperation measures. The United Nations had been moving in a similar direction until its group of government experts (UN GGE) failed to reach consensus in 2017.[2] Microsoft's private initiative, the 'Digital Geneva Convention',[3] is currently the most recent development in this area.

---

[1] Council of Europe, Details of Treaty no.185, Convention on Cybercrime, Budapest, November 23, 2001,https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Monitoring and logging

A first and essential preventive approach involves technical measures that monitor access to IT systems, the connections and data transferred between them as well as user-performed operations like creating, editing, copying or deleting files. The level of detail of the collected data and the retention period[4] play a crucial role because in the absence of these elements investigations of attacks may not be pursued effectively. On the other hand, however, these same elements constitute a sensitive area in terms of data privacy. This issue has recently been debated in Germany, when allegedly Russian attackers broke into the Federal Foreign Office and undermined security mechanisms set in place by the secure government network.[5] The data storage is considered sufficient when logged information covers the entire attack within a specific system. This enables the defender to consolidate a detailed timeline about the attacker's actions, what the origin of the attack was, what data has been extracted and to which location the stolen data has been transferred.[6] Additionally, the logged information needs to be stored in a secure and tamperproof way to prevent attackers from erasing their digital footprints.

Computer forensics

When an attack has been detected, there is a range of possible reactive measures that can help in identifying the attacker. Besides analysing the collected data to trace the attacker's operations history, other measures are the search and collection of software or software fragments that attackers have left on the compromised system to perform their unauthorised activities. These tools are often handcrafted and form part of larger toolsets. They are frequently reused for different operations over a period of several years. A software code analysis of these tools can be instrumental in detecting similarities and establishing connections with former incidents. This

---

2. Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?," Blog post, Council on Foreign Relations (CFR), June 29, 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what

3. Brad Smith, "The Need for a Digital Geneva Convention," Microsoft,14 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

4. The retention period for stored information can be a critical aspect because sometimes attackers break into systems and create backdoors but then stay silent over a long period of time. When the attack is carried out, the log files only contain data about the 'strike command' but not necessarily the more significant information about the break-in itself.

5. Dana Heide, „Will der Bund die Cybersicherheit erhöhen, muss er den Datenschutz opfern", *Handelsblatt*, March 14, 2018, http://www.handelsblatt.com/my/politik/deutschland/cybersecurity-will-der-bund-die-cybersicherheit-erhoehen-muss-er-den-datenschutz-opfern/21070060.html?ticket=ST-546642-G2ZE5mIzhcUXbO5Jbvle-ap2

6. This is just an example. Usually log files can contain a lot more data and specific information on tampered data, modified executable files etc.

ranges from the language, geolocation or working hours uncovered by this form of assessment to code fragments and linked IT-infrastructures, such as email addresses and device IPs. This analysis therefore helps to identify familiar tactics and hacking approaches, linking them to known malicious actors.

Passive tracking

Passive tracking gives the defender additional information to potentially identify the attacker. While the attack is still in progress valuable information and evidence can be collected if the defender is able to observe the attacker's operations. This can be achieved by luring the attacker with so-called 'honeypots': systems or flaws that are easy to exploit and therefore will probably be targeted by the attacker. If the attacker takes the bait, the honeypot enables the defender to monitor all of the attacker's actions.[7] A similar approach is the presentation of manipulated documents, relevant data or information that an attacker is potentially looking for and which contain malicious code, specific digital fingerprints or slightly manipulated information that can later be used to identify the data when it resurfaces.[8] These so-called 'beacons' might also send back the IP address of the systems to which they have been transferred, which could reveal the original location of the attacker.

Active tracking

Strong evidence about the origin of an attack can be gathered by tracing back the attacker to the IT system where the connections or the controlling commands for the attack originate. Common attack approaches often use a so-called command and control (C2 or C&C) infrastructure, where specific computers are used to coordinate the attack and collect the stolen data. In order to identify the attacker it is necessary to monitor and gather information about user operations from these specific systems either through hacking them or through international cooperation with the states where the compromised devices are located. The former strategy is known as 'hack-back' or 'active defence' and has drawbacks that need to be considered.[9] These disadvantages are for example misinterpretations and wrongful attribution due to insufficient information, the risks of falling for deliberately created 'false flags' and

---

7. After incidents, detailed information about the tools of the 'defending' side are rarely revealed. Therefore it is difficult to point out a real-world example of honeypot usage. Press reports covering the recent attack against the Federal Foreign Office in Germany however stated that the investigating agencies are aware of the incident and are monitoring the attackers' activities which may be an indication that tools like honeypots or beacons had been used. For more details see "Cyber-Espionage Hits Berlin - The Breach from the East," *Der Spiegel*, March 2018, http://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html.

8. Honeypots can also be installed as a preventive measure but are most effective when tailor-made to a specific attack and its anticipated goals.

9. Thomas Reinhold and Matthias Schulze, „Digitale Gegenangriffe - Eine Analyse der technischen und politischen Implikationen von ‚hack backs'", August 2017, https://cyber-peace.org/wp-content/uploads/2017/08/AP_Schulze_Hackback_08_2017.pdf.

the question whether the attributed system had been used intentionally for the attack or whether it had been exploited.[10] Another approach that enables monitoring an attack but avoids the risks of hack-back is to deliberately become one of the exploited systems that the attacker is using – similar to the honeypot approach.

Assembling the puzzle

All these approaches can help a defender to collect data and information about the tactics, the tools and the different steps of an attack in order to compare them to known capacities of threat actors and the sophistication and methods attested in former incidents.[11] It is important to bear in mind that while each of these individual pieces of information can be a lead to the attacker, they can also be manipulated or crafted to leave misleading tracks which could potentially incriminate a third party. A consolidated and coherent analysis needs data collected through a range of various measures. It is certainly possible to conduct such a technical analysis when time is not a problem.[12] While in certain scenarios, such as espionage operations, attribution of an attack might not be time-sensitive, other instances exist where time is a critical factor – for example if a hack-back needs to be conducted. Moreover, during military conflict, time might be of the essence but thorough technical attribution takes time and needs to be complemented by an analysis of the geopolitical context in which the attack takes place as well as by intelligence findings.

Intelligence aspects of attribution

Obtaining all kinds of intelligence, especially human intelligence and signal intelligence, is crucial to help establish the attribution of cyberattacks. Such intelligence can be gathered through a state's own means or accessed via shared resources by allies. Intelligence can help to attribute one attack or an entire set of attacks in combination with the technical aspects. If for example a technical attribution analysis reveals that certain cyber operations are linked to each other – e. g. because they rely on the same infrastructure – and intelligence can link one of those operations to the perpetrator, an entire campaign of cyberattacks might be unravelled. The indictment filed by the US Special Counsel investigator Robert Mueller for example, in the inquiry into Russian interference in the presidential election, shows that access to email accounts provided the investigators with useful intelligence, enabling them to connect certain dots.[13] Additionally, the public learned that America's National Security Agency is actively tracking various cyber threat actors via signals intelligence tools.[14] In the case of the attack on Sony Pictures Entertainment,[15] it was rumoured that American intelligence agencies had access to the network from which the attack originated and therefore were swiftly able to attribute it to North Korea. More information was revealed about Dutch intelligence services which were tracking the Russian hacking group 'Cozy Bear' at least between 2014 and 2015.[16] Hackers from the domestic Dutch intelligence agency AIVD were able to witness and monitor the launch of cyberattacks against the Democratic National Committee[17] because they had access to the network from which this operation was launched. AIVD also had access to security cameras monitoring the offices from which those attacks were conducted, conveniently allowing them to compare the pictures taken with those of known spies. This operation is likely responsible for the strongest proof of a Russian cyber aggression that has ever been obtained and found its way into the public sphere.

---

[10] A common and slightly overused example is that of a hospital IT system that may have been hacked itself and used by the attacker as a hub to indirectly perform another cyberattack. Any offensive countermeasures that disrupt the hospital's services would impair important primary tasks and could result in injuries to human life.

[11] It is important to point out that although still only a limited number of state actors have sufficient offensive cyber capacities, their number is rising. For example North Korea has developed significant cyber power over the last year with – compared to conventional military armament – few financial resources.

[12] An example is the 2013 Mandiant report "APT1: Exposing One of China's Cyber Espionage Units" which analysed and presented forensically detailed data and evidence about the Chinese state-driven cyber espionage programme about the PLA Unit 61398. See: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[13] United States of America v. Internet Research Agency LLC et al., Case 1:18-cr-00032-DLF, filed on 16 February 16, 2018, https://www.justice.gov/file/1035477/download

Although crucial to solving the challenge, the intelligence component has been the most underrated aspect in the public debate. The reason for that is the classification of intelligence materials and thus their rare exposure to public scrutiny. After the US presidential elections in 2016, the American intelligence community issued a declassified intelligence report[18] that was supposed to convince the public of Russia's guilt. It however achieved almost the opposite effect because – due to declassification – the public report no longer contained any hard proof of Russian intervention. When asked whether they think Russia attempted to meddle in the 2016 presidential elections, 45% of respondents in the US answered either that they do not know or that it is not true.[19] At the end of the day, it is the state's strategic choice how much it discloses about what it knows and how it obtained its intelligence. Therefore, credible attribution is indeed within the realms of possibility. Whether that proof can be presented to international organisations (e.g. UN, NATO) and/or the public or not is a different story as this would likely mean exposure of the intelligence operation. Revealing such an intelligence operation would decrease the likelihood of it still being effective in the future. If attackers follow the counter-response to their actions closely, they might be able to identify what measures were used to track them down and circumvent/avoid them if possible.

---

[14] Kim Zetter, "Leaked Files Show How the NSA Tracks Other Countries' Hackers," *The Intercept*, March 7, 2018, https://theintercept.com/2018/03/06/leaked-files-show-how-nsa-tracks-other-countries-hackers/

[15] Andrea Peterson, "The Sony Pictures hack explained," *Washington Post*, December 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained

[16] Huib Modderkolk, "Dutch Agencies Provide Crucial Intel about Russia's Interference in US Elections," *de Volksrant*, January 25, 2018, https://www.volkskrant.nl/media/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/

[17] Sven Herpig, "Cyber Operations: Defending Political IT-Infrastructures. A comparative problem analysis supported by the Transatlantic Cyber Forum," Stiftung Neue Verantwortung, June 2017, https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_lt-infrastructures-problem_analysis.pdf.

[18] 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," January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[19] IPSOS/REUTERS Poll Data, July 18, 2018, https://www.ipsos.com/sites/default/files/ct/news/documents/2018-07/2018_reuters_tracking_-_russia_7_18_2018.pdf

Geopolitics of attribution

Geopolitics might only play a minor role in the attribution of cyber operations but this dimension should not be disregarded. While a thorough analysis of the technical aspects and solid intelligence can clearly provide hard facts and concrete evidence when it comes to attribution, a geopolitical assessment can help validate the overall process of attribution. A geopolitical assessment ultimately focuses on the attacker's motivation and hinges on two questions: *cui bono*? ('who benefits?') and 'was it a «false flag»[20] operation?'[21] It is rare for an actor to take responsibility for a cyberattack.[22] Even then, the admission has to be vetted and treated with a certain amount of scepticism because it might just be part of a deception strategy. *Cui bono?* asks the question who would directly and most significantly benefit from the attack. Such an analysis can factor in various political aspects, such as ongoing conflicts, current negotiations or recent events. Findings of the technical analysis, such as what documents were stolen and which positions the employees whose computers were breached held in the organisation, add value to an assessment. A major reason why Russia has been blamed for so many attacks in recent years is that it stood to gain from all of them, assuming that Russia's main goals are to destabilise Western democracies and project power partly in an endeavour by the Kremlin to divert attention from the country's own domestic problems. The shortcoming of that assumption in terms of attribution is that it is overly broad and therefore involves the risk that Russia is automatically blamed for most cyberattacks.

The second aspect of a geopolitical assessment, false flag operations,[23] is straightforward because it asks a similar question: who benefits from the cyberattack in a case where another and/or the most obvious actor identified by a *cui bono* assessment will be blamed for the attack? Many of the indicators examined in a technical analysis, such as timestamps, language configurations, comments or hidden pictures in the code, can be easily manipulated to point in a certain direction. Using a geopolitical cover at the same time makes a false flag operation even more effective. A notable example of this was the alleged Russian cyber operation 'Olympic Destroyer' which not only relied on borrowing technical elements from previous North Korean cyber operations but targeted the Winter Olympics in South Korea[24] at a crucial moment in the North Korean-South Korean and American diplomatic relationship. If Russia was indeed behind it, this false flag operation was definitely smart. If North Korea is blamed for the attack, the relationship between the two Koreas would further deteriorate, forcing the United States to devote more of its attention to that part of the world (instead of towards Russia). If Russia is blamed for the attack, it can further its agenda of power projection and at the same time undermine public confidence in attribution in democratic countries.[25] False flag operations add an additional layer of complexity to an already complex phenomenon.

---

[20] An attack which while disguising the real perpetrator creates the impression that a third party is behind it.

[21] A third aspect could be 'for lulz' (for fun). While this kind of motivation has been in sharp decline in the past few years, groups such as Anonymous and LulzSsec have conducted a number of high-profile hacking operations with the apparent goal of ridiculing the victim.

[22] Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, March 11, 2009, https://www.wired.com/2009/03/pro-kremlin-gro/

[23] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks," 2015, https://ccdcoe.org/multimedia/mitigating-risks-arising-false-flag-and-no-flag-cyber-attacks.html

[24] Andy Greenberg, "Russian Hacker False Flags Work - Even After They're Exposed," *Wired*, February 27, 2018, https://www.wired.com/story/russia-false-flag-hacks/

Why it is problematic to point to Russia

Russia has repeatedly been blamed for cyberattacks in the past decade. Every other operation is currently linked to Russia by politicians, the media or IT security companies.[26] Some of the attribution might be correct, some might be wrong. The challenge here is not attribution but *credible attribution*. Credible attribution does not only mean getting the technical, geopolitical and intelligence aspects of attribution right, it also means convincing the target audience.

Whereas attributing the source of an armed attack is possible for missiles or conventional military forces, such attribution is arguably nearly impossible or considered impracticable[27] in the case of attacks carried out via cyberspace as described earlier. Cyberspace offers perfect conditions for attackers to obfuscate their tracks and deceive the defenders and forensics. Attackers could use uninvolved third party IT infrastructure – or could fly to a different country with a 'burner laptop'[28] – to conduct an attack. A targeted victim can only immediately identify the last element of the chain of computers used in the attack but not the origin behind it.[29] Strong empirical attribution would need to identify every device in the attack chain, and gather and analyse available traces to forensically link them to the real origin of the attack. This is a complex task[30] which is challenging even under optimal conditions where every IT system within the described chain contains traces of the attacker and the victim is able to gather these data via international cooperation.[31] Such a task will not work in specific conflict situations where an immediate response is necessary and 'conclusions shortcuts' are dangerous because the ambiguity and incompleteness of the information about a cyberattack raises the risks of misunderstandings, miscalculations, misinterpretations and wrong responses, especially when other means of crisis communication or confidence-building measures between the adversaries are missing. Besides such 'hard facts', prior events have shown that attribution is still ultimately a political decision based on information collated by intelligence and security agencies or influenced by foreign policy interests and considerations[32]. There are only very few instances in which states based a public response, e.g. sanctions, on the findings of an attribution assessment. One of them was the US response to Russia's alleged meddling in the 2016 presidential election campaign.[33]

---

[25] Levi Maxey, "False Flags in Cyberspace: Targeting Public Opinion and Political Will," *The Cipher Brief*, March 6, 2018, https://www.thecipherbrief.com/false-flags-cyberspace-targeting-public-opinion-political-will

[26] See for example the FireEye report from 2014 on the APT28 group; "APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?," https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf as well as the CrowdStrike report from 2016 "Who Is COZY BEAR?," September 19, 2016, https://www.crowdstrike.com/blog/who-is-cozy-bear/

[27] See the conclusions of the UNIDIR report of the International Security Cyber Issues Workshop Series, 2016, http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

[28] A device which is only used for a particular attack and then trashed to hinder attribution. Derived from the concept of a 'burner phone'.

[29] An attack might have several 'origins', which are intermediate systems exploited by the attacker to make an uninvolved third party look like the adversary. The 'real origin' of an attack is the point where the attack was started by the aggressor.

[30] Two case studies that show the complexity of this task, the different sources that have to be taken into account, the technical difficulties and challenges of tying this information together are the final report of Ralph Langner on Stuxnet, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", The Langner Group, November 2013, https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, as well as the 2013 Mandiant report "APT1 - Exposing One of China's Cyber Espionage Units,"https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[31] A good example of the complexity of this task is given in Ralph Langner's analysis of the Stuxnet incident. See Ralph Langner, "To Kill a Centrifuge".

Additionally, states that are blamed for an attack often distance themselves from the hacking group that conducted the operation and deny any official involvement or control of the group. Even though the UN GGE decided to hold states accountable for cyber operations conducted from within their territory,[34] pledging to help the investigation with any means possible will take some pressure off a state that finds itself under suspicion. Plus, linking a cyberattack to a hacker group is one thing, linking that hacker group or a specific incident to a state and especially to a particular governmental or military order as is required by the UN Charter is quite another. Even if due diligence is a commonly accepted principle in cyberspace,[35] it is not enforced in the current public debates on potential cyberattacks from Russia. In fact, prior to the establishment of a military cyber unit in 2017, the Federal Security Service (FSB) was responsible for overseeing Russia's cyber capabilities.

From the perspective of the international community and as described earlier in respect to international law, attribution and accusations in specific conflicts need to be based on a credible, evidence-based argumentation that has to be made by the affected state. But so far few cases exist where such evidence that points strongly to Russia had been made public. Two instances which provided the most public information about a state-backed attribution pointing towards Russia are the US Director of National Intelligence's report[36] and the Dutch domestic intelligence AIVD findings.[37] In yet another milestone development, several countries – among them the US, the Netherlands and the UK – simultaneously went public in October 2018, jointly attributing cyber operations to the (allegedly) Russian-sponsored GRU hacking unit APT28. The attribution included cyber operations carried out against the World Anti-Doping Agency (WADA) and the Organisation for the Prohibition of Chemical Weapons (OPCW). Enabling states to conduct more severe responses to cyberattacks would require public and international attribution. This in turn leads to a Catch-22 situation in intelligence sharing. Pointing the finger at the usual suspect without credible attribution when a cyberattack occurs not only further emboldens Russia in its projection of power (while it continues to deny responsibility) but fails to sufficiently convince the public or the international community.

---

[32] For instance the hacking attacks against German governmental and parliamentary IT systems from 2015 and 2018 yielded no official reaction against the suggested attackers, whereas a hacking attack against the US-based company Sony Pictures Entertainment from 2014 almost immediately (in terms of days) resulted in US sanctions against North Korea.

[33] David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html

[34] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

[35] Annegret Bendiek, „Sorgfaltsverantwortung im Cyberraum - Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik", SWP Berlin, 2016.

[36] 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," January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf

[37] Huib Modderkolk, "Dutch Agencies Provide Crucial Intel..."

This pattern of accusation and denial underlines again the necessity for binding international rules of state behaviour in cyberspace that include a commitment to the validity of due diligence principles in this domain. This would provide a strong basis for enforceable regimes of international law in cyberspace.

CHAPTER 4

Russia’s cyber diplomacy

Elena Chernenko

Russia has been concerned about the misuse of cyber tools for political, military and criminal purposes for at least the past two decades. This chapter provides an overview of what Russia has tried to achieve internationally with regard to cyber regulations and explains why it has failed in this endeavour so far. It first explores Russia’s early cyber diplomacy initiatives and the motivations behind them. The second part provides a detailed analysis of Russia’s diplomatic efforts in the cyber field at the global, regional and bilateral levels. The chapter concludes by outlining the future orientation of Russia’s cyber diplomacy and anticipating challenges which might lie ahead.

The early days of Russian cyber diplomacy

The history of Russia’s diplomatic engagements concerning the impact of information and communications technology (ICT) on international stability shows that the stated goal of Moscow’s initiatives was from the beginning to prevent conflicts and a cyber arms race between states.[1] Russia put the issue of interference in countries’ internal affairs on the international political agenda by pointing to such risks as early as in 1998 when Moscow introduced the first resolution on ‘Developments in the Field of Information and Telecommunications in the Context of International Security’ in the United Nations General Assembly (UNGA).[2]

The document, which was adopted without a vote, expressed concern that new technologies and means ‘can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States.’[3] To make the resolution acceptable for most countries, the authors stressed the need to prevent the misuse of information

---

1. Elena Chernenko, “Cold War 2.0? Cyberspace as the New Arena for Confrontation”, Russia in Global Affairs, 1, April 15, 2013, http://eng.globalaffairs.ru/number/Cold-War-20-15929
2. UN General Assembly, Resolution A/RES/53/70, “Developments in the field of information and telecommunications in the context of international security,” January 4, 1999, http://undocs.org/A/RES/53/70
3. Ibid.

resources and technologies 'for criminal or terrorist purposes.'[4] In his statements, the Russian foreign minister Igor Ivanov went further and called for another threat to be addressed – that of the militarisation of cyberspace, stressing the potentially devastating effects of cyber weapons.[5]

In 1999 Russia introduced a similar resolution but added two points that were important for Moscow: namely, that cyberspace may be misused for military purposes and that the international community should come up with principles on how to mitigate such dangers. But at this point the level of cyber connectivity and vulnerability of states was much lower[6] compared to the situation prevailing today (in December 1999 there were 248 million internet users worldwide, by December 2017 this number had surpassed 4 billion) and the acuteness of emerging threats was not as evident or at least not officially recognised by all countries. However, Russia's diplomatic efforts paid off when in 2009 the United Nations General Assembly adopted another landmark resolution on 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'.[7] But since UNGA resolutions have no binding power this track – although important as a geopolitical barometer – did not yield any practical results.

Cyber diplomacy in the UN

A more promising approach – from Moscow's point of view – was the launch of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) in 2004. Russia (which along with the US was one of the main participants in the group) was hoping that the efforts of this body would lead to the adoption of some kind of rules of behaviour for states in cyberspace.[8] The prevention of the militarisation of this domain was not a realistic goal anymore since all major cyber players (including Russia) were actively developing these kinds of potentials.[9] So Moscow started acting according to the principle 'if you can't prevent it, try to regulate it'.

---

[4] Ibid.

[5] Elena Chernenko, «Политическая кибервойна началась» ["The Political Cyber War has Started"], *Global Affairs Journal* (9 October 2016), http://globalaffairs.ru/global-processes/Politicheskaya-kibervoina-nachalas-18415

[6] "Internet Growth Statistics, (1995-2017)", Internet World Stats – Usage and Population Statistics, https://www.internetworldstats.com/emarketing.htm

[7] "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures", Resolution adopted by the General Assembly on 21 December 2009, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

[8] Sergey Boyko, «Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее» ["United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: a look from the past into the future"], *International Affairs Journal*, (August 2016), https://interaffairs.ru/jauthor/material/1718

[9] Kenneth Geers, "Strategic Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), June 2011, https://www.defcon.org/images/defcon-19/dc-19-presentations/Geers/DEFCON-19-Geers-Strategic-Cyber-Security-WP.pdf

But the group did not produce significant results until 2013 when it finally drafted a consensus report which aimed at 'promoting a peaceful, secure, open and cooperative ICT environment' and stated that 'cooperative measures that could enhance stability and security include norms, rules and principles of responsible behaviour by states, voluntary measures to increase transparency, confidence and trust among states and capacity-building measures.'[10] The report for the first time underlined that 'international law, and in particular the Charter of the United Nations, is applicable' in cyberspace and at the same time stated that 'state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'. It also provided for a set of recommendations on voluntary confidence-building and capacity-building measures.

2015 was marked by another achievement that Russian diplomats had long hoped for: the next UN GGE report provided the foundation for an internationally recognised governmental cyber code of conduct. The document included eleven basic depoliticised norms, including a determination that states should not knowingly allow their territory to be used for internationally wrongful cyber acts; should not conduct or knowingly support ICT activities that intentionally damage critical infrastructure; and should seek to prevent the proliferation of malicious technologies and the use of harmful hidden functions.[11]

Moscow hoped to turn this report into a proposal for a new global convention that would be addressed at the UN GA in 2017 but when the group met again in June that year it failed to agree on further steps. Looking ahead, it is unclear if the UN GGE has a future.

Bilateral and regional tracks

Russia accompanied its multilateral cyber diplomacy with efforts to spur cooperation in the cyber field at both regional and bilateral levels. Its allies became countries that were also mostly concerned with the idea of promoting state sovereignty and tighter government control on the internet.

In September 2011 four countries of the Shanghai Cooperation Organisation (SCO) – Russia, China, Tajikistan and Uzbekistan – proposed (also at the UN level) an international code of conduct for information security.[12] Later in the same month Russia also presented to the UN a draft of a Convention on International Information Security. Both documents reflect the development of Russian foreign policy thinking with regard to the cyber domain. While Western countries at that time were only using the term ‘cyber security’, which addresses the need to protect software and hardware as well as user’s information from malicious actors, Russia was promoting another term: ‘international information security’. This concept not only encompasses ‘cyber security’ but also focuses on preventing the misuse of information and communication technologies for political purposes. Both the draft Code of Conduct and the draft Convention of 2011 authored by Russia emphasise the importance of state sovereignty and territoriality in cyberspace. The draft Convention also calls for states to acknowledge that aggressive ‘information warfare’ is ‘a crime against international peace and security’ and urges them to refrain from using information and communication technologies (ICTs) ‘to interfere with the internal affairs’ of other countries.[13] Some of the main threats listed in this document include actions aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a state with the intent of destabilising society. It also goes into detail about how to prevent military conflicts, as well as the use of the internet by terrorist networks and cybercrime, but the effort to promote non-interference in a country’s internal affairs clearly stands out as one of Russia’s main reasons for drafting the paper.

---

[10] UN General Assembly, Resolution A/68/98, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

[11] UN General Assembly, Resolution A/70/174, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[12] UN General Assembly, "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", A/66/359, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

One explanation of such Russian thinking is that the Convention was presented in the midst of a global discussion on what role new technologies – especially social media – played in the wave of popular uprisings that occurred in the Arab countries in 2011, as well as in Iran and some countries in the post-Soviet space before that. A significant number of people who influenced Moscow thinking in the digital domain were convinced that the so-called ‘Arab spring’ and other ‘coloured revolutions’ were inspired and managed from outside and that the internet was one of the tools used to create and foment anti-government sentiment.[14] So the goal was to protect the Russian political system from outside manipulation. For that, stricter national legislation was needed – not as intrusive as China’s but resembling it in some ways. One example is the internet blacklist law (that gives the authorities the right to blacklist and shut down certain websites without a trial) adopted in Russia in 2012.[15] International agreements were also to be strived for – they should legitimise the right of governments to establish rules in their sovereign cyberspace and ideally record on paper the promise of countries not to use the internet to destabilise other regimes and interfere in their affairs.

All members of the Collective Security Treaty Organisation (CSTO) were very much concerned about the same threats and eagerly supported Russian initiatives. During a roundtable discussion in 2013 representatives of the organisation voiced concern that they were losing the 'information war' against 'Western opponents' and agreed on the need for 'instruments of counter-propaganda.'[16] Russian diplomatic efforts within the BRICS group were also quite successful. In 2015, following an initiative by Moscow, BRICS agreed on the establishment of a working group on cooperation in the ICT sphere.[17]

---

[13] Russian Ministry of Foreign Affairs, Convention on International Information Security (Concept), September 22, 2011, http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB

[14] Nikolai Patrushev, “The Color Revolutions Will Not Pass in Russia” [An interview with Komsomolskaya Pravda], December 18, 2012, https://www.kp.ru/daily/26003/2929408/

[15] Federal law of Russian Federation no. 139-FZ, https://rg.ru/2012/07/30/zakon-dok.html

In parallel Moscow started to create a network of bilateral agreements aimed at building confidence and enhancing trust between Russia and its partners. In 2013 Russia signed the first ever bilateral cyber agreement – with the US. This set of agreements focused entirely on the technical aspects of cooperation and avoided the issue of content: it provided for the exchange of information between national Computer Emergency Response Teams (CERTs), and the establishing of instant lines of communication on cyber incidents and channels for information exchanges about incidents between the national Nuclear Risk Reduction Centres.[18] There were hopes in Moscow that this would be an initial step towards a much more far-reaching treaty with the US, but the conflict in Ukraine that erupted in 2014 put such plans on ice. Since 2015 similar bilateral agreements on confidence-building measures and cooperation in cyberspace have also been concluded with China, India, South Africa, Belarus and Cuba.

Russia's goals for cyber diplomacy

Moscow will most probably continue to pursue its goals on a global level – in the UN – as well as on a regional level with like-minded countries, but most actively on a bilateral basis. It is important to mention that Russia has changed or nuanced its position in some respects: Moscow is now publicly acknowledging the importance of the role of other actors in cyberspace – especially business.[19] For example the Russian government strongly supported an initiative by the Nornickel group of companies to create an international information security charter for critical industrial facilities.

One of the key objectives for President Putin will be the normalisation of the relationship with the United States. In 2017 Moscow proposed to Washington to sign a bilateral agreement on the prevention of dangerous military activities in cyberspace, similar to the US-Soviet Incidents at Sea Agreement of 1972.[20] The response from the US side has so far been mixed – Washington initially agreed to consultations but then suddenly postponed them just a day before they were about to start at the end of February 2018 in Geneva. One reason for this hesitant position

---

16. CSTO summary of the round table of December 19, 2013, http://www.odkb-csto.org/presscenter/detail.php?ELEMENT_ID=3132

17. Declaration of Ufa, (Ufa, Russian Federation), *VII BRICS Summit*, July 9, 2015, http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf

18. Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security", *Washington Post*, June 17, 2013, https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.

19. Andrey Krutskhikh, Interview in *Kommersant*, April 23, 2018, https://www.kommersant.ru/doc/3611689

20. Ibid.

might be the ongoing investigations in the US about possible Russian meddling in the 2016 presidential elections. In this regard it is noteworthy that in 2017 Moscow also proposed to Washington to sign an agreement on non-interference in each other's political affairs. But the US administration declined to follow up on this initiative.[21] The US ambassador to Moscow, John Huntsman, indicated in March 2018 that Washington might be willing to come back to the idea of consultations on cyber issues with Moscow – provided there is no interference in the November elections.[22] But Russian officials vehemently deny the notion that Moscow ever meddled in US internal politics and thus are unwilling to even discuss the idea of giving one-sided guarantees of future non-interference.

At the same time, Russia is keen to pursue consultations on possible bilateral agreements in cyberspace with Germany, France, Israel, Japan and South Korea. This list of countries is mentioned in an internal document of the Russian Security Council.[23] But given the differences of approach to cybersecurity and accusations of Russian meddling in internal political processes in several of the above-mentioned countries, it is unlikely that the negotiations will yield any quick results. Berlin already cancelled one round of planned consultations, claiming that the Russian government is behind a hacker group called 'Snake' that organised a cyberattack on the German ministry of foreign affairs. Russian officials deny this.[24]

Russia also hopes to rally support for an UNGA resolution by calling for the GGE to be reconvened in 2019. In this matter it especially counts on countries that are members of the CSTO, the SCO and BRICS, and they have voiced preliminary support for Moscow's position.[25]The continued and strengthened cooperation on cyber issues with regional organisations – CSTO, SCO, BRICS and the Organisation for Security and Cooperation in Europe (OSCE) – also remains high on the agenda of Russia's cyber diplomacy.

Finally, Russia is also the key actor behind a new convention on countering cybercrime that was presented to the UN two years ago. Russia is not party to the Budapest Convention on Cybercrime of the Council of Europe (mainly because its paragraph 32 allows trans-border access to publicly available stored computer data during cybercrime investigations without prior authorisation).[26] The message from Moscow is clear: either the Budapest Convention is adapted (paragraph 32 should be amended

---

21. John Hudson, "How Secret Talks With Russia To Prevent Election Meddling Collapsed", *BuzzFeed*, December 8, 2017, https://www.buzzfeednews.com/article/johnhudson/no-deal-how-secret-talks-with-russia-to-prevent-election#.worZ08JedJ

22. An interview with Ambassador John Huntsman. *Kommersant*, March 26, 2018, https://www.kommersant.ru/doc/3585482

23. Elena Chernenko, "Russia Is Installing Anti-hacker Programmes", *Kommersant*, November 30, 2017, https://www.kommersant.ru/doc/3481987

24. Readout of the joint press-conference of head of Russian MFA Sergey Lavrov and the German minister of foreign affairs Heiko Maas from the 10th of May 2018, May 10, 2018, http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3213546

25. Elena Chernenko and Mikhail Korostikov, "Russia Enters the internet Through the UN", *Kommersant*, July 2, 2018, https://www.kommersant.ru/doc/3674882

26. Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561; Keir Giles, "Russia's Public Stance on Cyberspace Issues", Proceedings of 2012 4th International Conference on Cyber Conflict, Tallinn, 2012, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf

to specify a voluntary form of cooperation but not a binding one) to attract more signatories (right now 55 countries have signed and ratified it), or a new treaty needs to be adopted. The second option would be preferable for Russia. In 2017 Moscow already presented an alternative document to replace the Budapest Convention.[27]

Russia's cyber diplomacy – a double-edged sword

The approach adopted by the government of Russia – but also the evolving nature of the risks emanating from the cyber domain – have had two major effects.

For quite a long time the dividing lines between different countries were clearly demarcated. Russia and its closest partners (China, members of the CSTO) were promoting the need for global rules of behaviour for governments in cyberspace stressing especially such principles as the sovereignty of states and non-interference in a country's internal affairs. The US and their allies were very sceptical about these ideas, suspecting that the real motivation behind the other camp's demands is the wish to legalise censorship and expand governmental control of a free domain.[28] But with threats from cyberspace growing (cybercrime, the spreading of terrorist propaganda and hostile acts at state level), more and more Western countries are starting to use similar language calling for more regulation and the right of governments to control information within their jurisdiction. Recently this idea was for the first time publicly endorsed by the UN Secretary General Antonio Guterres, who said that global rules are needed to minimise the impact of electronic warfare on civilians as in his opinion 'the next war will begin with a massive cyberattack to destroy military capacity … and paralyze basic infrastructure such as the electric networks.'[29]

But while we see a growing overlap between Russia and the West in terms of policies and cyber threat perception, the irony of it all is that the negative dynamics in US-Russia and EU-Russia relations make the achievement of any global consensus extremely difficult if not impossible. But without cooperation between the main players – including Russia and the Western countries – no regulatory regime in the cybersphere will be effective.

---

[27] Elena Chernenko, "The Virtual Clash of Super Powers," *Kommersant*, April 14, 2017, https://www.kommersant.ru/doc/3270136

[28] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace", *New York Times*, June 27, 2009, https://www.nytimes.com/2009/06/28/world/28cyber.html

[29] "UN Chief Calls For Regulatory Scheme For Cyberwarfare," *Radio Free Europe/Radio Liberty*, February 19, 2018, https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html

Case studies of Russian cyberattacks

CHAPTER 5

The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine

Piret Pernik

This chapter traces the background to and evolution of Russia's cyber operations against Estonia, Georgia and Ukraine in 2007-2017. Russia has for long employed traditional coercive tools and tactics in its dealings with neighbouring states – threats to cut off energy supplies, capturing political and business elites, co-opting organised crime, disseminating targeted disinformation and propaganda, and manipulating Russian-speaking minorities abroad.[1] In recent years Russia has begun to deploy coercive tools in the realm of cyberspace and launch low- and high-end cyberattacks and social media disinformation campaigns.[2] In Ukraine Russia seems to have escalated conflict in cyberspace and there is concern that other authoritarian countries who possess cyber and information capabilities may begin to emulate Russia.[3]

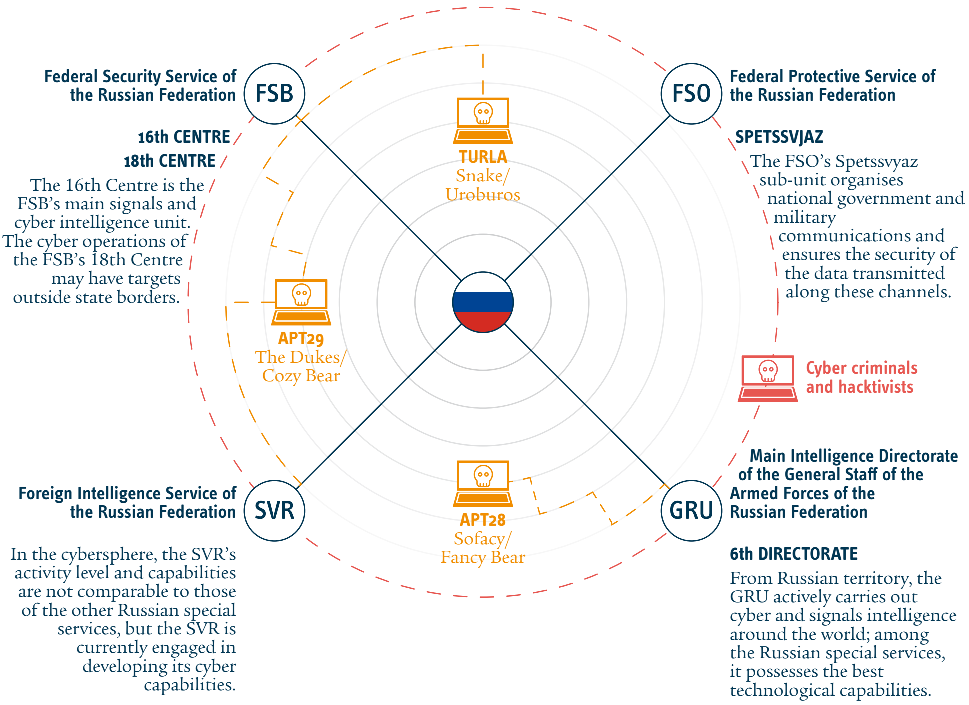
Cyberattacks are difficult to attribute (at least with a high level of confidence) and Moscow has denied the accusations levelled at it on the grounds that countries

---

1. See "Factbox: Russian Oil and Gas as Political Weapon?", *Reuters*, May 2, 2007, https://www.reuters.com/article/us-russia-estonia-energy/factbox-russian-oil-and-gas-as-political-weapon-idUSL0211261020070502; Piret Ehin and Erkki Berg, "Incompatible Identities? Baltic-Russian Relations and the EU as an Arena for International Conflict," in *Identity and Foreign Policy: Baltic-Russian Relations and European Integration*, ed. Piret Ehin and Erkki Berg (Routledge, 2016). For disinformation, propaganda, and the manipulation of Russian-speaking minorities in the Baltic States, see for example, Estonian Foreign Intelligence Service, *International Security and Estonia 2017*, 16-21, https://www.valisluureamet.ee/pdf/EIB_public_report_Feb_2017.pdf; Estonian Internal Security Service, *Annual Review 2007*, 8, https://www.kapo.ee/en/content/annual-reviews.html. For capturing elites and co-opting organised crime in European countries, see Mark Galeotti, "Controlling Chaos: How Russia Manages its Political War in Europe," European Council on Foreign Relations (ECFR), September 1, 2017.
2. Stephen Blank, a senior fellow for Russia at the American Foreign Policy Council, argues that Russia used cyberattacks against Georgia and Ukraine as coercive tools to compel them to take account of Russian interests. Stephen Blank, "Cyber War and Information War *à la Russe*," in *Understanding Cyber Conflict: 14 Analogies,* ed. George Perkovich and Ariel Levite (Washington, D.C: Georgetown University Press, 2017), https://carnegieendowment.org/2017/10/16/understanding-cyber-conflict-14-analogies-pub-72689; For Russia's cyberattacks and disinformation campaigns against European and North American countries see for example "Moscow is Regaining Sway in the Balkans", *The Economist*, February 25, 2017.
3. For instance, Vietnam takes China as a model in developing state censorship including setting up a military unit of internet commentators similar to the Chinese 50 Cent Party. John Reed, "Vietnam army reveals 10,000-strong cyber warfare unit," *Financial Times*, December 26, 2017; David Bond, "More countries are learning from Russia's cyber tactics," March 15, 2018.

who have attributed cyberattacks to Russia have not presented enough evidence to support their claims. The EU and NATO have not drawn ‘red lines’ in cyberspace and Russia exploits this ‘strategic ambiguity’ by operating under the threshold of what would be considered the use of force. Russia is also adept at taking advantage of the ambiguity pertaining to the application of international law to cyberspace and the lack of enforcement of voluntary non-binding norms of responsible state behaviour in this domain.[4]

FIGURE 1 | Russian cyber espionage/attack actors


Federal Security Service of the Russian Federation
FSB
16th CENTRE
18th CENTRE
TURLA
Snake/ Uroburos
FSO
Federal Protective Service of the Russian Federation
SPETSSVJAZ
APT29
The Dukes/ Cozy Bear
Cyber criminals and hacktivists
Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation
GRU
Foreign Intelligence Service of the Russian Federation
SVR
APT28
Sofacy/ Fancy Bear
6th DIRECTORATE

The 16th Centre is the FSB’s main signals and cyber intelligence unit. The cyber operations of the FSB’s 18th Centre may have targets outside state borders.

The FSO’s Spetssvyaz sub-unit organises national government and military communications and ensures the security of the data transmitted along these channels.

In the cybersphere, the SVR’s activity level and capabilities are not comparable to those of the other Russian special services, but the SVR is currently engaged in developing its cyber capabilities.

From Russian territory, the GRU actively carries out cyber and signals intelligence around the world; among the Russian special services, it possesses the best technological capabilities.

Data: Estonian Foreign Intelligence Service, 2018.

Cyberattack against Estonia (2007)

Throughout the 1990s and 2000s the Kremlin attempted to manipulate interpretations of history in the Baltic States (e.g. maintaining that the Baltic States voluntarily joined the USSR in 1940). Already in 2005, following an episode where several World War II memorials in the country were vandalised, Russia accused Estonia of rewriting history, and even of ‘rehabilitating fascism’ and glorifying Nazism. The 2007 cyberattacks must be seen as part of this broader fight between Moscow and Eastern and Central European countries over war monuments, in this specific instance 'the Bronze Soldier crisis'. On 26 April 2007 the Estonian government began preparations to relocate this Soviet World War II memorial from the centre of Tallinn to a military cemetery.[5] Unrest and riots involving Russian-speaking youths ensued in Tallinn and Ida-Viru County.[6] Russian State Duma members threatened to sever diplomatic relations with Estonia and called on the Estonian government to step down. Russia introduced restrictions on Estonian exports, Russian companies suspended contracts with Estonian firms, Russian rail and port freight transit via Estonia was reduced sharply, and train connections between Estonian and Russia were suspended.[7] The members of Nashi, a pro-Kremlin youth group, physically attacked the Estonian ambassador and besieged the embassy facilities in Moscow. Russian information channels went into full-on disinformation mode.[8] In addition mobile phone text messages were utilised for spreading disinformation, exhorting the Estonian population to take up armed resistance against the government.[9] Russian-language social media platforms and websites called upon volunteers to launch cyberattacks against Estonian political parties and government websites, as well as providing lists of targets, instructions and attack tools.[10]

---

[4] Robert McLaughlin and Michael Schmitt, “The Need for Clarity in International Cyber Law”, *Policy Forum*, September 18, 2017, https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/

Types of cyberattacks: targets, impact, and attribution

In this context, cyberattacks against Estonian state institutions, news portals, political parties, banks and other entities commenced on 27 April, a day after the public protests started, and lasted for a period of three weeks until 18 May. Initially the cyberattacks were rather primitive and unsophisticated, mainly consisting of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, website defacements, email spamming and posting of automated comments. However, on 30 April coordinated and sophisticated cyberattacks targeted Estonian critical information infrastructure such as Domain Name Servers (DNS), international routers and the network nodes of telecommunications companies, including the largest service provider Elion, as well as the state data communication network. The firewalls and servers of public institutions were targeted as well.[11] The most serious attacks were launched on 9-15 May against state institutions, telecommunications companies, and the country's two largest banks (Hansapank and SEB Eesti Ühispank).

---

[5] "Russia's Involvement in the Tallinn Disturbances," International Centre for Defence and Security, May 11, 2007, https://icds.ee/russias-involvement-in-the-tallinn-disturbances/; for a detailed timeline see "Monument of Contention: How the Bronze Soldier was Removed," err.news, https://news.err.ee/592070/monument-of-contention-how-the-bronze-soldier-was-removed.

[6] Piret Ehin and Erkki Berg, "Incompatible Identities? "

[7] Compared to 2006, in 2007 Estonian port transit decreased by 15%, and rail transit by 25%. 80-90% of transit comes from Russia. *Quarterly Bulletin of Statistics Estonia* 2/11, "Statistics Estonia": 91-102, http://www.stat.ee/valjaanne-2011_eesti-statistika-kvartalikiri-2-11; European Parliament, "European Parliament resolution of 24 May 2007 on Estonia", http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0215&language=EN&ring=B6-2007-0220

[8] For example RTR and Komsomolskaja Pravda spread propaganda. See Estonian Internal Security Service, *Annual Review 2007*, 8. For examples of Russian propaganda in the internet see Heiki Pääbo,"War of Memories: Explaining 'Memorials War' in Estonia," *Baltic Security & Defence Review* 10 (2008): 22.

[9] European Parliament, "European Parliament resolution of 24 May 2007 on Estonia".

[10] Tarmo Ranel, "CERT Eesti tegevuse aastakokkuvõte 2007", Estonian Information System Authority, https://www.ria.ee/public/CERT/CERT_2007_aastakokkuv6te.pdf. The Estonian authorities charged an IT student, Dmitri Galushkevich. In addition, Konstantin Goloskokov, a member of the pro-Kremlin Russian youth group Nashi, and Sergei Markov, a State Duma deputy, admitted responsibility for launching cyberattacks.

The attacks primarily affected banking and communications infrastructure: online banking services were inaccessible for all users over a period of two days for up to two hours at a time (and later functioned only partially), in parts of the country DNS services were offline, and three mobile communications operators experienced disruption. As part of an effort to limit the damage caused by the cyberattack, international internet traffic was blocked and users outside Estonia were not able to access online banking and Estonian media and government websites for longer than users in Estonia.[12] The government's ability to communicate effectively and in real time with the media was impaired because its online briefing room was shut down. People were not able to obtain information from websites and email communication with government officials was affected due to the large quantity of spam emails. However, these disruptions were short-lived and did not significantly affect the provision of the government's communication services. The major inconvenience experienced by ordinary people was their inability to access online banking services, while users outside Estonia were unable to use other e-services because the state portal was inaccessible to them.

The Estonian ministry of defence working group that compiled lessons learned from the 2007 cyberattacks suggested that the negative impact of the cyberattacks was marginal mainly because Estonian first responders were able to mitigate the attacks, increase network and server capacity, and take other response measures swiftly and effectively. Had the response not been so professional and efficient, there would have been 'a critical impact on infrastructure'.[13] The financial damage caused by the cyberattack, including the additional costs induced by remedial measures undertaken in the public sector, amounted to about six and a half million Estonian kroons (approximately €415,000). Hansapank's cybersecurity expert estimated at the time that costs incurred by the biggest bank in Estonia could range from ten million to a billion Estonian kroons (approximately €640,000 to €6.5 million).[14]

Regarding the attribution of responsibility for the cyberattacks, foreign cybersecurity experts who investigated the 2007 events in Estonia agreed that they were carried out by voluntary or 'patriotic' non-state hackers who sympathised with the Russian government's views.[15] According to officials from the Estonian Computer Emergency Response Team (CERT), Russian-language websites called on volunteers to launch cyberattacks targeting Estonian websites weeks before the start of the cyberattacks that were originally planned for 9 May when Russia celebrates Victory Day.[16] Another cybersecurity expert noted that 'preparations for an online attack' started 'in the days leading up to the attack.'[17] However, according to Stephen Blank, sources in the Estonian government told him that the planning of street demonstrations and cyberattacks began already in 2006.[18] While there is no evidence to support the latter viewpoint, the fact that relatively sophisticated cyberattacks targeted key nodes of critical information infrastructure indicates that some reconnaissance activities were carried out in advance.

---

[11] The volume of the strongest DDoS attacks was approximately 4-5 Mpps (million packets per second). In comparison, in September 2016 the volume of DDoS attacks launched by the Mirai botnet (which was composed primarily of embedded and IoT devices) exceeded 600 Gbps (billion bits per second). See: https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46301.pdf.

[12] Patrick O'Neill, "The cyberattack that changed the world," *The Daily Dot*, May 20, 2016, https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/.

[13] "Küberrünnete ja küberkaitsealane koondanalüüs" [Comprehensive Analysis of Cyberattacks and Cyber Defence], Estonian Ministry of Defence, Tallinn, 2007.

[14] Kärt Anvelt, "Täismahus: Jaan Priisalu: küberrünnakutest sai Hansapank kahju kuni miljard krooni" [To the full extent: Jaan Priisalu: Cyberattack inflicted loss of up to a billion kroons on the Hansapank], *Eesti Päevaleht*, 26 April 2012, http://epl.delfi.ee/news/eesti/taismahus-jaan-priisalu-kuberrunnakutest-sai-hansapank-kahju-kuni-miljard-krooni?id=64309855.

Apart from the lack of conclusive technical evidence there was little doubt in the eyes of Estonians that the objectives of the cyber campaign aligned with the interests of the Russian government. Several Estonian politicians, for example Urmas Paet, the minister of foreign affairs, said that IP-addresses used for launching the cyberattacks belonged to the Russian government and government officials, including the President's administration.[19] Moreover, only a well-resourced organised crime group or a state actor would have been in a position to identify key targets, and rent sufficiently large botnets to sustain the volume of cyberattacks over such a long period. The Russian authorities implicitly supported the perpetrators because they declined to cooperate on legal issues with Estonian authorities investigating the attacks. This indicates that it was not in the interest of the Russian government to stop the cyberattacks and to punish the perpetrators.

Changing perceptions of the 2007 cyberattacks

Given the evolution of Russia's more aggressive cyber espionage and increasingly devastating cyberattacks in the intervening decade, perceptions of the 2007 cyberattacks have changed. It has become a widely-shared view among security experts that Russia is waging a political war aimed at undermining the legitimacy of democratic institutions in liberal democratic countries.[20] Accordingly, the 2007 cyberattacks are interpreted by Russian foreign policy analysts and cyber experts as an example of Russia's coercion employed together with diplomatic, economic, information and other tools.[21] At the time of the incident, the international media speculated that the attacks were carried out by unorganised non-state actors, who acted spontaneously motivated by nationalism, and that they were not directly supported by the Kremlin. At the same time, several Estonian politicians tried to frame the cyberattacks as a military or existential threat from the very beginning, describing them as 'cyber war', 'cyberterrorism' and even invoking 'World War III.'[22]

---

[15] Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (Winter/Spring 2008): 122–23, https://ht.transparencytoolkit.org/FileServer/FileServer/whitepapers/botnet/Battling%20Botnets.pdf; See discussion about the involvement of the Russian government in Andreas Schmidt, "The Estonian Cyberattacks", in ed. Jason Healey, *The Fierce Domain - Conflicts in Cyberspace 1986-2012*, Atlantic Council, 2013, 19-20.

[16] Andreas Schmidt, "The Estonian Cyberattacks", in ed. Jason Healey, *The Fierce Domain - Conflicts in Cyberspace 1986-2012*, Atlantic Council, 2013, 6.

[17] Gadi Evron, 'Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War'.

[18] Stephen Blank, "Cyber War and Information War *à la Russe*", http://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

[19] Välisministri avaldus, May 1, 2007, https://www.valitsus.ee/et/uudised/valisministri-avaldus

[20] Political war can be understood as a foreign policy strategy that deploys a mix of traditional and covert instruments of influence (diplomacy, economic measures, intelligence operations, military pressure, organised crime, etc.). Other scholars use the notions of hybrid, non-linear, new generation, asymmetric, non-kinetic, etc. warfare.

The 'Bronze Soldier crisis' highlighted the cognitive dimension of cyberattacks, i.e. the way in which cyberattacks can impact perceptions, induce emotions, and potentially even change opinions and behaviour. It is widely recognised today, including by some militaries, that cyberattacks can have a far-reaching psychological impact, in particular when employed in support of information operations.[23] In 2007 Jaak Aaviksoo, the Estonian minister of defence, said that the aim of the cyberattacks was to 'destabilise Estonian society, creating anxiety among people that nothing is functioning, the services are not operable. This was clearly psychological terror in a way.'[24] Indeed, the psychological effects on Estonian decision-makers and the population at large can be considered as the most significant consequence of the 2007 cyberattacks. A senior official, a member of the government's crisis management committee who discussed the situation at an extraordinary meeting, has recalled that the committee was uncertain about the potential impact that the ongoing cyberattacks would have not only on key infrastructure but also on Estonia's international reputation as a global leader in the development of e-government and the digital society. Had the cyberattacks disabled the provision of vital services on a large scale, public trust in the government and digital infrastructure would have been seriously compromised.[25]

---

[21] Russia's actions in Estonia in 2007 are seen as part of its long-term attempt to preserve influence in its near abroad. See for example Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CAN Corporation, March 2017, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf. Jason Healey and Michelle Cantos write that "The Russian cyber assault on Estonia in 2007 was a blueprint for a geopolitically inspired and just-deniable-enough digital disruption." Jason Healy and Michelle Cantos, "What's Next for Putin in Ukraine: Cyber Escalation?" in *Cyber War in Perspective: Russian Aggression against Ukraine,* ed. Kenneth Geers (Tallinn: NATO CCD COE, 2015.)

[22] Jaak Aaviksoo, "Tähelepanuta jäänud III maailmasõda," *Eesti Päevaleht*, 18 June 2007, http://epl.delfi.ee/news/arvamus/jaak-aaviksoo-tahelepanuta-jaanud-iii-maailmasoda?id=51091172.

[23] According to the US Joint Doctrine cyberspace operations create effects in the information environment. Joint Publication 3-12, "Cyberspace Operations," 8 June 2018, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930. Cyberattacks against Estonia in 2007 can be considered as 'cyber influence attacks' with the aim of influencing decision-making or public opinion. See Pascal Brangetto and Matthijs Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations", in *8th International Conference on Cyber Conflict,* ed. N. Pissanidis, H. Rõigas and M. Veenendaal (Tallinn: NATO CCD COE Publications, 2016), 113–26. The cognitive effects of cyber operations are discussed in Larry Welch, "Cyberspace – the Fifth Operational Domain," Institute of Defense Analysis, Research Notes, 2011.

[24] "Looking West – Estonian Minister of Defense Jaak Aaviksoo," *Jane's Intelligence Review*, October 2007.

[25] Interview with Lauri Almann, ICDS, 2013.

Cyberattacks against Georgia (2008)

The attack

Cyberattacks on Georgian websites coincided with the start of the military conflict on 8 August (according to the LEPL Data Exchange Agency the cyberattacks had been planned in advance but started on 9 August).[26] Targets of DDoS attacks included 54 Georgian websites, including about 90% of state institution (gov.ge) websites and a large number of .ge domain addresses. Attack methods included website defacements, mass email spamming and malicious payloads on web applications (SQL injections).[27] Similarly to what happened during the 2007 Estonian cyberattacks Russian-language internet forums (e.g. *StopGeorgia.ru*, *Xakep.ru*) distributed lists of targets, instructions and attack tools. According to the Georgian Computer Emergency Response Team (CERT) the IP addresses and DNS that were used to launch attacks belonged to a Russian organised crime group known as the Russian Business Network (RBN).[28] Several cybersecurity experts maintain that RBN was affiliated with the Russian security services (the group ceased their activities shortly after the cyberattacks conducted in Georgia).[29]

Innovations

Compared to Estonia a year earlier, a new feature was a sophisticated cyber espionage campaign conducted around the time that the military conflict occurred. The campaign was discovered by the Georgian authorities several years later, in March 2011. A malware, *WIN32/Georbot*, collected sensitive and classified information related to national security in the networks of Georgian state institutions, financial and non-governmental organisations. The Georgian authorities attributed the campaign to the Russian security services (and substantiated the allegation with technical evidence which included a web camera screenshot of a person who carried out the campaign).[30] Several cybersecurity experts who analysed technical evidence combined with the overall geopolitical and strategic context, believe that the cyberattacks against Georgia during the military conflict were coordinated with Russian military operations.[31] This indicates that the perpetrators had links to the Russian military or state authorities. Some security experts are of the opinion that the cyberattacks were pre-planned and pre-attack reconnaissance was conducted.[32] The technical report of a cybersecurity company provides evidence for this opinion and attributes the cyberattacks to Russian hackers who have links to the Russian security services.[33]

---

[26] DDoS attacks started on 8 August, but some attacks were also conducted in July, for example, on 19 July the website of the President of Georgia was hit by DDoS attacks. See Eneken Tikk, Kadri Kaska and Liis Vihul, "Georgia 2008", in *International Cyber Incidents: Legal Considerations* (Tallinn: NATO CCD COE, 2010).

[27] Structured query language (SQL) injections are one of the most prevalent and most dangerous web application hacking techniques.

[28] Presentation by Irakli Gvenetadze, LEPL Data Exchange Agency, Garmisch-Partenkirchen, Germany, 12 December 2014.

[29] A report by the US Cyber Consequences Unit implied that DDoS attacks were executed via RBN botnets and servers. Other security experts also identified the use of RBN infrastructure and tools. See John Markoff "Before the Gunfire, Cyberattacks," *New York Times,* August 12, 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html.

[30] LEPL Date Exchange Authority and the Ministry of Justice linked the cyberattacks to "Russian Official Security Agencies". See "Cyber Espionage against Georgian Government. Georbot Botnet," CERT.gov.ge, http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf

[31] Stephen Blank, "Cyber War and Information War *à la Russe*."

Cyber as a tool in military conflict

The 2007 attacks against Estonia led to a paradigm shift denoting the expansion of national security and defence into cyberspace, while the Georgian cyberattacks marked the use of cyberattacks as part of military conflicts. The Georgian cyberattacks facilitated a radical shift in military thinking – for example, Kenneth Geers, a cyber expert, wrote in August 2008 that all political and military conflicts 'now have a cyber dimension'.[34] Many NATO militaries in the late 2000s recognised cyberspace as a military domain, followed by the NATO declaration at the 2016 Warsaw summit. The document states: '[...]we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.'[35]

Russia deployed cyberattacks, disinformation and psychological operations as part of its broader 'information confrontation' approach and as force multipliers for conventional military operations. The activities of various proxies, Russian state media, military, and security services appear to have been coordinated and occasionally even synchronised.

In sum, 15 months after a concerted attempt to undermine Estonian state institutions Russia demonstrated an enhanced ability to outsource cyberattacks to non-state proxies, to effectively coordinate cyber, information and military operations among various actors, and to leverage strategic impact from targeted cyber-espionage operations.[36] Non-kinetic cyber activities supported the achievement of Russia's strategic and military objectives in Georgia.

---

[32] Ibid.

[33] John Leyden, "Russian Spy Agencies Linked to Georgia Cyber-attacks", *The Register*, March 23, 2009, http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/.

[34] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SCMagazine*, August 27, 2008 https://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/554872/

[35] Warsaw Summit Communiqué, NATO, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[36] Piret Pernik, "Hacking for Influence," *ICDS Analysis*, February 18, 2018, https://www.icds.ee/fileadmin/media/IMG/2018/Publications/ICDS_Analysis_Hacking_for_Influence_Piret_Pernik_February_2018.pdf.

Cyberattacks against Ukraine (2014-2017)

First wave

The number of DDoS attacks and website defacements against Ukrainian websites had been increasing since December 2013, but the majority of the cyberattacks were relatively unsophisticated and their impact on digital infrastructure was negligible. In addition to these types of attacks hackers compromised email accounts and broadcast stolen information online, flooded mobile phones with calls and sms messages and sent out mass text messages containing propaganda. Main targets were news portals, media outlets, state institutions, banks and political parties.[37]

The scale of the cyberespionage campaigns in Ukraine was unprecedented. Cybersecurity companies and experts detected malware affiliated to Russian hackers (Snake/Uroburos/Turla, RedOctober, MiniDuke, NetTraveler) in Ukrainian networks that had been active since 2010. In 2017 a cybersecurity company, Palo Alto Networks, discovered another Russian cyberespionage operation in Ukrainian networks – the Gamaredon Group that had been active at least since 2013. Another cybersecurity company discovered the Russian cyberespionage campaign Operation Armageddon which according to them had targeted officials in the Ukrainian military and national security establishment in 2013-15. The Ukrainian security services attributed the cyberespionage to their Russian counterparts.

Escalation: cyberattacks on infrastructure

Apart from cyberattacks against the election infrastructure and the long-term cyber-espionage campaigns, other cyberattacks targeting Ukraine were relatively unsophisticated. This changed in December 2015 when it was first publicly acknowledged that cyberattacks against the energy sector had caused a major power outage. Damaging cyberattacks were carried out also in 2016 against Ukrainian critical infrastructure (the energy sector including the Kyiv power grid, Kyiv airport, and the financial sector including the Treasury, Pension Fund, etc.).[38] It seems likely that these attacks were preplanned as already in May 2014 the destructive malware BlackEnergy 2/3 was delivered to six Ukrainian railway companies and in August 2014 the same malware infected the computer systems of regional state institutions. The Ukrainian security services accused the Russian government of being behind these attacks. The cyberattacks that caused the most extensive economic damage were carried out with NotPetya ransomware/wipeware in June 2017 by Russian military intelligence. These attacks disabled 10% of computers in Ukraine and inflicted financial costs amounting to 0.5% of Ukraine's GDP.[39] Cyberespionage and destructive cyberattacks against the energy and financial sectors required long-term network reconnaissance, were pre-planned and carefully targeted.

---

[37] Glib Pakharenko, "Cyber attacks in the Ukraine: Quantitative Analysis December 2013-March 2014", (Powerpoint presentation, unpublished).

[38] John Leyden, "BlackEnergy Power Plant Hackers Target Ukrainian Banks," *The Register*, December 15, 2016, http://www.theregister.co.uk/2016/12/15/ukraine_banks_apt; "Cyber Operations Tracker," Council on Foreign Relations (CFR), https://www.cfr.org/interactive/cyber-operations#CyberOperations.

Some cyberattacks were attributed to pro-Russian and pro-separatist hacker groups (e.g. CyberBerkut, Cyber Riot Novorossiya, Green Dragon).[40] One of the most serious cyberattacks for which CyberBerkut admitted responsibility compromised the networks of the Ukrainian Central Election Committee (in April and in May 2014). Information in the election infrastructure databases was destroyed and the hackers deleted log files in order to cover their tracks.[41] The attackers also deployed a malware designed to interfere with software that was used to broadcast election results on the Central Election Committee webpage. According to an official of the Ukrainian Computer Emergency Response Team, traces of the Russian Advanced Persistent Threat (APT) 28 (Tsar Team/Sofacy/Sednit/Fancy Bear/Pawn Storm) group were detected in 2014 in the Ukrainian Central Election Committee networks.[42] APT28 has been attributed by the US security services and those of many other countries to Russian military intelligence. *The New York Times*, citing FBI sources, also reported that APT28 was found in hardware on the Ukrainian Central Election Committee servers.[43] This evidence suggests that the Russian security services and/or military were involved in the cyberattacks against Ukrainian election infrastructure in 2014. Exchange of information regarding the election results must have been pre-planned between the hackers and the Russian TV station Channel 1 which again suggests that the Russian government was involved.[44]

Impact

In terms of disruption of Ukrainian communication networks the most effective operations were physical attacks against digital infrastructure by Russian military and special forces during the annexation of Crimea. Russian forces cut data cables, took over servers, confiscated mobile phones and seized local radio and TV towers, as well as the Internet Exchange Point in Crimea, and rerouted internet traffic via Russian network nodes. Russian social media companies blocked access to accounts, webpages, and the blogs of Ukrainian opposition figures. In addition to the physical destruction and disruption of infrastructure and cyberattacks, the Russian military carried out disinformation operations and electronic warfare (EW). They used integrated cyber and electromagnetic capabilities to geo-locate Ukrainian troops and bombarded them and their relatives with demoralising and threatening text messages.[45]

---

[39] NotPetya has been attributed to Russian military intelligence by several countries, including Australia, Canada, New Zealand, the UK, the US and Denmark.

[40] Cybersecurity experts believe that CyberBerkut has links to the Russian security services. For hactivist groups see Nastia Kostyuk, and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?", University of Michigan, July 12, 2017, https://scholar.harvard.edu/files/zhukov/files/kz_idf_v25.pdf.

[41] Oleksii Baranovskyi et al, "(Cyber)Securing Ukrainian Energy Infrastructure," Fundacja im. Kazimierza Pulaskiego, Warsaw 2016.

[42] Nikolai Koval, "Revolution Hacking," in *Cyber War in Perspective: Russian Aggression against Ukraine,* ed. Kenneth Geers (Tallinn: NATO CCD COE, 2015).

[43] Andrew Kramer and Andrew Higgins, "In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking," *New York Times*, August 16 2017, https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html.

[44] The Russian state TV station Channel 1 broadcast the fake graphic, which had clearly been provided by hackers in advance. Andrew Kramer and Andrew Higgins, "In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking," *New York Times*, August 16, 2017.

Russian information operations against Ukraine also took place on an unprecedented scale and according to security experts were successful.[46] There was effective, almost real-time coordination of information operations with military operations, special operations, and diplomatic measures.

In sum, Russian government cyberattacks against Ukraine incurred extensive economic losses for the country, and damage to digital and critical infrastructure; while Russia's integrated deployment of information, cyber and EW capabilities was successful. Compared to Georgia in 2008, in Ukraine Russia demonstrated a more sophisticated approach and an increased emphasis on the need to achieve information superiority.

Conclusion

The cyber-operations campaign conducted by Russia against Estonia in 2007 constituted 'a blueprint for a geopolitically inspired and just-deniable-enough digital disruption.'[47] A comparison of the successive cyberattacks undertaken by Russian hackers against Estonia, Georgia and Ukraine in the period 2007-2017 demonstrates that Russia was able to draw lessons from previous experiences and has over time perfected the use of cyberattacks to support both political warfare and conventional military operations. The Russian military has integrated cyber, EW and information operations capabilities with military operations, and Ukraine was a testing ground for novel approaches. Russia escalated the cyber conflict in Ukraine by conducting destructive cyberattacks against 'supercritical' infrastructure (specifically the energy and finance sectors) and causing large-scale economic damage. Russian cyber-operations capability has evolved during the last decade and now plays a key role in the military operational environment and contributes to increasing its asymmetric capability.

Russian government cyber actors have undermined democratic institutions, caused great economic loss and damaged critical infrastructure in neighbouring countries and in Western Europe and North America. Destructive malware used by Russian

---

[45] Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," International Centre for Defence and Security (ICDS) Report, September 2017.

[46] Vladimir Sazonov et al. (eds.), *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Tartu: NATO Strategic Communication Centre of Excellence, 2016), https://www.stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces-0.

[47] Jason Healy and Michelle Cantos, "What's Next For Putin in Ukraine?"

APTs has been found in the administrative and business networks of the US energy grid.[48] US, UK and Australian intelligence authorities have warned that Russia has infiltrated Western energy, telecommunications and media sectors.[49] Security services caution that the purpose of such infiltration is not merely cyberespionage, but that it is motivated by an intent to activate destructive malware at a time of crisis. Given the way in which Russia escalated cyber conflict in Ukraine in 2015-2017, it is possible that if the present political and information confrontation with the West intensifies, the Russian government would not have any qualms about conducting destructive cyberattacks against the West.

---

[48] E.g. BlackEnergy, Havex, CrashOverride. See James Conca, "Here Are The Clever Means Russia Used To Hack The Energy Industry," *Forbes*, March 28, 2018, https://www.forbes.com/sites/jamesconca/2018/03/28/how-on-earth-did-russia-hack-our-energy-systems/#64fbe87d6104; Andy Greenberg, "Hackers Get Direct Access to US Power Grid Controls," *Wired*, June 9, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems.

[49] "UK Cyber-defence Chief Accuses Russia of Hack Attacks," *BBC News*, November 15, 2017, http://www.bbc.com/news/technology-41997262; "Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices", *US-CERT*, April 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-106A

CHAPTER 6

Russian cyber activities in the EU

Jarno Limnell

In an increasingly digital and interconnected world, in which cyber threats pose a growing danger to the safety and security of EU member state citizens, effectively addressing such threats has become a key priority for the EU. As European Commission President Jean-Claude Juncker pointed out in his 2017 State of the Union address, 'cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks'.[1] Nation-states and non-state actors are currently testing the boundaries of the 'cyber battlefield' while malicious cyber activities are not only occurring more frequently but are also becoming increasingly sophisticated. Resourceful state-sponsored actors must be understood as the most ubiquitous malicious agents in cyberspace. Defending their networks against such attackers is therefore a primary concern for both commercial organisations and governmental institutions.[2] At the same time, nation-states are significantly investing in strengthening their cyber capabilities.[3] As stated in the 2018 Munich Security Report, the past few years have been marked by the emergence of a group of countries with superior cyber-capabilities.[4] And Russia is foremost among them.

This chapter focuses on how Russia employs its cyber capabilities in the EU member states. First, it briefly sketches the evolving cyber threat landscape and the role of cyber in Russia's hybrid operations. The second part explores Russia's malicious cyber activities in the EU. The chapter concludes with some practical recommendations on how to beef up cyber defence capabilities in Europe.

---

[1] European Commission, President Jean-Claude Juncker´s State of the Union address 2017, September 13, 2017, https://ec.europa.eu/commission/sites/beta-political/files/soteu-explained_en.pdf

[2] European Union Agency for Network and Information Security (ENISA), *Threat Landscape Report 2017*, January 2018, 7, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[3] Jarno Limnéll, "The Cyber Arms Race is Accelerating – What are the Consequences?", *Journal of Cyber Policy*, 1, no.1 (2016): 50-60.

[4] Munich Security Conference, *Munich Security Report 2018*, 51, https://www.securityconference.de/en/discussion/munich-security-report/munich-security-report-2018/

The evolving cyber threat landscape

When assessing the EU's security environment it is vital to keep in mind that the current trend in societies and businesses, – as well as in methods of conducting warfare – is a drive towards a convergence between the cyber/virtual world and the physical world. The EU's endeavour to finalise the Digital Single Market and strengthen the EU's digital economy is underpinned by an awareness of this convergence between the virtual and physical spheres. The central role of digital platforms and internet-enabled technologies also implies that in today's world many threats are intertwined and cyber has become a critical component of most hybrid operations. The 2018 Global Risks Report from the World Economic Forum clearly illustrates these growing interconnections between different threats and vulnerabilities.[5] The multifaceted cause-effect relationships between different threats and actors, and their constantly morphing interaction, make operating in the security environment even more challenging.

The complex and 'innovative nature' of today´s threats appears also in hybrid warfare, which 'intentionally blurs the distinction between the times of peace and war',[6] and in which cyber operations are often a key element. This can be explained by the fact that the anonymity that characterises cyber operations sometimes makes it very difficult to locate and identify the adversary and consequently design the appropriate response (for a detailed analysis, see chapter 3 of this volume on the attribution of cyberattacks, pp. 33-42). In addition, ambiguity pertaining to the legal definition of the digital environment in which cyber capabilities are deployed makes the conduct of malicious cyber activities politically less risky for the perpetrators. One of the associated challenges is the practical application of existing international law to cyberspace, which many states have recognised as a principle but still struggle with operationalising. The lack of clarity on this aspect and unwillingness of some countries to move the debate forward results in a situation whereby 'little green bytes' can move freely across borders causing damage equivalent to that wrought by conventional weapons and conflicts.[7] An aspect that complicates cyber-enabled operations further is the involvement of non-state actors which allows governments sanctioning an unlawful act to hide behind a veil of plausible deniability. Several such hacker groups have been linked to cyber operations subsequently attributed to Russia. [8]

---

[5] World Economic Forum, *The Global Risks Report 2018*, 5, https://www.weforum.org/reports/the-global-risks-report-2018

[6] Aapo Cederberg and Pasi Eronen, "How are Societies Defended Against Cyber Threats?", *Strategic Security Analysis*, no. 9, September 2015, https://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats

[7] See e.g. Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCDCOE,2015).

[8] For example the hacker groups described as APT28 (also known as Fancy Bear and Sofacy) and APT29 (also known as Cozy Bear and The Dukes).

Russia’s objectives and information warfare doctrine

Russian theorists and practitioners conceptualise cyber operations within the broader framework of information warfare, a holistic concept that includes computer network operations, electronic warfare, psychological operations and information operations.[9] Russia´s National Security Strategy 2020 states that ‘confrontation in the global information arena’ is now intensifying and that achieving information superiority in cyberspace is Russia´s essential goal.[10] During the Cold War ‘active measures’ or disinformation and malign influence operations, were well-integrated into Soviet policy and involved virtually every element of the Soviet party and state structure. Today´s hybrid operations are simply the continuation of those measures. In this context, as Russia employs all available means to achieve its national and geostrategic objectives,[11] the cyber domain has become one of the primary theatres for Russian military and political operations.

What is undeniably new in Russia’s approach is the reliance on new tools and methods specific to the cyber domain. General Valery Gerasimov – who masterminded Russia’s approach to cyber operations[12] – confirmed some years ago that ‘the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy’.[13] The ‘weaponisation of information’ involves the exploitation of social media in particular to disseminate propaganda and disinformation (including factual distortion and fabricated information) in order to manipulate public opinion and achieve certain political ends.

Russia´s cyber-enabled activities are deployed to further Moscow’s broader geopolitical aspirations: to assert Russia´s claim to ‘great power’ status; to consolidate its dominance over its self-proclaimed sphere of influence; to destabilise and distract the West to such a degree that it cannot counter Russian actions effectively; and to undermine hostile governments and Western power structures such as NATO and the EU.[14] Over the years, Russia has invested steadily in developing its cyber capabilities. The conflict in Ukraine has provided opportunities for Moscow to further refine its cyber and disinformation techniques. Even if it is difficult to ascertain precisely how ‘cyber capable’ a certain state is, Russia is believed to be one of the global leading players in this domain with several high-profile attacks attributed directly to groups linked to the Russian government. For example, the Russian government has been suspected of sponsoring cyberattacks on energy infrastructure throughout Europe, especially in Ukraine and the Baltic States.[15]

---

[9] See e.g. Michael Connell and Sarah Vogler, *Russia´s Approach to Cyber Warfare*, CNA, September 2016, http://www.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf

[10] Security Council of the Russian Federation, *National Security Strategy to 2020*, Moscow 2009, 4.

[11] See “New Cyber Defence Doctrine Approved by Russian Government”, *SC Magazine UK*, January 6, 2017.

[12] Mark Galeoti, “I’m Sorry for Creating the Gerasimov Doctrine,” *Foreign Policy*, March 5, 2018, http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

[13] Valery Gerasimov, “Tsennost Nauki v Predvidenniye,” *Voenno-promyshlenni Kurier*, February 27, 2013.

[14] See e.g. Mark Galeotti, “Controlling Chaos: How Russia Manages Its Political War in Europe,” *Policy Brief*, European Council on Foreign Relations (ECFR), September 1, 2017, https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe

Russia's malicious activities against the EU

The extensive scope of Russia's cyber operations is generally recognised by EU policymakers. The European Parliament in November 2016 adopted a resolution stating that Russia's goal is to distort truths, provoke doubt, divide member states, engineer a strategic split between the European Union and its North American partners, discredit the EU institutions and transatlantic partnerships as well as to undermine and erode 'the European narrative based on democratic values, human rights and the rule of law'.[16] Sir Julian King, European Commissioner for the Security Union, stated openly that 'there is little doubt' that the EU is subject to a sophisticated, carefully orchestrated pro-Russian government-led disinformation campaign in Europe.[17] A report presented by the Estonian Foreign Intelligence Service in 2018 also asserted that the past few years have shown that the cyber threat against the West is growing and that most of the malicious cyber activity originates in Russia.[18] An analysis by the Alliance for Securing Democracy found, for instance, that the Russian government has 'used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004.'[19] Recently the so-called Five Eyes – the intelligence alliance between the US, UK, Canada, New Zealand and Australia – and several EU member states have openly attributed WannaCry and NotPetya malware attacks to Russia.[20]

---

[15] Symantec, "Dragonfly: Western Energy Sector Targeted By Sophisticated Attack Group," October 20, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks; Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-Backed Hackers Target Baltic Energy Networks", *Reuters*, May 11, 2017, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5

[16] European Parliament, "European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against it by Third Parties," 2016/2030(INI), November 23, 2016.

[17] "EU-Kommissar geißelt prorussische Desinformationskampagne", *Zeit online*, January 27, 2018.

[18] Estonian Foreign Intelligence Service, International Security and Estonia 2018, 52. In a similar vein, the Council on Foreign Relations has found that Putin's regime appears intent on using almost any means possible to undermine the democratic institutions and transatlantic alliances that have underwritten peace and prosperity in Europe. See: Committee on Foreign Relations United States Senate, "Putin´s Asymmetric Assault on Democracy in Russia and Europe," January 10, 2018, 8, https://www.gpo.gov/fdsys/pkg/CPRT-115SPRT28110/html/CPRT-115SPRT28110.htm

[19] The countries included Belarus, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Italy, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Norway, Poland, Portugal, Spain, Sweden, Turkey, United Kingdom, Ukraine, and the United States. Oren Dorell, "Alleged Russian Political Meddling Documented in 27 Countries Since 2004," *USA Today*, September 7, 2017, https://eu.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/

[20] Phil Muncaster, "Five Eyes Nations United in Blaming Russia for NotPetya", Info-Security, February 19, 2018, https://www.infosecurity-magazine.com/news/five-eyes-united-blaming-russia/

Attacks against digital societies and infrastructure

In 2017, advanced persistent threats (APTs) of Russian origin received considerable attention in Europe. The German government reportedly suffered a large-scale cyberattack, when the Russian hacking group APT28 placed malware in a government network and infiltrated both the foreign ministry and the defence ministry.[21] Also, to cite just a few examples, Norway, Denmark, the Netherlands and Italy have accused Russia of advanced cyber espionage. For example in Norway, according to the Norwegian security service, democratic institutions, the Police Security Service and the country's Radiation Protection Authority have been targeted.[22] German intelligence officials have accused Russia of hacking the German government's computer networks as well as those of national energy firms.[23] These cyber espionage and hacking activities – targeting governments, political entities and EU institutions in order to extrapolate and collect classified information – suggest that sophisticated cyber espionage and data manipulation operations are being conducted in the EU. The most serious risk emanating from these activities is not so much the theft or loss of digital information but rather the fact that it can be manipulated. Manipulation of such data compromises its integrity – the validity of the information can no longer be trusted. Unreliable, manipulated information could pose a serious challenge to judicious political decision-making as well as to societies in the digital era.

At the same time, it is often forgotten that the internet relies on physical infrastructure in order to function. Approximately 97% of global communications are still transmitted via transoceanic cables. In a single day, these estimated 213 independent cable systems carry $10 trillion worth of financial transfers and vast amounts of data, including phone and video communications, emails and classified diplomatic and military messages.[24] While geopolitical boundaries can be easily and quickly crossed in cyberspace, there are still sovereignty issues tied to the physical cable systems. In sum, undersea cables are vital to digital societies and their importance will increase – also as one method of hybrid influencing.

---

21. "Germany Admits Hackers Infiltrated Federal Ministries, Russian Group Suspected", *DW*, February 28, 2018, https://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517

22. "Norway Blames Russian Hackers for Cyber Attack on Spy Agency, Ministries", *Sydney Morning Herald*, February 4, 2017, https://www.smh.com.au/world/norway-blames-russian-hackers-for-cyber-attack-on-spy-agency-ministries-20170204-gu5hx4.html

23. "Cyber-Espionage Hits Berlin: The Breach from the East", *Der Spiegel*, March 5, 2018, http://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html"German Intelligence Sees Russia Behind Hack of Energy Firms: Media Report", *Reuters*, June 20, 2018, https://www.reuters.com/article/us-germany-cyber-russia/german-intelligence-sees-russia-behind-hack-of-energy-firms-media-report-idUSKBN1JG2X2

24. Rishi Sunak, "Undersea Cables: Indispensable, Insecure", *Policy Exchange*, London 2017, 12-13, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

FIGURE 2 | Submarine telecommunications cables that supply the world's internet

CABLES WORLDWIDE

97%

(approx.) of
global communications
transmitted via cables
beneath the oceans

213

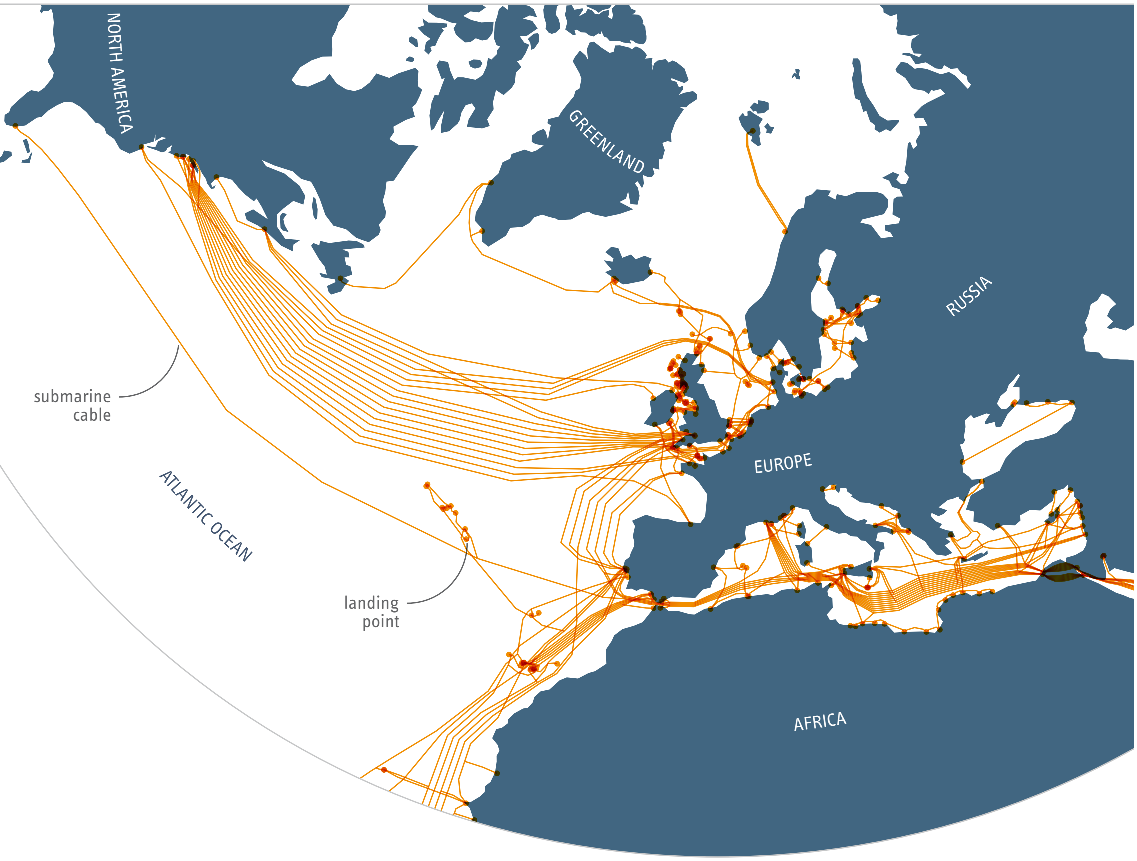
estimated
independent
cable systems

$10

trillion in
financial transfers
per day

CABLES IN AND AROUND EUROPE

schematic


NORTH AMERICA
GREENLAND
RUSSIA
submarine cable
EUROPE
ATLANTIC OCEAN
landing point
AFRICA

Data: policyexchange.org.uk, 2018; European Marine Observation and Data Network, *MODnet Human Activities: Telecom cables (schematic routes)*, 2018.

There has been increasing concern in the West (especially in the US and UK) that Russia may interfere with Western undersea communications infrastructure. Recently NATO decided to re-establish a Cold War-era command post in the North Atlantic as Russian submarines increase activity in the vicinity of undersea cables.[25] At the same time Russia is investing in and enhancing its maritime capabilities. Intensified Russian interest in civilian internet communications infrastructure is one possible indicator of future plans. These activities (damaging and/or tapping cables) can be seen as another manifestation of Russia´s asymmetric 'grey zone operations' – allowing Russia to achieve its objectives from behind a mask of deniability and thus without triggering a strong response.

Attacks against digital democracies

Elections lie at the heart of the democratic political process. They are seen as nothing less than democracy in practice. The risk of cyber-enabled meddling in European elections is real, and, when assessing the hybrid threat, elections have emerged as key targets. The Italian general election this year, the French presidential election in 2017 (for more detailed analysis, see the chapter on 'The Macron leaks' on pp. 73-81 of this volume), the Brexit referendum and US General Election in 2016, to name but a few, have all been subject to influence by malign external agents. It is hard to evaluate precisely how strong or far-reaching an impact these cyber-psychological operations have had, but interfering in European elections is something that should not be tolerated under any circumstances.

The interference in the election campaign in France is a good example of how cyber operations include not just hacking and leaks, but the use of fake news and other forms of manipulation. According to several research findings and reports, the interference originated from Russia.[26] Russia not only denies responsibility for these activities but claims that European countries were meddling in its presidential election.[27] Russian officials have denied hacking France and Germany and have tended to shrug off the wider allegations, with President Vladimir Putin dismissing them as nonsense. Moreover, the Russian government is striking back and saying that 'a new era of information warfare against Russia is upon us.'[28] But Western countries are becoming more vocal in their accusations against Moscow as Russia's cyber interference in European elections shows no signs of abating. Clearly a set of measures to defend digital democracies against disinformation campaigns, hackers and cyberattacks is urgently required.

---

[25] "Facing Russian threat, NATO boosts operations for the first time since the Cold War", *Washington Post*, November 8, 2017.

[26] "Cyber Experts '99% Sure' Russian Hackers are Targeting Macron", *France24*, April 27, 2017.

[27] "Russia Accuses Europe of Meddling in Presidential Election", *Politico*, 15.2.2018, https://www.politico.eu/article/russia-accuses-europe-election-meddling/

[28] "Kremlin Slams 'Russophobic' Allegations that Pin NotPetya Cyber Attack on Russia", *TASS*, February 15, 2018, http://tass.com/politics/990154

What next?

As all the signs are that hostile cyber activities initiated by Russia will continue, it is important that EU countries take the necessary steps to defend themselves against such attacks. The more digitalised societies in the EU become, the more vulnerable they are to targeted attacks of this nature – and the more effective these cyberattacks will be. In addition to increasing cyber defence and societal resilience to confront different forms of cyber hostility, it is important for European countries to reinforce their cyber capabilities in four distinct areas.

Firstly, one defensive strategy is of course the old-fashioned solution, i.e. de-digitalisation; however, states should have recourse to this only where it is absolutely necessary. Elections constitute one area where the use of digital technologies should be reconsidered. For example, even if Finland is one of the most digitalised countries in the world, the Finnish government has recently decided that online voting should not be introduced in general elections as the risks are greater than the benefits.[29] In the Netherlands the Dutch government's approach to dealing with the fear of Russian election hacking has been to abandon electronic vote counting and revert to hand-counted votes, opting for a 'pen and paper' election.[30]

Secondly, the EU´s 'political cyber playbook' is currently still a slim volume that needs to be substantially expanded. In order to counteract Russia´s increasing cyber aggression the EU needs to strengthen its political decision-making process and develop practical tools to respond to these hostile cyber activities. Europe must have a stronger deterrent against cyberattacks. The Russian government will continue its state-sponsored cyberattacks because it perceives that it currently can do so with relative impunity. It is in the EU's interests to develop effective strategies to counter Russia's cyber operations and have the political courage to act against it. The publication of the EU's 'Cyber Diplomacy Toolbox'[31] initiative is a step in the right direction, but active deterrence is also necessary.[32]

Thirdly, the way private sector companies collect and analyse data, create increasingly sophisticated algorithms, develop disruptive technology and build their own global undersea internet cable systems, for example, already reflects their power and influence in today's world.[33] Technology companies should be actively consulted and invited to participate in discussions where the EU is making decisions on cybersecurity. Engaging the private sector is an important step in order to strengthen European cybersecurity.

---

[29] Oikeusministeriö, Nettiäänestyksen edellytykset Suomessa, Mietintöjä ja lausuntoja 60/2017 [Ministry of Justice, Prerequisites for online voting in Finland, reports and statements, no. 60, 2017.]

[30] "Dutch Go Old School against Russian Hacking", *Politico,* May 3, 2017, https://www.politico.eu/article/dutch-election-news-russian-hackers-netherlands/

[31] European Council, "Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions," Press Release, June 19, 2017, http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[32] Jarno Limnéll and Sico van der Meer, "EU Cyber Diplomacy Requires More Commitment", *EUObserver,* July 7, 2017, https://euobserver.com/opinion/138456

Last but not least, if we only prepare ourselves for the cyber-enabled disinformation and influence methods that have been seen and experienced hitherto, we will always be one step behind the attacker. It is vital that European countries are able to both pool and share their experiences of cyberattacks and together to be able to anticipate future cyber threats – and be ready to respond to them.

---

[33] Jarno Limnéll, "Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed," Hybrid CoE, Strategic Analysis, March 2018, https://www.hybridcoe.fi/wp-content/uploads/2018/03/Strategic-Analysis-2018-3-Limnell.pdf

CHAPTER 7

Lessons from the Macron leaks

Jean-Baptiste Jeangène Vilmer

Introduction[1]

In the long list of attempts by foreign entities to interfere in electoral processes in recent years, the 2017 French presidential election will remain the exception that proves the rule. The coordinated attempt to undermine the electoral campaign of candidate Emmanuel Macron succeeded neither in interfering with the outcome of the election nor in swaying French voters and, for this reason, is especially interesting to study. In the second round run-off Macron defeated the far-right candidate, Marine Le Pen.

In using the term 'the Macron leaks', we refer here not only to the release on Friday 5 May 2017 – just two days before the second and final round of the presidential election – of gigabytes of data (including 21,075 emails) that were hacked from Emmanuel Macron's campaign team, but more generally to the orchestrated campaign against him that started months earlier with a series of disinformation operations.

The researcher Mika Aaltola, who used the 2016 US presidential election as a reference case,[2] has identified five distinct stages of election meddling. According to this paradigm, the Macron leaks reached only stage three: there was a disinformation campaign, data hacking, large-scale leaking of e-mails and text documents, but no whitewashing or mainstreaming. What was successfully prevented was 'information laundering,' the process whereby traces of external meddling are 'washed' from the information, stories and narratives manufactured by the hackers.[3]

---

[1] This chapter is a synthesis of a longer report, *The Macron Leaks: A Post-Mortem Analysis*, to be published by the CSIS, Washington, D.C. in the autumn of 2018. A Brief focusing on the lessons learned has already been published: Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks," CSIS, Washington D.C., 21 June 2018.

[2] Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling," *Briefing Paper* 226, Finnish Institute of International Affairs (FIIA), November 2017.

[3] Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case", Center for Strategic & International Studies, *Commentary,* August 31, 2017.

What happened?

An orchestrated disinformation campaign against the presidential candidate had started months earlier: it included the dissemination of rumours, fake news and forged documents, a hacking operation and finally the leak of emails and data at a key moment in the election campaign.

Step 1: Disinformation campaign

It began with rumours and insinuations that intensified in January and February 2017. For example, on 4 February 2017, the Kremlin-affiliated Sputnik news agency published an article presenting Macron as a 'US agent' backed by a 'very wealthy gay lobby.'[4] Some political attacks came also from 'Marine Le Pen's "Foreign Legion" of American Alt-Right Trolls.'[5] Attacks were both political (characterising Macron as an aristocrat who despises the common man, a rich banker, a globalist puppet, a supporter of Islamic extremism and an advocate of uncontrolled immigration, etc.) and personal (including salacious remarks about the age difference between him and his wife, rumours that he was having an affair with his step-daughter, speculation about his sexual orientation, etc.).

Last but not least was the '#MacronGate' rumour spread two hours before the final televised debate between Emmanuel Macron and Marine Le Pen, on Wednesday, 3 May at 7:pm (French time). A user with a Latvian IP address posted two fake documents on the US-based forum *4chan*, suggesting that Macron had a secret offshore account. It was quickly spread by some 7,000 Twitter accounts, mostly pro-Trump, often with the #MacronGate and #MacronCacheCash hashtags. During the live televised debate, Le Pen herself alluded to it. The rumour was quickly debunked and several media sources decisively proved these documents to be fabricated.[6]

Step 2: Data hacking and leaking

Interestingly, the same people who posted the fake documents on *4chan* on Wednesday announced on Friday morning that more were coming.[7] Those responsible for 'MacronGate' thereby provided evidence that they were the same people responsible for the 'Macron leaks' that came out later that day. The hack was performed by phishing attacks. Macron's team confirmed that their party had been targeted since

---

4. "Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests," *Sputnik*, February 4, 2017.
5. Josh Harkinson, "Inside Marine Le Pen's 'Foreign Legion' of American Alt-Right Trolls," *Mother Jones*, May 3, 2017.
6. "How We Debunked Rumours that Macron Has an Offshore Account," *France 24 – The Observers*, May 5, 2017.
7. Chris Doman, "MacronLeaks – A Timeline of Events," *AlienVault*, May 6, 2017.

January 2017.[8] Several attacks were carried out by email spoofing: in one instance, for example, campaign staffers received an email apparently coming from the head of press relations, providing them with 'some recommendations when [talking] to the press' and inviting them to 'download the attached file containing talking points.'[9]

In total, the professional and personal email accounts of at least five of Macron's close collaborators were hacked, including those of his speechwriter, his campaign treasurer and two members of parliament.[10] The hackers waited until the very last moment to leak the documents: 5 May 2017, only one hour before official campaigning stopped for the period of 'election silence,' a 44-hour political media blackout ahead of the closing of the polls. The files were initially posted on *Archive.org*, then on *PasteBin* and *4chan*. Pro-Trump accounts (William Craddick,[11] Jack Posobiec[12]) were the first to share the link on Twitter, with the hashtag #MacronLeaks, quickly followed by WikiLeaks. Overall, the hashtag '#MacronLeaks reached 47,000 tweets in just three and a half hours after the initial tweet.'[13] Other fake documents spread on Twitter included emails that were *not* in the dump, from or to people who did *not* exist. An obviously fake email, allegedly written by Macron's Director of General Affairs, included declarations such as 'my love for Yaoi [Japanese gay manga] and progressive metal prevented me from seeing the truth.'[14] This and other obscene statements were retweeted more than 1,000 times.

The Macron leaks reveal the following pattern of operation: first, the content is dumped onto the political discussion board of *4chan* (/pol/). Second, it is transferred to mainstream social networks like Twitter. Third, it is spread through political communities, notably the US alt-right and French far-right, via 'catalyst' accounts, or 'gurus' (Craddick, Posobiec), and retweeted by both real people ('sect followers')[15] and bots. The use of bots was pretty obvious given that some accounts posted almost 150 tweets per hour.[16]

---

[8] Michel Rose and Eric Auchard, "Macron Campaign Confirms Phishing Attempts, Says No Data Stolen," *Reuters*, April 26, 2017.

[9] Mounir Mahjoubi, interviewed in Antoine Bayet, "Macronleaks : le responsable de la campagne numérique d'En Marche! accuse les 'supports' du Front national,» *France Info*, May 8, 2017, https://mobile.francetvinfo.fr/politique/emmanuel-macron/video-mounirmahjoubi-patron-de-lacampagne-numerique-d-emmanuel-macron-le-macronleaks-ca-pue-la-panique_2180759.html#xtref=https://t.co/cJLsohjh7U

[10] Frédéric Pierron, «MacronLeaks : 5 victimes et des failles de sécurité,» fredericpierron.com blog, May 11, 2017.

[11] The founder of Disobedient Media, Craddick is notorious for his contribution to the 'Pizzagate' conspiracy theory that targeted the Democratic Party. He was one of the first to spread the rumour about Macron's supposed secret bank account on Twitter at 9:37 pm. It was quickly retweeted by some 7,000 Twitter accounts, mostly pro-Trump.

[12] An infamous American alt-right and pro-Trump troll: https://en.wikipedia.org/wiki/Jack_Posobiec

[13] Ben Nimmo, Naz Durakgolu, Maks Czuperski and Nicholas Yap, "Hashtag Campaign: #MacronLeaks. Alt-right Attacks Macron in Last Ditch Effort to Sway French Election," Atlantic Council's Digital Forensic Research Lab, 6 May 2017.

[14] Josh Caplan, (@joshdcaplan) (@BreitbartNews), May 2017, https://twitter.com/joshdcaplan/status/860868394534522880/photo/1?tfw_creator=%40Slatefr&tfw_site=Slatefr&ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fwww.slate.fr%2Fstory%2F145221%2Fle-macronleaks-est-une-fakenews

[15] The 'gurus'/'sect followers' mechanism has been described by Lion Gu, Vladimir Kropotov and Fyodor Yarochkin, "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public," A Trendlabs Research Paper, *Trend Micro*, 2017, 42.

[16] Nimmo et al., "Hashtag Campaign".

Who did it?

Attribution is a complex and sensitive issue. At the time of writing, more than a year after the incident, France still has not publicly attributed the attacks to any particular perpetrator. On June 1, 2017, Guillaume Poupard, the head of the French National Cybersecurity Agency (ANSSI), declared that 'the attack was so generic and simple that it could have been practically anyone.'[17]

The expert community, however, has pointed to the Kremlin. There were several reasons to justify this attribution. First, the email address (frankmacher1@gmx.de) initially used to upload the files on *Archive.org* is registered with the same German webmail provider that was implicated in the 2016 cyberattack against Angela Merkel's party,[18] which was attributed to APT28, a cyberespionage group linked to Russia's Main Intelligence Directorate, better known by its Russian acronym GRU.[19] Of course, this alone does not prove anything as GMX Mail has over 11 million active users. Second, all of the Excel bookkeeping spreadsheets that were leaked contained metadata in Cyrillic and indicate that the last person to have edited the files is an employee of the Russian information technology company EUREKA. Among the company's clients are several government agencies, including the Russian Federal Security Service (FSB).[20] However, it is difficult to infer anything from this connection as it could very well be a false flag operation pointing to Moscow. Third, Putin's confidant Konstantin Rykov, sometimes nicknamed the 'chief troll', who boasted of his role in securing Trump's election, also acknowledged having failed in the case of France: 'We succeeded, Trump is president. Unfortunately Marine did not become president. One thing worked, but not the other.'[21]

It was no secret that Macron's opponent, Marine Le Pen, was the Kremlin's favoured candidate. In 2014, her party, the Front National, received a loan of €9.4 million from the First Czech-Russian Bank in Moscow. One month before the election, Le Pen travelled to Moscow to meet with Putin; she claimed that it was their first meeting, but in reality it was their third.[22] This suggests that the Kremlin made a major 'investment' in the Front National.[23]

None of these facts *proves* anything, but the available evidence, taken together, does point in the direction of Moscow. With one notable exception: the user responsible for ‘Macron Gate’ two days before the leak, may in fact be an American neo-Nazi hacker, Andrew Auernheimer.[24] Given the well-known alliance that exists between the Kremlin and American far-right movements,[25] these two hypotheses are not incompatible.

---

[17] Andrew Rettman, "Macron Leaks Could Be 'Isolated Individual', France Says," *EU Observer*, June 2, 2017.

[18] Sean Gallagher, "Evidence Suggests Russia Behind Hack of French President-Elect," *Ars Technica,* May 8, 2017.

[19] Feike Hacquebord, "Pawn Storm Targets German Christian Democratic Union," TrendLabs Security Intelligence Blog, May 11, 2016.

[20] Gallagher, "Evidence Suggests Russia Behind Hack of French President-Elect".

[21] Konstantin Rykov in a mediametrics.ru interview, in the documentary directed by Paul Moreira, "La guerre de l'info: au cœur de la machine russe" 2017, https://www.arte.tv/fr/videos/075222-000-A/guerre-de-l-info-au-coeur-de-la-machine-russe

[22] According to Pierre Malinowski, former adviser to Jean-Marie Le Pen, interviewed in the documentary "La guerre de l'info."

[23] Ibid.

Why did it fail?

Ultimately, the whole operation did not significantly influence French voters. This outcome can be attributed to a combination of structural factors, luck, as well as good anticipation and reaction by the Macron campaign staff, the government and civil society, especially the mainstream media.

Structural reasons

Compared with other countries, especially the US and the UK, France presents a less vulnerable political and media environment for a number of reasons. First, the election of the president is direct, making any attempt at interference in the election in favour of one of the candidates more obvious. Furthermore, the French election has two rounds, which creates an additional difficulty for the attackers as they do not know in advance who will make it to the second round. Additionally, this permits voters to mobilise in the event of an unexpected result after the first round.

In addition, the French media environment is pretty resilient: there is a strong tradition of serious journalism, the population refers mostly to mainstream sources of information, while tabloid-style outlets and ‘alternative’ websites are less popular than they are in the US and in the UK.

Finally, cartesianism plays a role: rationality, critical thinking, and a healthy scepticism are part of the French DNA and are encouraged from primary school and throughout one’s professional life.

The element of luck

In this story, as in any success story, good luck has a part to play: the Macron team was lucky that the hackers and other actors involved in this operation made a number of mistakes.

First, they were overconfident. They overestimated their ability to shock and mobilise online communities, underestimated the resistance and the intelligence of the

---

24. David Gauthier-Villard, “U.S. Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm,” *Wall Street Journal*, May 16, 2017.

25. Casey Michel, “America’s Neo-Nazis Don’t Look to Germany for Inspiration. They Look to Russia”, *Washington Post*, August 22, 2017.

mainstream media and, above all, they did not expect that the Macron campaign staff would react – let alone react so cleverly (see below). They also overestimated the interest of the population in an operation that ultimately revealed nothing. They assumed that creating confusion would be enough, and that the content of the leaks would somehow be secondary. But, as it became obvious that the thousands of emails and other data were, at best, boring and, at worst, totally ludicrous, the public lost interest.

Second, the idea to launch the offensive just hours before the electoral silence period was a double-edged sword: the goal was certainly to render Macron unable to defend himself, and to mute the mainstream media. And maybe, because the leaks did not contain anything interesting, they decided to play up the announcement of the revelation rather than the content itself. In any case, this choice of timing did not leave provocateurs with sufficient time to spread the information.

Third, the attack also suffered from cultural clumsiness. Most of the catalyst accounts (and bots) were in English because the leaks were first spread by the American alt-right community. This was not the most effective way of penetrating a French-speaking population. It also likely alienated some French nationalist voters who are not inclined to support anything American.

Learning from others

Paris somehow learned from the mistakes witnessed during the American presidential campaign: disdain for and an attitude of benign neglect towards disinformation campaigns, reluctance to address and frame the hacking of the Democratic National Committee (DNC), a delayed response, etc. In January 2017, the defence minister acknowledged that 'our services are having the necessary discussions on this subject, if only to draw lessons for the future.'

Relying on the relevant actors

Two bodies played a particularly crucial role. First, the National Commission for monitoring the presidential electoral campaign (CNCCEP), a special body set up in the months preceding every French presidential election and serving as a campaign watchdog. Second, the National Cybersecurity Agency (ANSSI), whose mission was two-fold: to ensure the integrity of electoral results and to maintain public confidence in the electoral process. In addition, the campaign managers were quick to reach out to law enforcement authorities and report the hack. As a consequence, on Friday night, as the leak was underway and only hours after the initial dump, the public prosecutor's office in Paris opened an investigation.

Raising awareness

ANSSI and the CNCCEP alerted the media, political parties and the public about the risk of cyberattacks and disinformation during the campaign. ANSSI proactively offered to meet and educate the campaign staffs of all candidates in the very early stages of the election: in October 2016, it organised a workshop. All but one party (the Front National) participated.

Showing resolve and determination

From the start of the electoral campaign, the French government promptly signalled its determination to prevent, detect and, if necessary, respond to foreign interference, both publicly and through more discreet and diplomatic channels. The minister of defence said that 'by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty' and that 'France reserves the right to retaliate by any means it deems appropriate.'[26] The minister of foreign affairs said that 'France will not tolerate any interference in its electoral process.'[27] A similar message was conveyed directly by the minister to his Russian counterpart and by President Hollande to President Putin.

Beat hackers at their own game

ANSSI raised the level of security for voting infrastructures by securing the whole electoral process chain to ensure its integrity. Following ANSSI's recommendation, the ministry of foreign affairs announced at the beginning of March 2017 the end of electronic voting for citizens abroad because of an 'extremely high risk' of cyberattacks. As the hacks could not be avoided, the *En Marche!*[28] team set up traps: 'You can flood the emails of your employees with several passwords and logins, both real and fake, that the [hackers] spend a lot of time trying to understand them,' explained Mounir Mahjoubi, the digital manager of Macron's campaign team.[29] This diversionary tactic, which involves creating fake documents to confuse the attackers with irrelevant and even sometimes deliberately ridiculous information, is called 'cyber blurring' or 'digital blurring'. It was successful in shifting the burden of proof on to the attackers: the Macron campaign staff did not have to justify potentially compromising information contained in the Macron leaks; rather, the hackers had to justify why they stole and leaked information which seemed, at best, useless and, at worst, false or misleading.

---

[26] Ibid.

[27] Martin Untersinger, "Cyberattaques: la France menace de 'mesures de rétorsion' tout État qui interférerait dans l'élection," *Le Monde,* 15 February 2017.

[28] The name of Emmanuel Macron's political movement is *La République en Marche!* (*REM*), sometimes shortened to *En Marche!*

[29] Mounir Mahjoubi, interviewed in Raphaël Bloch, "MacronLeaks: comment En Marche a anticipé les piratages ", *Les Echos*, May 10, 2017.

The importance of strategic communication

During the entire campaign, the *En Marche!* team communicated openly and extensively about its susceptibility to a hacking attack, and then very soon about the hacking operation itself. When the leaks finally happened, *En Marche!* reacted in a matter of hours. At 11:56 pm on Friday 5 May, only hours after the documents were dumped online and 4 minutes before the electoral media blackout went into effect, the campaign staff issued a press release.[30] The robust and continuous presence of the Macron campaign staff on social media enabled them to respond quickly to the spread of the information. They systematically responded to posts or comments that mentioned the 'Macron Leaks.' The campaign's injection of humour and irony into their responses increased their visibility across different platforms. The *En Marche!* press release says that the leaked documents 'reveal the normal operation of a presidential campaign.' In fact, nothing illegal, let alone interesting, was found.

In addition, Macron's team was very engaged with traditional media outlets, stressing their responsibility for professional reporting. On Friday night, Macron's team referred the case to the CNCCEP which issued a press release the day after, asking 'the media not to report the content of this data, especially on their websites, reminding them that the dissemination of false information is a breach of law, notably criminal law.'[31] The majority of traditional media sources responded to this call by choosing not to report on the content of the leaks.

Undermining propaganda outlets

On April 27, Macron's campaign confirmed that it had denied RT and Sputnik accreditations to cover the rest of the campaign. Even after the election, both outlets have been banned from the Élysée presidential palace and foreign ministry press conferences. The decision is justified on two grounds. First, these outlets are viewed as propaganda organs for the Kremlin – this is not only Macron's position, expressed clearly during the campaign and most famously in front of President Putin at the Versailles press conference only weeks after the election, but it has been the position of the European Parliament as early as November 2016.[32] Second, attendance at these press conferences is by invitation only so there is no need for French institutions to justify their exclusion of these news outlets.

---

30. En Marche!, Communiqué de Presse, « En Marche a été victime d'une action de piratage massive et coordonnée », May 5, 2017, https://en-marche.fr/articles/communiques/communique-presse-piratage

31. Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle, « Recommandation aux médias suite à l'attaque informatique dont a été victime l›équipe de campagne de M. Macron, » May 6, 2017, http://www.cnccep.fr/communiques/cp14.html

32. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)).

Conclusion

Overall, structural factors as well as an effective, proactive strategy allowed the French authorities to successfully mitigate the damage of the Macron leaks. But the threat persists. Therefore, in the last year, the Macron administration took additional steps: first, in January 2018, the president announced his intention to pass legislation on the issue of 'fake news' by the end of the year. In March 2018, the minister of culture, Françoise Nyssen, revealed further details about the 'fake news' bill,[33] which was renamed in May from a law "Against false information" (*contre les fausses informations*) to a law "relating to the fight against information manipulation" (*relative à la lutte contre la manipulation de l'information*). It has yet to be passed.

Second, in March 2018,[34] the minister of culture committed to double her ministry's allotted budget for media and information literacy, increasing it from €3 to €6 million.

Third, the foreign ministry's Policy Planning Staff (*Centre d'analyse, de prévision et de stratégie*, - *CAPS*) and the defence ministry's Institute for Strategic Research (*Institut de recherche stratégique de l'Ecole militaire*, of which the author is the director), launched an inter-ministerial working group on what we refer to as 'information manipulation.' The final product is a report including concrete recommendations for all actors – states, civil society and digital platforms.[35] For France, our main recommendation is the creation of an inter-ministerial structure entirely devoted to detecting and countering information manipulation.

---

[33] Françoise Nyssen, Speech at the "Assises du journalisme" (annual gathering of French media professionals), Tours, March 15, 2018, http://www.culture.gouv.fr/Presse/Discours/Discours-de-Francoise-Nyssen-prononce-a-l-occasion-des-Assises-internationales-du-journalisme-de-Tours-jeudi-15-mars-2018

[34] Ibid.

[35] J.-B. Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.

CHAPTER 8

The next front: the Western Balkans

Oscar Jonsson

For many years now, countries in the Western Balkans have been on a steady, albeit slow, path towards membership of Europe's two main regional organisations: the EU and NATO.[1] Until 2014, Russia was not perceived as a major obstacle *vis*-à-*vis* their Western integration. Since the annexation of Crimea, however, Russia has reemerged as a disruptive actor and a problem for the EU in the region. For Russia, the enlargement of the EU and NATO represents a strategic setback, and hindering, and potentially reversing, this process is a primary objective for the Kremlin. The Western Balkans has thus become an arena for increasing geopolitical competition between Russia and the EU and the US. As Russia's economy has faltered under the impact of declining oil prices and Western sanctions and the country has become increasingly isolated on the international stage, Moscow's strategy since 2014 has been characterised by disruption and manipulation.

In this competition, cyber tools are a key instrument enabling Russia to promote its political agenda. Russia has repeatedly employed cyber tools to punish, disrupt and disinform. Large-scale cyberattacks have been carried out either discretely or as a part of complex hybrid operations in combination with other coercive means. Cyberattacks seek not only to cause widespread disruption but also to undermine partners' confidence in the targeted states and increase the potential cost of integrating them.

Russia has been especially effective in the information-psychological arena, where Russian narratives have received significant amplification through social media, Russian-language websites and dissemination in local media outlets. The information-psychological domain is key for eroding support for the EU and NATO in the region and increasing polarisation between pro-EU and pro-Russian factions.

---

[1] Albania, the former Yugoslav Republic of Macedonia (FYROM), Montenegro and Serbia are candidate countries to the EU. The latter two are currently engaged inmembership negotiations. Albania and FYROM obtained conditional opening of accesion negotiaitons. Bosnia and Herzegovina, and Kosovo have the status of potential candidates. Albania and Montenegro are NATO-members, FYROM received an invitation in 2018 to join NATO, while Bosnia and Herzegovina is an aspirant country; Serbia has an individual partnership action plan with NATO. See European Commission, "A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans", 2018, https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf

Cyberattacks and espionage

Countries in the region have been frequently targeted by malicious activities. The most notable of these was the alleged theft of the entire Serbian national identity database in late 2014. The hackers were apparently motivated by grievances that the Serbian police were lax on Albanian cyber criminals.[2] A month later, Serbia faced its largest cyberattacks – in the form of distributed denial-of-service (DDoS) attacks – so far, targeting the majority of Serbian media websites.[3] Many of the targeted webpages were knocked offline for hours and the hackers claimed to be working for Albanian interests. Other cyberattacks that occurred in the region included: the Serbian justice ministry's website being hacked with calls for civil resistance;[4] DDoS attacks on the OSCE's Freedom of the Media website after the organisation publicised criticism of Serbia;[5] cyberattacks against Kosovar journalists;[6] as well as a denial-of-service (DoS) attack on Bosnian, Albanian and Serbian media outlets.[7] Cyberattacks and cyber intrusions are thus a common occurrence, which increases the opportunities for Russia to conduct them in the knowledge that they cannot be attributed to Moscow with any degree of certainty.

However, in the Western Balkans, Montenegro has been the most notable target of cyberattacks and cyber espionage with a Russian footprint. Such activity increased notably as Montenegro embarked on its path to NATO membership; Montenegro concluded association negotiations with NATO in May 2016 and joined the Alliance in June 2017. The Montenegrin government saw the number of cyberattacks increase from 22 in 2013 to over 400 in 2017, where the state institutions and media were the most frequent targets.[8]

A report for the public administration ministry concluded that 'the severity and sophistication of cyberattacks affecting Montenegro during 2016 were reflected in the increased number of identified attacks on infrastructure and cyber espionage cases, as well as through phishing campaigns which targeted civil servants.'[9] The ministry also mentioned an increase in the hacking of banks and private companies.

---

2. Pierluigi Paganini, "Serbia – Hackers claimed to have stolen the entire national database," *Security Affairs*, December 13, 2014, https://securityaffairs.co/wordpress/31068/cyber-crime/serbia-hackers-stolen-national-database.html
3. Mike Walker, "The Cyber-attacks and Fears of Cyber-war to Come,"*InSerbia*, 21 October 21, 2014, https://inserbia.info/today/2014/10/the-cyber-attacks-and-fears-of-cyber-war-to-come/
4. Nemanja Cabric, "Serbs Detain 'Anonymous' Cyber Warrior for Sabotage", *Balkan Insight*, March 9, 2012, <http://www.balkaninsight.com/en/article/serbs-detain-anonymous-cyber-warrior-for-sabotage>
5. Marija Ristic, "Hacker Attacks 'Try to Censor' OSCE Website," *Balkan Insight*, June 4, 2014, <http://www.balkaninsight.com/en/article/osce-website-under-cyber-attack>
6. Die Morina, "Kosovo Authorities "Failing to Punish Journalists' Attackers," *Balkan Insight*, February 24, 2017, <http://www.balkaninsight.com/en/article/safety-of-journalists-in-kosovo-02-24-2017>
7. OSCE, "Hacker Attacks on Media Websites Endangers Media Freedom, Says OSCE Representative," October 21, 2014, https://www.osce.org/fom/125709
8. Dusica Tomovic and Maja Zivanovic, "Russia's Fancy Bear Hacks its Way Into Montenegro," *Balkan Insight*, March 5, 2018, <http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018>
9. Dusica Tomovic, "Montenegro on Alert Over Rise in Cyber Attacks," *Balkan Insight*, January 10, 2017, http://www.balkaninsight.com/en/article/montenegro-on-alert-over-cyber-attacks-01-09-2017

On the day of the parliamentary elections, 16 October 2016, large-scale DDoS attacks targeted state webpages and network infrastructure, as well as the websites of pro-NATO and pro-EU political parties, civil society webpages and electoral monitors' webpages.[10] Several state institution websites were brought down by the attacks, as well as the webpages of pro-governmental parties. The website of the electoral watchdog, the Center for Democratic Transition, also became inaccessible.

Montenegrin media claimed that the attack was carried out by the same Russian hackers that interfered with the 2016 US elections.[11] This claim was echoed by the cybersecurity group Trend Micro, who identified APT28 (Advanced Persistent Threat 28) as the actor responsible for the attacks.[12] APT28 is also known as Fancy Bear and is a hacking group directed by the GRU, the Russian military intelligence agency. They gained notoriety for leaking the Democratic National Committee's emails in the 2016 US election campaign, but also for carrying out cyberattacks against the German parliament and the French television channel TV5.

The government in Podgorica directly accused Russia of intervening in the Montenegrin election.[13] This should also be seen in conjunction with the attempted coup in Montenegro that took place on election day. On the same day as the cyberattacks, the Montenegrin authorities arrested twenty people with Serbian, Montenegrin and Russian citizenship. Notably, Russian GRU intelligence officers Eduard Shirokov (alias Shishmakov) and Vladimir Popov were identified as the organisers of the coup, which sought to assassinate the prime minister.[14] Both Shirokov and Popov were intercepted in Serbia in possession of Montenegrin special forces uniforms and are being prosecuted *in absentia* for their involvement in the coup attempt.[15] Twelve people have been indicted in Montenegro and are awaiting trial.

In January 2017, the Montenegrin ministry of defence was targeted by a spear phishing attack (a targeted attempt to steal data and/or install malware). Emails that appeared to come from the EU and NATO had attachments that enabled hackers to upload a malware called Gamefish, which has been a signature method used by APT28.[16] Gamefish is a Trojan virus that allows access to the computer at hand so that its data can be exfiltrated.[17] The data can be used for intelligence purposes, but also for targeting in cyberattacks.

---

[10] Vesko Garcevic, "Congressional Testimony to Committee on Senate Select Intelligence," June 28, 2017.

[11] Dusica Tomovic, "Montenegro on Alert Over Rise in Cyber Attacks", *Balkan Insight*, January 10, 2017, http://www.balkaninsight.com/en/article/montenegro-on-alert-over-cyber-attacks-01-09-2017

[12] "Update on Pawn Storm: New Targets and Politically Motivated Campaigns, *Trend Micro*, January 12, 2018, https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns

[13] Dusica Tomovic, "Montenegro on Alert Over Rise in Cyber Attacks," *Balkan Insight*, January 10, 2017, http://www.balkaninsight.com/en/article/montenegro-on-alert-over-cyber-attacks-01-09-2017

[14] Vesko Garcevic, "Congressional Testimony to Committee on Senate Select Intelligence," June 28, 2017,.

[15] Dimitar Bechev, "The 2016 Coup Attempt in Montenegro: Is Russia's Balkans Footprint Expanding?," Foreign Policy Research Institute, April 12, 2018, https://www.fpri.org/article/2018/04/the-2016-coup-attempt-in-montenegro-is-russias-balkans-footprint-expanding

[16] Pierluigi Paganini, "Russia-linked hacker group APT28 continues to target Montenegro", *Security Affairs*, June 7, 2017, http://securityaffairs.co/wordpress/59820/hacking/apt28-targets-montenegro.html

[17] Chris Bing, "APT28 targeted Montenegro's government before it joined NATO, researchers say", *CyberScoop*, June 6, 2017, https://www.cyberscoop.com/apt28-targeted-montenegros-government-joined-nato-researchers-say/

Subsequently, in February 2017, a DDoS-attack larger than the ones targeting the elections was launched. The main targets were again the government, state institutions, and pro-government media. The Montenegrin government stated that 'the scope and diversity of the attacks and the fact that they are being undertaken on a professional level indicates that this was a synchronised action'.[18] Three cybersecurity firms – FireEye, Trend Micro and ESET – concluded that the February attacks also came from APT28.[19]

Neither of the cyberattacks had any large-scale impact on the course of Montenegrin politics. Montenegro joined NATO on 5 June 2017 and has since aligned itself closely with the Western camp, as demonstrated for example by its expulsion of a Russian diplomat/intelligence agent after the poisoning of Sergei Skripal. Nonetheless, cyberattacks are a tool which Russia might again deploy in the future against Montenegro and their effects could be more destructive the next time around.

Disinformation and strategic communications

Another sphere that Russia exploits for political purposes is the media. Russian disinformation and propaganda is implemented through a myriad of actors, including Russian embassies, state-owned media, hackers, the Internet Research Agency and *faux* civil society organisations. A leaked intelligence report from FYROM showed how Russian intelligence services were coordinating the activities of Russian journalists and *Rossotrudnichestvo,* the state agency for Russian compatriots living abroad.[20] The Center for Euro-Atlantic Studies, a Serbian think tank, recently concluded that 51 different pro-Kremlin organisations were active in Serbia.[21] This multitude of actors allow for both ambiguity and the creation of an echo chamber-effect that is amplified in social media.

The most important part of the Russian toolkit is Sputnik Serbia (*Srbjia),* which has emerged as a crucial outlet for the Russian narrative not only in Serbia, but also in the wider Western Balkans region. Another government-connected actor is Russia Beyond the Headlines (RBTH), a government-sponsored news agency that is part of TV Novosti, which also owns RT. RBTH launched a mobile application that is available in Macedonian, Serbian and Slovenian. Moreover, in Serbia and other Serbian-speaking part of the region, key pro-Russian outlets include Fakti, IN4S, Pravda.rs, Princip, Sedmica, Srbin.info, and Vostok.

---

[18] Dusica Tomovic, "Montenegro on Alert over New Cyber Attacks," *Balkan Insight,* February 21, 2017, http://www.balkaninsight.com/en/article/montenegro-govt-on-alert-over-new-cyber-attacks-02-21-2017

[19] Dusica Tomovic and Maja Zivanovic, "Russia's Fancy Bear Hacks its Way Into Montenegro," *Balkan Insight*, March 5, 2018, http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018.

[20] Luke Harding et al, "Russia actively stoking discord in Macedonia since 2008, intel files say," *The Guardian*, June 4, 2017, https://www.theguardian.com/world/2017/jun/04/russia-actively-stoking-discord-in-macedonia-since-2008-intel-files-say-leak-kremlin-balkan-nato-west-influence

[21] Center for Euro-Atlantic Studies (CEAS), "Eyes Wide Shut: Strengthening Russian Soft Power in Serbia: Goals, Instruments, and Effects" , May 2016, https://www.ceas-serbia.org/en/ceas-publications/study-eyes-wide-shut

The narratives vehicled by the media and internet portals are a mix of the more general pro-Russian, pro-Orthodox, anti-EU and anti-NATO rhetoric as well as more specific narratives, for example promoting Russian military cooperation and warning against Albanian expansionism.[22] The West is blamed for inciting unrest[23] and 'Colour Revolutions' in the Balkans and trying to topple Miroslav Dodik, the leader of *Republika Srpska* in Bosnia.[24] The EU is furthermore depicted both as trying to impose foreign values and standards on the people of the Balkans, but also as disunited, chaotic, dysfunctional and not worth joining.[25]

The Russian approach to the information-psychological sphere has been effective, as attested by the extent to which the Russian narrative has been echoed and magnified in local media and in opinion polls. Sputnik Serbia and RBTH have become key linchpins for news reporting in the region and their stories are republished daily in Serbian, Montenegrin and Bosnian outlets.[26] The number of media outlets taking a pro-Russian stand has recently grown from a dozen to over a hundred and Sputnik has emerged as the most quoted foreign source.[27] In Serbia, Sputnik provides online stories and news to over 20 radio stations.[28]

Sputnik and RBTH have managed to acquire this predominant role due to the edge that they have over other, less well-resourced news outlets at a time of massive structural transformation in the media industry. This is also reflected in the recent decline in the operations of Tanjug, the former Yugoslavian and now Serbian press agency. Sputnik allows its articles to be reproduced for free, which makes it easy and cheap for journalists to republish an already well-written article articulating the Russian narrative. Furthermore, Sputnik articles often have a sensationalist angle, an asset in today's era of click-bait journalism.

Opinion polls in Serbia demonstrate that Russia has been successful in strengthening its image: 42% of Serbians see Russia as their most supportive partner, while only 14% indicate the EU.[29] Similarly, 64% of Serbs see NATO as a threat, even though military cooperation is significantly closer with NATO than with Russia. In 2016, Serbia had 125 military-to-military exchanges with NATO compared to only four with Russia.[30] While Russian aid, trade and foreign direct investment is of a lesser order of magnitude than that provided by the EU, most Serbians believes that Russia is their main benefactor.[31] It is easier to sell cooperation with Russia than with the West to the Serbian people – despite the fact that Serbia is on an accession trajectory to the EU.

---

[22] Dusica Tomovic, "Pro-Russian Montenegrins Publish New Anti-Western Media", *Balkan Insight*, October 18, 2017, <http://www.balkaninsight.com/en/article/pro-russian-montenegrins-publish-new-anti-western-media-10-17-2017>

[23] Nenad Zorić, "Nije ruska propaganda – Balkan je namerno nestabilan" [It's not Russian propaganda - the Balkans are deliberately unstable], *Sputnik Serbia*, December 7, 2015,, https://rs-lat.sputniknews.com/komentari/201512071101643828-Nije-ruska-propaganda-Balkan-je-namerno-nestabilan/.

[24] "'Sputnjik': Postoji tajni plan za rušenje Dodika" [Sputnik: There is a secret plan to destroy Dodik], *Blic,* November 23, 2015, https://www.blic.rs/vesti/politika/sputnjik-postoji-tajni-plan-za-rusenje-dodika-kulminacija-napada-posle-bozica/hlvxvc5.

[25] US Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe", January 10. 2018, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[26] John Cappello, "Russian Information Operations in the Western Balkans," Foundation for the Defence of Democracies, February 2, 2017, http://www.defenddemocracy.org/media-hit/john-cappello-russian-information-operations-in-the-western-balkans/

[27] US Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe," January 10, 2018.

[28] Andrew Byrne, "Kremlin-Backed Media Adds to Western Fears in Balkans," *Financial Times*, March 19, 2017, https://www.ft.com/content/3d52cb64-0967-11e7-97d1-5e720a26771b

[29] US Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe," January 10, 2018.

This is not to argue, however, that Russia has managed to reverse the strategic alignments in the region through its use of disinformation and strategic communication. As a matter of fact, many of the states in the Western Balkans are closer to the EU in terms of both economics and their accession process. However, the fact that Russia, despite weaker ties in the region, has managed to maintain its popularity, and increase local distrust of the EU, even though the EU contributes significantly more to the region than Russia, is a sign of how successful its strategy has been.[32] Russia's success in projecting this subversive influence, however, primarily reflects pragmatism on the part of the local actors who have no problem in playing Russia and Europe off against each other to advance their own interests.

Looking ahead: Russia's future strategy

Russia will likely continue to seek to hinder or reverse Western integration in the region using whatever tools are at its disposal. A defining dynamic of the future competition is EU and NATO-accession. In February 2018, the EU adopted a new strategy for the Western Balkans which emphasised that the EU is open to accession, with a perspective of EU membership for Serbia and Montenegro by 2025.

The country that is at greatest risk of future cyberattacks is Montenegro: it has been the hardest hit so far and its networks are likely the most infected with malware used by the hackers. As Skopje and Athens made progress on the name dispute dossier,[33] FYROM was invited to join NATO and received a conditional date to kick off accession negotiations with the EU. In this case, the Russian approach is likely to mirror that adopted towards Montenegro, with more extensive cyberattacks and disinformation campaigns unfolding in the coming year.

Serbia is less likely to face significant Russian opposition in its bid to join the EU. Rather, Russia is likely to be content with having a state within the EU that is relatively sympathetic to Russia (and that could be more useful to it inside than outside of the EU). Another means of hindering Western integration is stirring

---

30. Kaitlin Lavinder, "Russia Ramps Up Media and Military Influence in Balkans," *The Cipher Brief*, October 13, 2017, https://www.thecipherbrief.com/russia-ramps-media-military-influence-balkans

31. "Moscow is regaining sway in the Balkans," *The Economist*, February 25, 2017, https://www.economist.com/news/europe/21717390-aid-warplanes-and-propaganda-convince-serbs-russia-their-friend-moscow-regaining-sway

32. European Parliament, "Russia in the Western Balkans," *At A Glance*, July 2017, http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/608627/EPRS_ATA%282017%29608627_EN.pdf

33. "Macedonia to hold referendum on name change on 30 September", *Euractiv*, July 31, 2018, https://www.euractiv.com/section/enlargement/news/macedonia-to-hold-referendum-on-name-change-on-30-september/

up secessionist sentiments and ethnic discontent. The most likely target for such a strategy is Republika Srpska in Bosnia, whose secessionist claims the Russian government supports.[34] Both the leader of Republika Srpska and pro-Russian media are pushing for a referendum on independence.[35]

Provoking more tensions in the already strained relations between Serbia and Kosovo is another likely future tactic aimed at obstructing the EU's efforts to bring the sides closer. This could particularly be the case if Kosovo makes further progress towards UN membership.

The use of cyber tools to coerce and disinform is likely to increase given Russia's interest in thwarting the process of Western integration in the region, as well as the fact that digital connectivity in the region is on the rise. Resorting to cyber operations will not in itself alter the strategic reality in the Western Balkans, but the use of cyber tools and weapons will remain a cost-effective way for Russia to create societal disruption and tarnish the image of the EU.

---

[34] Misha Savic and Gordona Filipovic, "Europe's Next Separatist Time Bomb Is Ticking," *Bloomberg*, November 16, 2017, https://www.bloomberg.com/news/articles/2017-11-16/europe-s-next-separatist-time-bomb-is-ticking-in-the-balkans

[35] Seth Cropsey and Kevin Truitte, "Bosnia: They're at It Again," *National Review*, July 7, 2017, https://www.nationalreview.com/2017/07/bosnia-russian-interference-renewed-putin/

EU and NATO approaches to cyber threats

CHAPTER 9

NATO’s responses to cyberattacks

Siim Alatalu

Since NATO was founded in 1949, the tasks of the Alliance have evolved, reflecting the key international security challenges of the day while maintaining the commitment to the core task of collective defence. For most of its history, NATO’s role has first and foremost been to provide military security for its constituent nations where they are geographically located – in Europe and North America. Cyber, however, which is of a global and real-time nature by definition, could bring distant threat actors and acts close to home for NATO and vice versa, thereby inducing the Alliance to develop a fully-fledged strategy to also counter challenges from far away. 2017 saw two global outbreaks of malware[1] attacks, known as WannaCry and NotPetya, which caused economic damage on an unprecedented scale – and in unprecedented areas. NATO was confronted with the resurgence of an old foe – Russia – this time in cyberspace.[2]

NATO’s thinking on cyber since 9/11

NATO is not a novice when it comes to dealing with cybersecurity issues. In fact, the word ‘cyber’ first entered NATO vocabulary in November 2002 when at the Prague Summit the Heads of State and Government (HOSG) of the then 19 Allies agreed to ‘strengthen [their] capabilities to defend against cyber-attacks’,[3] after a number of NATO websites had suffered cyberattacks in the years before.[4] The Prague Summit was the first meeting of NATO's leaders since the 9/11 terrorist attacks and was therefore transformational in many ways for both individual Allies and for NATO as a whole. The rather limited attention paid by NATO to cyber in 2002 may seem surprising by today's standards.

---

[1] “Software that may be stored and executed in other software, firmware or hardware that is designed to adversely affect the performance of a computer system”: Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017.)

[2] “Environment formed by physical and non-physical components to store, modify, and exchange data using computer networks” (*Tallinn Manual 2.0*)

[3] “Prague Summit Declaration”, November 21, 2002, http://www.nato.int/docu/pr/2002/p02-127e.htm

[4] Jason Healey and Klara Tothova Jordan, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, *IssueBrief*, Atlantic Council, September 2014, https://www.files.ethz.ch/isn/183476/NATOs_Cyber_Capabilities.pdf

While the internet was already a global public good at the time, in 2002 its effects on how society works were markedly different from today. The number of people connected online was only 587 million or 9.4% of the global population,[5] compared to 3.553 billion or 53.8% in 2017.[6] For sure, cyberspace was not foreseen as a theatre (or as an enabler) for military operations – and not therefore as an arena in which NATO might have to engage. Rather, attention was more focused on national efforts[7] to tackle emerging, and mainly domestic, cyber-related challenges to governments, induced by individuals rather than by organised, national or trans-border entities which NATO as an organisation reflected.

Today, every second person on the planet is connected online – representing roughly a sixfold growth since 2002. However, what matters is not just the number of people who have access to the internet, but more importantly what connectivity allows users and indeed the range of different online devices to achieve in cyberspace in terms of speed and effects. This is what makes cyber relevant for NATO, and NATO relevant in the new cyber threat landscape, not least for its member states.

After 2002 NATO continued to take a *laissez-faire* approach to cyber issues.[8] Of course, there were imminent and grave challenges for it to tackle on behalf of its members such as, *inter alia,* terrorism and military operations in Afghanistan. However, this state of affairs was to change quickly and notably in 2007 when massive, well-coordinated and politically motivated cyberattacks were launched against Estonia's government and other infrastructure. The attacks were informally[9] but virtually universally attributed to Russia,[10] and the episode acted as a wake-up call for the Alliance. Already at their Bucharest Summit in April 2008, the NATO HOSG were far more explicit on the Alliance's way forward in cyber, as reflected in their approval of NATO‘s first Policy on Cyber Defence and commitment to develop 'the structures and authorities to carry it out'.

---

[5] "Internet World Stats. Usage and Population Statistics", retrieved from https://www.internetworldstats.com/emarketing.htm

[6] "Global and Regional ICT Data", retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[7] Siim Alatalu, "NATO's New Cyber Domain Challenge," in *2016 International Conference on Cyber Conflict (CyCon U.S.) Proceedings*, ed. Aaron Brantly and Paul Maxwell (Washington, DC., 2016), 1-8.

[8] Meaning cyber not being considered a strategic task on its own but rather a support function which is handled routinely as necessary.

[9] Attribution was difficult due to the lack of hard evidence, while the 'defendant' refused to comply with Estonia's request for legal assistance and a bilateral investigation.

[10] John Arquilla, "Twenty Years of Cyberwar," *Journal of Military Ethics*, 12, no. 2 (2013): 81-82.

The HOSG stated in the Bucharest Summit Declaration that:

> 'Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber-attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities'.[11]

At the following Summit in 2009, the Strasbourg and Kehl Summit declaration devoted even more attention to cyber defence policy, including mentioning more new potential threats such as non-state actors. The establishment of two new NATO structures was announced:, the Cyber Defence Management Authority (CDMA),[12] which was charged with coordinating cyber defence activities throughout NATO's civilian and military bodies, and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Furthermore, the HOSG acknowledged the importance of international cooperation in this domain, including with non-NATO countries that are recognised as 'partners'.[13]

Such step-by-step enhancement continued at the next Summits in Chicago (2012) and Wales (2014). In Wales, NATO adopted one of the underlying ideas of the 2013 Tallinn Manual, i.e. that existing international law applies in cyberspace. The Tallinn Manual had been published by the NATO CCDCOE and relied on the expert opinion of an international group of legal experts. Politically it meant that most Western countries recognised that there was no need for a new international legal convention or other agreement to regulate cyberspace. Concurrently, the HOSG also adopted the principle that Article V of the Washington Treaty also applies in cyberspace. This meant that a cyberattack against one Ally could be considered an attack against all Allies.

At its 2016 Warsaw Summit the Alliance opened up a whole new paradigm and a new role for itself, by declaring cyberspace a domain of operations. Accordingly, Alliance militaries are developing a doctrine to integrate cyber operations in support of conventional operations through cyberspace, at an equivalent level of interoperability that it has developed in traditional areas of warfare. In Warsaw too the HOSG also made another important decision on cyber policy, called the Cyber Pledge, where they *inter alia* committed to developing 'the fullest range of capabilities to defend our national infrastructures and networks.'[14]

Naturally, implementing the aforementioned agreements in 29 countries spanning three continents needs time and one might even speculate that in Warsaw NATO achieved the necessary consensus to fulfil its mandate. This, however, might need to be reconsidered. The events in cyberspace that unfolded in the summer of 2017 – in particular the WannaCry and NotPetya malware attacks – also raised the game again for NATO. New questions have been tabled by experts that relate to information sharing, practical cooperation in cyber defence with likeminded non-NATO countries, technical safety standards and, finally, the attribution of malicious cyber acts to the actors.

---

[11] "Bucharest Summit Declaration", April 3, 2008, http://www.nato.int/cps/en/natolive/official_texts_8443.htm

[12] Today called the Cyber Defence Management Board (CDMB).

[13] "Strasbourg/Kehl Summit Declaration," April 4, 2009, http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease

[14] NATO, "Cyber Defence Pledge", July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Russia as a cyber threat

Like NATO, Russia is not a novice in cyber either – to say the least. One of the military lessons that might be gleaned from Russia's history is the tradition of taking territory and ensuring it will never return to *status quo ante*. Russia has demonstrated that it still applies this lesson in conventional warfare (it has its military boots-on-the-ground in virtually every hotspot in the former Soviet Union) and it has also developed an equivalent for cyberspace – 'people-with-bytes-online', referring to the so-called 'troll factories' or the Advanced Persistent Threats (APTs) associated with its intelligence services. For a military planner the analogy is obvious – in order for NATO to gain hold of the new domain it has embraced in recent years, it will now need to establish itself in it, including by delivering on the core tasks of collective defence, crisis management and cooperative security.[15] With NATO-Russia relations frozen and Russia currently showing no sign of having any intention of withdrawing from Crimea or Eastern Ukraine, threats from cyberspace are ever-more relevant, and involve a broader set of potential targets.

Since Russia invaded Ukraine and annexed Crimea in early 2014, all NATO nations and some of the Alliance's partners have imposed economic sanctions on the country, in the hope of persuading Moscow to reverse its actions. To date, however, the sanctions have not led the Kremlin to abide by its international obligations, although they appear to have at least deterred Russia from moving deeper into Ukraine militarily. Given the constraints it faced in using its military power against Ukraine and NATO allies, Russia began to rely more on coercive cyber tools. As an example, Russia has made headlines (including by being publicly blamed for cyberattacks) for resorting to cyber tactics in order to for instance meddle with the US, French and probably other elections, to fuel protest movements and to spread fake news – all as part of its strategy to derail the unity of the West, including NATO and the EU.

While these can be considered offensive and disrespectful actions in their own right, events took a more severe turn in July 2017. The outbreak of the so-called NotPetya malware attack wrought most havoc in Ukraine where it crippled banking, power, airport and transport services. However, the malware eventually had global ramifications. According to one estimate it has cost companies around the world an estimated $1.2 billion in revenues.[16] On 16 February 2018 Australia, Canada, Denmark, Japan, New Zealand, the United Kingdom and the United States[17] became the first countries (later followed by others) to formally attribute NotPetya to Russia. Politically, this event signals the birth of a global coalition of the willing, including two out of three nuclear powers in NATO, joined by several Allies as well as by NATO's closest non-NATO partners in cyber issues. Their demonstrated ability to collectively attribute cyberattacks to other states, including a nuclear power if need be, proved that sharing technical information is doable in a short timeframe if there is sufficient political will.

---

[15] Siim Alatalu, "NATO's New Cyber Domain Challenge".

Furthermore, on 12 March 2018 the British prime minister made a statement accusing Russia of having poisoned its former double agent Sergei Skripol, now a UK citizen living on British soil. Giving Russia a deadline of 'tomorrow midnight' to explain, the articles heralding the prime minister's statement hinted that the UK was considering countermeasures against Russia's actions, which might include cyberattacks.[18] Within days, the UK gained the political support of all NATO members of the UN Security Council as well as of the entire Alliance by way of a statement by NATO Secretary General Jens Stoltenberg.

Some legal experts have already speculated that the UK's room for manoeuvre in terms of undertaking such countermeasures may be constrained by its obligations under international law, and that these may also limit NATO's actions.[19] It is thus appropriate to ask what NATO could and should do in response to the new and more complex threat picture we have seen unfold in recent months and years. Is there anything NATO can do about NotPetya-style events at all? What follows *vis-à-vis* Russia after the attribution? Given the specifics of the UK assassination attempt and the statements subsequently made by the British prime minister and the NATO Secretary General, should such new and uncharted waters in international relations be left to individual, directly concerned Allies, or involve the entire Alliance and eventually its whole deterrence posture?

To some extent, the discussion is not new, as it is reminiscent of the aftermath of the cyberattacks against Estonia in 2007. At that time, however, NATO had far less expertise in cyber affairs than it has today. What have changed are the speed and possible effects of cyberattacks, leaving essentially no target immune. The perpetrators of so-called APTs, too, have gained a lot of experience over time. While the fairly

---

16. Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 billion in Revenue", *Cybereason*, November 9, 2017, https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

17. An example of the official attributions, by the United States can be read on the White House website: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

18. Gordon Rayner, "Theresa May's Ultimatum to Vladimir Putin: Russian Leader Given 24 Hours to Answer for Nerve Agent Attack on Spy," *The Times*, March 13, 2018.

19. "Only states that are injured may impose countermeasures: This means that a victim state's allies may not impose 'collective countermeasures' on the wrongdoing state if only the victim state was actually injured." Ashley Deeks, "Prime Minister May's Use-of-Force Claim: Clarifying the Law That Governs the U.K.'s Options', *Lawfare*, March 13, 2018, https://lawfareblog.com/prime-minister-mays-use-force-claim-clarifying-law-governs-uks-options

quick formal attribution on NotPetya (7-8 months, considering the technical, legal and political complexity and the demonstrated concerted action by governments, is in general not too long) can be considered a success story, the follow-up towards Russia has not been as clear.

NATO responses and limits

To try to respond to those questions, it is worth taking a closer look at some of the critical issues that shape NATO's cyber posture. Today, NATO needs to deal with at least the following real-time challenges in regard to cyber:

- A new type of a hyperconnected world and a rapidly evolving online threat environment where, to quote a modern proverb, 'we are all virtual neighbours'. In this new cyber threat landscape, geography, physics and distances, which still continue to play a major role in conventional warfare, do not have the same significance. In cyberspace, NATO has no geographic depth. At the same time, in an increasingly complex cyber world, new 'Fulda' or 'Suwalki Gaps'[20] – or, for example, unpatched zero-day vulnerabilities in tech talk – can be quick to emerge in cyberspace.

- The proliferation of increasingly complex cyberattacks: by now, there really are no limits to what might constitute a cyber weapon and how it could be used. While it is necessary, as suggested by the Estonian Foreign Intelligence Service in its 2018 Yearbook,[21] to also 'continue to be attentive to North Korean ransomware and other means of financial frauds, and Chinese industrial espionage', the main cyber threat to NATO as such will likely continue to be posed by Russia. The Estonian document – remarkable in itself as probably the first instance of the secret service of a NATO country making its cyber threat assessments public – highlights that 'Russia emphasises the importance of cyber warfare and espionage as equal to the conventional military capability. In doing so, Russia has become one of the world's leading players in the field of cyber espionage'.[22]

- The resurgence of an old enemy who, despite having lost the overall technological and arms race with the West in the 1980s, has continued to develop its offensive skills and has never lost the competitive edge it always enjoyed in the domain of applied sciences.

- Today's NATO Command Structure (NCS) is almost a decade old, designed in 2009 during the heyday of joint out-of-area operations in Afghanistan, Iraq and other theatres of war outside of NATO territory.[23] As a result, NATO has demonstrated commendable power projection capacity, such as rapid deployability of forces and mission sustainability, as well as conducting exercises in all parts of the Alliance. At the same time, today the NCS has no 'one-stop-shop' for cyber expertise. The NATO Communications and Information Agency (NCIA) and the NATO CCDCOE, neither of which are a part of the NCS, are but two examples of NATO's permanent and structural commitment to dealing with cyber defence. Only in November 2017 (a year and 4 months after the Warsaw Summit) did NATO's defence ministers agree to launch a cyber operations capability at the Supreme Headquarters Allied Powers in Europe (SHAPE) and it will take time before it becomes fully operational.

---

[20] For more information, see e.g. Zamira Rahim, "The Suwalki Gap: The Most Vulnerable Stretch of Land in Europe", Time Magazine, March 15, 2017, http://time.com/4675758/suwalki-gap-europe-photos/

[21] Estonian Foreign Intelligence Service, International Security and Estonia 2018, https://valisluureamet.ee/pdf/raport-2018-ENG-web.pdf .

[22] Ibid.

[23] The NATO Command Structure is currently under review. "NATO Defence Ministers Take Decisions to Strengthen the Alliance", NATO, February 15, 2018, https://www.nato.int/cps/en/natohq/news_152125.htm

What are the next steps for NATO?

Against this challenging background, what should the Alliance do?

First, there needs to be a clear understanding within the Alliance of how cyber fits into its overall deterrence posture. Negative attitudes surrounding this issue are frequently expressed in statements like 'deterrence will not work in cyber' and 'a cyberwar will not take place'. Of course, it is to be hoped that no adversary will seek to provoke NATO in an endeavour to test the credibility of its deterrence posture all the way to the nuclear option. At the same time, however, the 2014 Wales statement on Article V's applicability (a discussion born from the attacks on Estonia already carried out in 2007) to what occurs in cyberspace did not stop North Korea from spreading its WannaCry malware or Russia from interfering in the US elections or spreading the NotPetya ransomware.

Designing a cyber deterrence posture will require identifying how and where NATO works best for its Allies as a provider of practical cyber capabilities. Nations themselves are by definition responsible for their own cyber resilience while they may also be owners of offensive cyber capabilities. At the same time the EU can provide a platform for, for example, exchanging information and forging a consensual 'soft' response to malicious cyber activities such as imposing sanctions or travel restrictions on the responsible nations and individuals. Officials in the Alliance capitals might wish to consider when and how NATO will be called to action, as in the domain of cyber NATO's collective defence guarantee might need to be activated more quickly than in the other domains.

Secondly, cyber would need to fully become part and parcel of NATO's 'war machine'. No military conflict in the future will be fought without including cyber and/or electronic warfare as part of the plan of campaign. On the other hand, it cannot be ruled out that cyber offences could acquire lethal effects, thereby inducing nations to exercise their right to resort to kinetic self-defence and countermeasures. Therefore, while NATO today conducts exercises at all levels of its military structure to deal with military threats, the focus of its cyber defence exercises could and should try more to integrate the worlds of war and peace, defend both military and civilian critical infrastructure and train participants in both technical skills and strategic level decision-making. A good example to follow could be the NATO CCDCOE's cyber defence exercise *Locked Shields*. It is important to recognise that insight into and knowledge of offensive cyber capabilities is essential to ensure effective defence against cyber threats and attacks.

Thirdly, NATO's particular advantage in cyber defence could stem from cooperation with its partner countries and with other international organisations, especially the European Union. Neither the Alliance nor the Union is an island on its own when it comes to cyber threats and vulnerabilities. The EU can do a lot in areas that are relevant for NATO, such as cybersecurity certification of devices imported into and used in European markets. Dependence on non-EU and non-NATO software could become a critical national security concern, as illustrated by for instance the Kaspersky case in the US.[24] As highlighted by the recent attributions, there could be a global will for cooperation between NATO and non-NATO countries as any of them could become a target, as well as a bridgehead for further spreads of malicious cyber activities, as demonstrated by the WannaCry and NotPetya attacks.

Finally and as food for thought – NATO has partnership agreements on different levels with around 70 countries, whereas the EU has a total of 139 delegations whose mission is to represent the EU and its citizens in forging relations with other countries and organisations from around the world. These could become useful when considering that at least since the Estonian Presidency the EU, according to the so-called Cyber Diplomacy Toolbox, deems it critical to liaise with countries where malicious cyber activities might originate.[25] At the end of the day, to effectively address a global problem it is imperative to collaborate with likeminded partners around the world and it is clear that the two organisations can fruitfully complement each other in this regard.

---

24. "Trump Signs into Law U.S. Government Ban on Kapersky Lab Software," *Reuters*, December 12, 2017, https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4

25. For a useful brief read on the Toolbox, see Katriina Härmä and Tomaš Minarik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox," CCDCOE, September 18, 2017, https://ccdcoe.org/european-union-equipping-itself-against-cyber-attacks-help-cyber-diplomacy-toolbox.html

CHAPTER 10

Protecting and defending Europe's cyberspace

Patryk Pawlak

Ukrainian Constitution Day in 2017 was not just a day for celebration. On 27 June, several networks critical for the functioning of Ukraine's public services – including the Central Bank of Ukraine, the Kyiv metro, the international airport, and the radiation monitoring system at the Chernobyl nuclear plant – were hit by yet another malware attack named 'NotPetya'. The malware spread quickly across the world, infecting more than 12,500 computers in at least 65 countries, including in the European Union.

This episode clearly demonstrates that building resilience against digital threats is not only a technological challenge but also a political one. The very nature of the cyber domain facilitates this process: cyber armies do not need to be moved across borders; cyber weapons can be purchased on the darknet relatively cheaply; and the application of international law to cyberspace and norms of state behaviour is still contested. With geography and distance no longer offering security from criminals and enemies, the digital walls of Europe are under constant attack from state and non-state actors alike.

Whereas the primary responsibility for national security – including in cyberspace – lies with individual member states, the EU has demonstrated that it can and does add value in this domain, primarily through bolstering capacities, law enforcement cooperation, and strengthening international coalitions. Faced with mounting pressure and growing expectations on the part of EU citizens,[1] the European Commission has proposed several initiatives that aim to increase the cyber resilience of all member states, eliminate the weakest links, and strengthen Europe's resilience. Internally, the EU has reinforced its institutional set-up and legal frameworks to counter cyber threats. In addition, the EU's international engagement – through the EU institutions and member states – promotes EU values and stability in cyberspace through developing norms of responsible state behaviour, assuring respect for existing international law, promoting confidence-building measures (CBMs), and supporting cyber capacity building in partner countries.

---

[1] European Commission, "Europeans' Attitudes Towards Cyber Security," *Special Eurobarometer*, Report 464a, June 2017, https://ec.europa.eu/digital-single-market/en/news/special-eurobarometer-europeans-attitudes-towards-cyber-security

There are, however, limits to what can be achieved within the existing institutional set-up. As demonstrated by the NotPetya case, collective attribution is still a hotly debated issue among the member states, despite ongoing initiatives undertaken by the European External Action Service (EEAS) aimed at closing the existing gap in the understanding of issues linked to attribution and operational capacities to attribute malicious activities. Several legislative measures proposed by the Commission also depend on the Council and European Parliament reaching common positions in a timely fashion in order to avoid any delays in their implementation.

The aim of this chapter is to provide an overview and scrutinise steps that have been taken by the European Union and its member states to increase resilience and deter digital threats, including those allegedly originating from Russia.

Taming kittens, pandas and bears

Malicious activities against the networks of the EU institutions and member states are now the new normal. Over the past several years, the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT EU) has reported several attacks by state and non-state actors alike – often bearing innocent-sounding names like ‘pandas’ or ‘kittens’ (see Figure 3). Their aim is to challenge the EU’s interests at home (e.g. via cyber disruption, espionage, hacktivism, and the propagation of radicalisation and violent extremism online) and abroad (e.g. via cyber operations conducted against EU’s partners and allies). The threat comes in many shapes and from numerous directions:

- In January 2018, open sources reported multiple Distributed-Denial-of-Service (DDoS) attacks against Dutch financial institutions including ABN Amro, ING, Rabobank, and the Dutch tax office.[2] The Dutch single sign-on service, DigiD, and the Ministry of Infrastructure and Water Management were also disclosed as victims of these attacks.

- Threat actors like APT28 and Turla are suspected of having repeatedly targeted foreign affairs and security entities in the European Union.[3] In their annual security environment assessment for 2018[4] the Estonian Foreign Intelligence Service – which also hosts the National Communications Security Authority – linked APT28 to the Russian military intelligence GRU, Snake (Turla) to the Federal Security Service FSB, and APT29 to the FSB and the foreign intelligence service SVR.

---

[2] Laurens Cerulus, “Dutch Tax Authority, Banks Face Coordinated Cyberattack,” *Politico*, January 29, 2018, https://www.politico.eu/article/dutch-tax-authority-banks-under-cyberattack/

[3] See for instance: FireEye, “APT28: A Window into Russia’s Cyber Espionage Operations,” Special Report, 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html

[4] Estonian Foreign Intelligence Service, International Security and Estonia 2018, https://valisluureamet.ee/pdf/raport-2018-ENG-web.pdf.

- Throughout 2017 and 2018 the information systems of organisations dealing with European defence (military data) and foreign affairs (embassies, think tanks) were targeted by several actors likely based in China and Russia. For instance, UK think tanks specialising in international security and defence issues were hacked by China-based groups in 2017, according to the Crowdstrike cybersecurity company, who also said it investigated the breaches.[5]

- The Turkish hacker team 'ZoRRoKin' is responsible for opportunistic defacement attacks against EU domains.[6]

Addressing such malicious activities is challenging, primarily due to the difficulties with attribution. 'False flags'[7] are becoming a standard part of the toolkit for nation-state hackers. Instead of simply hiding their identity, they paste a new, invented and borrowed one over it. Russian hackers in particular have lately experimented with such devious 'digital mask-swapping' techniques. Olympic Destroyer – a malware associated with attacks during the 2018 PyeongChang Winter Olympics – has been simultaneously attributed by different cybersecurity researchers to North Korea, Russia and China.[8] Eventually, such tactics undermine efforts towards more credible attribution and increase the risks of misinterpretation and escalation of conflicts in cyberspace, which further highlights the need for adequate digital forensics capabilities. In order to contribute to reducing the risk of unintended miscalculation and escalation, the EU has been an active supporter of the processes led by the ASEAN Regional Forum (ARF) and Organisation for Security and Cooperation in Europe (OSCE) aimed at the development of confidence-building measures (CBMs).

Protecting digital societies

As a consequence of growing digitalisation, the risks to European societies have increased. The last five years have clearly demonstrated the extent to which cybercrime (e.g. ransomware, online fraud), attacks on critical infrastructure (e.g. energy plants in Germany, transportation networks in Sweden), or online disinformation – also known as information manipulation – can all have a dramatic impact on the proper functioning of societies.

---

[5] Gordon Corera, "UK Think Tanks Hacked by Groups in China, Cyber Security Firm Says," *BBC,* February 28, 2018, https://www.bbc.com/news/uk-43172371

[6] Janene Pieters, "Turkish Hacker Groups Focus Cyberattacks on Dutch Websites," *NL Times*, March 14, 2017, https://nltimes.nl/2017/03/14/turkish-hacker-groups-focus-cyberattacks-dutch-websites-incl-nl-times

[7] A false-flag is a diversionary or propaganda tactic that consists of deceiving an adversary into thinking that an operation was carried out by another party. See: Mauno Pihelgas, ed., *Mitigating Risks Arising from False-flag and No-flag Cyber Attacks*, NATO Cooperative Cyber Defence Centre of Excellence, 2015.

[8] See for instance: Andy Greenberg, "'Olympic Destroyer' Malware Hit Pyeongchang Ahead of Opening Ceremony," *Wired*, December 2, 2018, https://www.wired.com/story/olympic-destroyer-malware-pyeongchang-opening-ceremony.

Consequently, the EU's approach has evolved to include a mix of instruments focused on security of critical infrastructure, integrity and freedom of democratic institutions and processes, as well as protection of personal assets and information.[9] The 2017 Joint Communication on Resilience, Deterrence and Defence – a document complementing the 2013 EU Cybersecurity Strategy – embraced these strategic challenges under three broad objectives: building EU resilience to cyberattacks based on a 'collective, wide-ranging approach', creating effective cyber deterrence by putting in place credible measures to dissuade criminals and hostile states, and strengthening international cooperation to promote global cyber stability.[10]

FIGURE 3 | Malicious activities

China

●●●●● ●●●● **9 groups**

APT1
code name: Unit 61398, Comment Crew
Information technology, aerospace, public administration, satellites and telecommunications, scientific research and consulting, energy, transportation, construction and manufacturing, etc.

APT3
code name: UPS Team
Aerospace and defence, construction and engineering, high tech, telecommunications, transportation

APT10
code name: Menupass Team
Construction and engineering, aerospace, and telecom firms, and governments in the US, Europe, and Japan

APT12
code name: Calc Team
Journalists, government, defence industrial base

APT15
code name: Ke3chang, Mirage, Metushy, Vixen Panda
Government ministries across Europe

APT16
Japanese and Taiwanese organisations in the high-tech, government services, media and financial services industries

APT17
code name: Tailgator Team, Deputy Dog
US government, and international law firms and IT companies

APT18
code name: Wekby
Aerospace and defence, construction and engineering, education, health and Biotechnology, high tech, telecommunications, transportation

APT30
Members of the Association of Southeast Asian Nations (ASEAN)

---

[9] The Commission Communication on the EU Strategic Approach to Resilience defines resilience as 'the ability of an individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks'.

[10] European Commission, «Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU,» Join (2017) 450 final, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

Russia

●●● **3 groups**

APT28

code name: Fancy Bear, Sofacy, Pawn Storm, Tsar Team

The Caucasus, particularly Georgia, eastern European countries and militaries, NATO and other European security organisations and defence firms

APT29

code name: Cozy Bear, the Dukes

Targeted intrusions against the US Democratic National Committee

Western European governments, foreign policy groups and other similar organisations

code name: Turla, Snake, Uroburos, Venomous Bear

Likely campaign against federal institutions in Germany, including the Foreign Ministry

North Korea

●●● **3 groups**

APT37

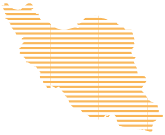
code name: Reaper, Group123, ScarCruft

Primarily South Korea – though also Japan, Vietnam and the Middle East – in the chemicals, electronics, manufacturing, aerospace, automotive and healthcare sectors

code name: Lazarus, BlueNoroff, Hidden Cobra

Suspected group behind the Sony hack

Iran



●● **2 groups**

APT33

Multiple industries – headquartered in the United States, Saudi Arabia and South Korea

APT34

Variety of industries, including financial, government, energy, chemical, and telecommunications in the Middle East

code name: Charming Kitten, Flying Kitten

Individuals of interest to Iran in the fields of academic research, human rights and media

Data: EUISS, 2018.

Critical information infrastructure

Reports of attacks on critical infrastructure are increasing in scope and frequency. For instance, in March 2018, the US CERT (under the Department of Homeland Security) together with the FBI issued a joint Technical Alert that provided information on a Russian threat actor (DragonFly) targeting US government entities as well as organisations in the energy, nuclear, commercial, water, aviation, and critical manufacturing sectors since at least March 2016. Similar activities were observed across the EU.

In an effort to ensure a minimum level of preparedness across the EU, the Network Information Security (NIS) Directive requires each member state to adopt a national strategy on the security of network and information systems, including measures to ensure high levels of security in critical sectors such as banking, energy, transportation, healthcare or digital infrastructure, as well as a governance framework, a list of actors tasked with the implementation of the strategy and a risk assessment plan.

Furthermore, each member state is expected to designate a Computer Security Incident Response Team (CSIRT) and provide adequate resources for cross-border cooperation. In an effort to stimulate strategic and operational cooperation among EU stakeholders, the NIS Directive also established a NIS Cooperation Group and CSIRT network. In addition, given the potential wide-ranging impact of cyber incidents and crises, in 2017 the European Commission proposed a set of measures that form a cooperation framework for the Union in the event of large-scale incidents and crises. The so-called Blueprint for providing 'an effective process for an operational response at Union and member state level to a large-scale cyber incident', endorsed by the Council in June 2018, describes the objectives and modes of cooperation between the member states and the EU institutions, bodies and agencies in specific cases and scenarios that will be tested during the crisis-management exercises.[11]

Democratic infrastructure

The experience of the United States and several European countries with alleged Russian interference in or attempts to influence the outcome of their national elections have elevated the protection of democratic institutions and processes into an international issue.[12] While disinformation often relies on the information obtained through hacking databases, email accounts or other information sources, it is the weaponisation of such information for the purpose of large-scale disinformation that poses a danger to free and fair electoral processes. In that context, the 2019 European Parliament elections will be an important test case. A frequently low degree of participation[13] and the local nature of the European election campaigns makes them more fragmented, which in turn allows for more targeted, contextualised, and convincing disinformation. A low turnout-low investment-high stakes combination potentially makes the 2019 elections an attractive target: their outcome will influence the EU's institutional set-up and might change the future direction of the Union's crucial foreign and security policy decisions – including the EU's position on bilateral relations with Russia.

Considering the negative impact of such measures on trust in democratic institutions and citizens' ability to take informed and free decisions, the European Commission published the Communication on Tackling Online Disinformation in April 2018. The Communication called for an EU-wide Code of Practice on Disinformation, the creation of an independent European network of fact-checkers and the support of member states in ensuring the resilience of elections against cyber threats.[14] The NIS

---

[11] Council of the European Union, "Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises," June 26, 2018, http://data.consilium.europa.eu/doc/document/ST-10086-2018-INIT/en/pdf

[12] It is worth noting that many of the problems linked to the security of election systems, for instance, had been addressed already in 2013 in the OSCE ODIHR's Handbook for the Observation of New Voting Technologies.

[13] The 2014 elections witnessed the lowest turnout since 1979 with an average turnout of 42.54%, but as low as 25% in some of the countries in Central and Eastern Europe.

[14] European Commission, "Communication on Tackling Online Disinformation: a European Approach," COM(2018) 236 final, April 26, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

Cooperation Group[15] engaged in the mapping of existing European initiatives on the cybersecurity of network and information systems used for electoral processes and in July 2018 delivered a compendium of practical recommendations and measures to secure election life-cycles.[16]

Societal infrastructure

Despite extensive discussions about the political consequences of malicious operations, practice shows that criminal justice and law enforcement instruments remain the most effective way of punishing the perpetrators.[17] This is particularly relevant in a context where the 'crime-as-a-service' model of cybercrime is gaining in popularity, with various elements of criminal infrastructure and services available for purchase on the darknet. Several reports suggest that some of the online organised groups operating in such markets are connected to the Russian government.[18]

In an effort to adapt to a rapidly evolving digital and data-driven environment as well as to minimise the potential negative consequences of cyberattacks, the EU has taken steps to increase the cost of operations for cyber criminals – both in terms of financial costs and circumscribing their activities. The 2013 Directive on Attacks Against Information Systems, for instance, introduced minimum standards in the definitions of criminal cyber offences and corresponding sanctions. In 2018, the European Commission has proposed legislation to facilitate and accelerate law enforcement and judicial authorities' access to electronic evidence through the introduction of the European Production Order and the European Preservation Order.[19] It is expected that these two instruments will significantly strengthen the existing European Investigation Order and the Mutual Legal Assistance agreements.

Furthermore, the EU has strengthened its data protection regime. The General Data Protection Regulation (GDPR) in force since May 2018 imposes a breach notification requirement that obliges any company or institution processing personal information to notify the relevant authorities within 72 hours of any data breach that is likely to result in a risk to the rights and freedoms of individuals. This is particularly relevant in the context of election interference as it implies, for instance, that any potential breach to the databases of electoral campaign teams will need to be notified rather than kept secret out of fear of incurring reputational damage.

---

[15] See: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[16] NIS Cooperation Group, *Compendium on Cyber Security of Election Technology*, CG Publication 03/2018, July 2018.

[17] In February and July 2018, the US Department of Justice publicly released an indictment accusing Russian companies and citizens of influence operations targeting the political process of the United States.

[18] See for instance: John Leyden, "Russia is Struggling to Keep its Cybercrime Groups on a Tight Leash," *The Register*, June 6, 2017, https://www.theregister.co.uk/2017/06/06/russia_cyber_militia_analysis/

[19] European Commission, "Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters," COM(2018) 225 final, 17 April 2018.

Strengthening resilience of partners and allies

The EU recognises that its vulnerability derives in part from the weak links in its security environment. Several intelligence and media reports suggest that Russia is actively involved in malicious operations against EU's partners and allies in Ukraine, Georgia or the Western Balkans. Consequently, cyber capacity building in partner countries and regions has become one of the strategic building blocks of the EU's cyber diplomacy.[20]

The specific actions taken by the EU aim at building the foundations of cyber resilience, including through support for development of national cybersecurity strategies and policies, establishing or reinforcing national Computer Emergency Response Teams (CERTs), and putting in place national systems for effective cyber crisis management.[21] The Global Action on Cybercrime Extended (GLACY+) – one of the EU's flagship projects implemented jointly with the Council of Europe – offers assistance in developing policies, strategies, and strengthening law enforcement and criminal justice legal frameworks in third countries.[22] Furthermore, the EU has launched a number of projects focused specifically on increasing the resilience of critical information infrastructure and networks supporting the vital services of selected priority countries worldwide, including the ENCYSEC project (Enhancing cybersecurity, protecting information and communication networks) and the CB4CyberResilience project (Capacity Building and Cooperation to enhance Cyber Resilience).

In addition, the Joint Communication on the ENP Review prioritises the Eastern partners in the area of cybersecurity and cybercrime.[23] Under the umbrella of the Support Group of Ukraine (SGUA), the EU has implemented a series of TAIEX[24] actions using the expertise of member states to assist Ukraine to strengthen its cybersecurity capacity for the protection of critical infrastructure. Their focus is primarily on establishing an appropriate legislative framework and implementable strategy, developing public-private partnerships and organisational aspects in national cybersecurity, and strengthening the technical ability and skills of CSIRTs.[25] At the same time, the EU initiatives on cybercrime aim to support the adoption of the standards proposed in the Council of Europe Convention on Cybercrime (the Budapest Convention) and focus, *inter alia*, on improving mutual legal assistance for international cooperation and electronic evidence, strengthening the role of 24/7 points of contact, and promoting practical measures for public-private partnerships.[26]

---

[20] Council of the European Union, "Council Conclusions on EU External Cyber Capacity Building Guidelines," 10496/18, June 26, 2018.

[21] Patryk Pawlak and Panagiota Nayia Barmpaliou, "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity," *Journal of Cyber Policy* 2, no. 1 (March 2017): 123-144.

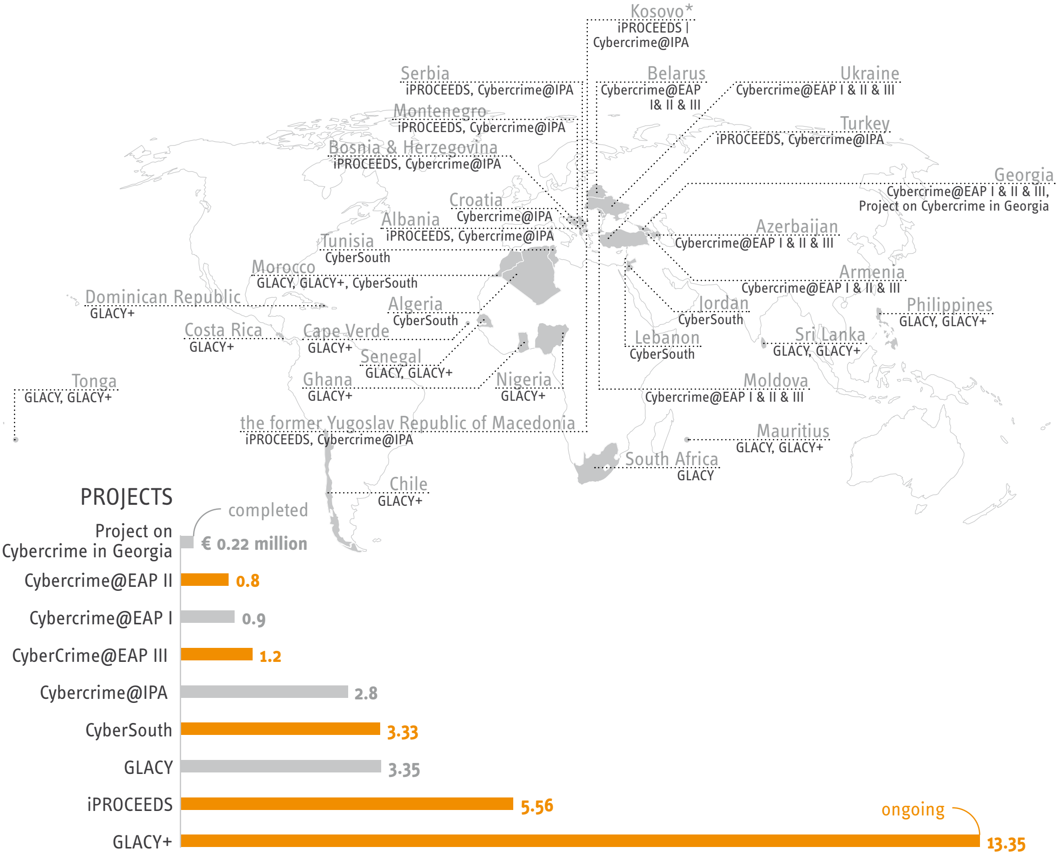
[22] Patryk Pawlak, "Cyber Resilience," in *After the EU Global Strategy - Building Resilience*, ed. Florence Gaub and Nicu Popescu (Paris: EU Institute for Security Studies, 2017), 17-20.

[23] European Commission, Joint Communication on Review of the European Neighbourhood Policy, Join (2015) 50 final, November 18, 2015, http://eeas.europa.eu/archives/docs/enp/documents/2015/151118_joint-communication_review-of-the-enp_en.pdf

[24] TAIEX is the Technical Assistance and Information Exchange instrument of the European Commission. TAIEX supports public administrations with regard to the approximation, application and enforcement of EU legislation as well as the sharing of EU best practices towards the countries under the EU neighbourhood policy and the countries engaged in enlargement negotiations.

[25] Efforts at strengthening Ukraine's cyber capacities are also implemented by NATO. See for instance, Patryk Pawlak, "Building Capacities for Cyber Defence," *Issue Alert* no. 26, EUISS, November 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2026%20Cyber%20development.pdf

FIGURE 4 | Cyber-related projects implemented by the Council of Europe with EU funding


Kosovo*
iPROCEEDS | Cybercrime@IPA
Serbia
iPROCEEDS, Cybercrime@IPA
Belarus
Cybercrime@EAP I& II & III
Ukraine
Cybercrime@EAP I & II & III
Montenegro
iPROCEEDS, Cybercrime@IPA
Turkey
iPROCEEDS, Cybercrime@IPA
Bosnia & Herzegovina
iPROCEEDS, Cybercrime@IPA
Georgia
Cybercrime@EAP I & II & III, Project on Cybercrime in Georgia
Croatia
Cybercrime@IPA
Albania
iPROCEEDS, Cybercrime@IPA
Azerbaijan
Cybercrime@EAP I & II & III
Tunisia
CyberSouth
Morocco
GLACY, GLACY+, CyberSouth
Armenia
Cybercrime@EAP I & II & III
Dominican Republic
GLACY+
Jordan
CyberSouth
Philippines
GLACY, GLACY+
Algeria
CyberSouth
Costa Rica
GLACY+
Cape Verde
GLACY+
Lebanon
CyberSouth
Sri Lanka
GLACY, GLACY+
Senegal
GLACY, GLACY+
Tonga
GLACY, GLACY+
Ghana
GLACY+
Nigeria
GLACY+
Moldova
Cybercrime@EAP I & II & III
the former Yugoslav Republic of Macedonia
iPROCEEDS, Cybercrime@IPA
Mauritius
GLACY, GLACY+
South Africa
GLACY
Chile
GLACY+
PROJECTS
completed
Project on Cybercrime in Georgia
€ 0.22 million
Cybercrime@EAP II
0.8
Cybercrime@EAP I
0.9
CyberCrime@EAP III
1.2
Cybercrime@IPA
2.8
CyberSouth
3.33
GLACY
3.35
iPROCEEDS
5.56
ongoing
GLACY+
13.35

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

Source: European Commission, *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building*, 2018.

Reinforcing international consensus

International engagements have also become an important element of the EU's response to malicious cyber activities. As stated in numerous Council conclusions, the primary objective of EU policy is to support and promote 'a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of our free and open societies'. The EU also maintains that 'international law, including international conventions such as the Council of Europe Convention on Cybercrime and relevant conventions on international humanitarian law and human rights (…) provide a legal framework applicable in cyberspace.'[27] There is, therefore, a clear divergence of views between the EU and Russia, as Moscow not only pursues policies limiting access to a free and open internet at home and curbing the freedom of expression, but also promotes the idea of two new international legal instruments: one to tackle cybercrime (Russia has not signed the Budapest Convention) and the other to regulate state relations in the cyber domain (modelled on the Code of Conduct proposed to the United Nations by the Shanghai Cooperation Organisation).

---

[26] Author's interview with a European Commission official.

The EU has taken several steps to promote its vision of cyberspace internationally. The 2015 Council conclusions on cyber diplomacy elaborate the EU's position on a range of issues such as norms of responsible state behaviour, internet governance, global competitiveness or the promotion and protection of human rights online.

Simultaneously, the EU has been working on strengthening international response and deterrence capacities. In 2017, the member states agreed to develop a joint EU diplomatic response to malicious cyber activities, the Cyber Diplomacy Toolbox, accompanied by the implementing principles and follow-up activities focused on attribution of malicious cyber incidents. Options for action range from statements by the Council or the High Representative, to Council conclusions and adoption of restrictive measures, among others.[28] Finally, the EU has also developed a Cyber Defence Policy Framework for cyber protection of the CSDP missions and operations, and encourages cooperation between member states through projects implemented in the framework of the Permanent Structured Cooperation (PESCO).[29] Closer strategic cooperation with NATO has been initiated in 2016 via a EU-NATO cyber defence information-sharing agreement.

In April 2018, the Council of the European Union adopted conclusions on malicious cyber activities which stressed that 'the use of ICTs for malicious purposes is unacceptable as it undermines [the EU's] stability, security and the benefits provided by the Internet and the use of ICTs'. Even though the document did not explicitly attribute NotPetya to Russia – although several EU member states have done so unilaterally – it recalls the EU's established view that existing international law applies to cyberspace. More importantly, it incorporates into the EU's *acquis* two norms proposed by the UN Group of Governmental Experts, namely that (a) states must not use proxies to commit internationally wrongful acts using ICTs, and should ensure that their territory is not used by non-state actors to commit such acts; and (b) states should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for malicious activities involving ICTs.

---

[27] European Commission, "Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU," Join (2017) 450 final, September 13, 2017.

[28] Council of the European Union, "Council Conclusions on Cyber Diplomacy," 6122/15, February 11, 2015, http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

[29] For instance: the 'Cyber Threats and Incident Response Information Sharing Platform' project will develop more active defence measures, potentially moving from firewalls to more active measures; Cyber Rapid Response Teams (CRRTs) will allow member states to help each other to ensure a higher level of cyber resilience and to collectively respond to cyber incidents.

Building a malware-proof construction

The EU Global Strategy reaffirmed the EU's intention to be a 'forward-looking cyber player' with the focus on protecting critical assets and promoting a free and secure global Internet. To fully achieve that objective, the whole-of-society and whole-of-government approaches cannot be just a bumper sticker but need to be fully embraced through concrete policies and matched with adequate resources – in terms of budgets, manpower and political leadership. This can be achieved through a reinforced effort in the following five areas:

1. **Building the culture of cyber resilience by promoting cyber hygiene and awareness-raising at all levels of society and across governments**. This goes beyond initiatives focused on improving digital skills, training or adopting standards to ensure that awareness of digital risks, vulnerabilities and potential countermeasures becomes part of the DNA within institutions, companies, and among the individual users, including by developing proper risk analysis and mitigation strategies.

2. **Reinforcing joint action and deterrence capabilities through further work on operationalising the concept of attribution and an EU cyber sanctions regime** in the framework of the EU Cyber Diplomacy Toolbox. While attribution and possible countermeasures are a national competence, a better mutual understanding of the methodology and processes guiding the decision-making processes in each of the member states is required for more effective collective attribution and cooperation at the EU level, in particular with regard to the imposition of the restrictive measures.[30] Concrete initiatives could also focus on strengthening digital forensics capacities and methods.

3. **Building confidence and trust between states by improving transparency on the member states' practice and approach to the application of the existing international law in cyberspace**. This can be achieved by making public and clarifying national laws, doctrines and strategies adopted by individual countries. Eventually, this would contribute to the emergence of a common strategic cyber culture among the EU member states, as has been the case in other security domains.

4. **Strengthening global cyber resilience through partnerships with other international and regional organisations** (OSCE, NATO, AU, World Bank) as well as the private sector. The initiatives within the OSCE and ARF – where Russia is also a participating

---

[30] For instance, only a few states – UK, US, Canada, Australia, New Zealand and Denmark – publicly attributed the destructive NotPetya cyberattacks to Russia.

state – might prove particularly useful in clarifying positions and resolving conflicts, in particular through further work on measures and mechanisms increasing transparency in the cyber domain.

5. **Supporting alternative venues for dialogue on cyber-related issues**, including through building on the already existing **track 2.0 engagements** such as the Trianon Dialogue[31] or establishing new formats for informal exchanges between experts.

---

[31] A permanent structure for fostering interaction between French and Russian civil societies established in 2017.

Conclusion: Russia – from digital outlier to great cyberpower

Nicu Popescu and Stanislav Secrieru

Currently the world appears to be in the grip of 'cyber hysteria'. Formerly perceived as a rarefied issue confined to the domain of specialist 'geeks', cyber seems to have evolved almost overnight into a mainstream political and security preoccupation. Today's headlines are dominated by reports about the rise and fall of cryptocurrencies, the risks posed by increasingly sophisticated cyberattacks, great powers' investments in cyber capabilities, ongoing 'crypto wars' and the coming dominance of Artificial Intelligence (AI). Cyber concerns have in recent years become increasingly prominent in (geo-) politics too. These days no major political speech or high-level diplomatic meetings can take place without mentioning or debating cyber challenges. Governments and international bodies are busy drafting documents to address diverse facets of cybersecurity and how the challenge should be tackled. While the alarm about threats emanating from cyberspace and from cyber-related vulnerabilities is justified, the surprise is not. People tend to think of cyber challenges as something new. But in fact the phenomenon is not that new.

In April 1965 *Time* magazine ran a cover story entitled 'The Cybernated Generation' reflecting on emerging vulnerabilities stemming from society's growing reliance on computers. In this pre-cyber world a doomsday scenario of what would happen if the Western world were suddenly to experience a massive computer breakdown was evoked.[1] However, in the 1960s such anxieties were overshadowed by the nuclear arms race and the spectre of total annihilation which the use of nuclear weapons could bring about. But as the world embraced the age of the internet in the late 1990s, with the emergence of new computer devices and innovative technologies, cybersecurity challenges made the headlines again. Concern about weapons of mass destruction among the expert community and wider public was now matched by concern about cyber as a 'weapon of mass disruption.'[2]

In recent years a series of cyberattacks orchestrated by Russia has raised awareness internationally about how cyber tools can be employed in malign ways. This has shifted the cybersecurity debate away from concerns about technological risks to worries about human-induced cyber disruptions that can have direct, immediate and substantial repercussions across a whole range of domains, ranging from the safety of electoral processes to the West's capacity to use its sophisticated military arsenals.

---

[1] Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld & Nicholson, 2015), 67-68.

[2] Fred Kaplan, *Dark Territory. The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 52.

The rise of a great cyber power

Post-Soviet Russia was plunged into chaos in the 1990s, as economic shock therapy, hyperinflation, deepening poverty and rampant organised crime took their toll on Russian society. Few could have imagined that in the midst of such sharp economic decline and social crisis Russia would find the resources to invest in cutting-edge cyber tools. But it did.

In March 1998, the US military discovered that unidentified hackers had infiltrated computers at the Wright-Patterson Air Force Base in Ohio and downloaded sensitive R&D files. The attack was nicknamed 'Moonlight Maze' and it transpired that the hackers had managed to steal 5.5 gigabytes of data. The NSA experts who monitored the hackers' moves in real time were awed by the sophistication of the operation. To trap the culprit they set up an elaborate 'honey pot', which would enable them to attribute the attack with a high degree of precision. The cyber trail led them to an IP address which hosted the Russian Academy of Sciences in Moscow. One month later, a US delegation travelled to Moscow to clarify the matter. A high-ranking military official confirmed the hack, blaming Russia's intelligence services.[3]

By the late 1990s, Russia had no need to recruit hackers from elsewhere (as it did back in 1986): it was able to rely on indigenous skills and resources to hack the most advanced cyber nation itself. The technological gap which was supposed to shield the West from economically and technologically backward players in the cyber domain had vanished. From this point on, the instances of Russia-initiated or guided cyberattacks against Western powers and the post-Soviet states increased exponentially.

The cyber escalation ladder

Throughout the 2000s and 2010s Russia sought to establish itself as a 'great cyber power'. In this respect its status rests on two pillars. Firstly, Russia significantly boosted its cyber capabilities, be it within state agencies or through the co-optation of 'rogue' criminal cyber actors and private IT companies, resulting in a diffuse complex network.[4] In the 1980s the Soviet Union recruited non-state actors because it lacked hacking skills and expertise. In the 2000s Russia possessed know-how but often hired the services of non-state actors (closely linked to law enforcement institutions) in order to be able to hide behind the mask of 'plausible deniability'. Secondly, this mastery of cyber capabilities was matched by a strong political will to use them in a more integrated way both for domestic and foreign policy purposes. Up until the early years of the new millennium Moscow was primarily engaged in cyber espionage, but from the mid-2000s onwards the scope of malicious cyber activities significantly widened.

---

[3] Fred Kaplan, *Dark Territory*, 78-88.

The track record of documented cyberattacks conducted or masterminded by Russia makes it possible to distinguish three levels of cyber-offensive operations. The first level concerns classical intelligence-gathering activities in cyberspace. In this Russia is not alone, nor particularly unique. Plenty of other countries rely massively on cyber intelligence. Certainly, Russia's cyber targets have included a wide array of players such as political parties, law enforcement bodies (e.g. Dutch prosecutors investigating the downing of flight MH17,[5] police officers from Scotland Yard investigating the Skripal poisoning case etc),[6] international sports organisations and even the clergy of the Eastern Orthodox Church.[7] And even if it seems that more is known in the public domain about the presumed targets of Russian cyber intelligence efforts, it is generally assumed that other cyber powers – whether China, the US or some European states – might be less visible, but are probably not much more reticent than Russia about using cyber intrusions for intelligence purposes. What makes Russia somewhat different from other cyber powers is the way in which it operates at two other levels.

Russia is almost unabashed about its integration of cyber intrusions and strategic communications. The data obtained through cyber espionage often feeds the compromised material released ahead of important political or sporting events. A key example is the release by Russian hackers of the medical records of Western athletes stolen from the World Anti-Doping Agency, which happened in the midst of a doping investigation involving Russian sportsmen.[8] Bots and trolls are put to use to distribute 'anonymous leaks', as happened in the 2016 US and 2017 French presidential elections. The primary aim of such manipulative use of information is to draw attention away from Russia's own shortcomings or wrongdoings, discredit foreign politicians, confuse and mislead public opinion, and derail democratic processes abroad. Neither China, the US nor other cyber powers integrate to such an extent information stolen via cyber means into targeted information campaigns that seek to influence elites or the wider public in other countries, especially at election time.

---

[4] Anna Shnygina, "How Russia's War in Georgia Sparked Moscow's Modern-day Recruitment of Criminal Hackers", *Meduza*, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland; Kevin Poulsen, "LEGION OF DOOM – This Hacker Party Is Ground Zero for Russia's Cyberspies", *Daily Beast*, August 3, 2018, https://www.thedailybeast.com/this-hacker-party-is-ground-zero-for-russias-cyberspies-3?ref=scroll

[5] Interview with Dutch diplomat, April 2018.

[6] Robert Mendick, "Russian Cyber Hackers 'Targeted' Police Inquiry into Skripal Nerve Agent Attack", *The Telegraph*, July 16, 2018, https://www.telegraph.co.uk/news/2018/07/16/russian-cyber-hackers-targeted-police-inquiry-skripal-nerve/

[7] Mark Mazzetti and Katie Benner, "12 Russian Agents Indicted in Mueller Investigation", *New York Times*, July 13, 2018, https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html; Sam Thielman, "Same Russian Hackers Likely Breached Olympic Drug-testing Agency and DNC", *The Guardian*, August 22, 2016, https://www.theguardian.com/technology/2016/aug/22/russian-hackers-world-anti-doping-agency-dnc-hack-fancy-bear; Raphael Satter, "Ungodly Espionage: Russian Hackers Targeted Orthodox Clergy", *AP*, August 27, 2018, https://apnews.com/26815e0d06d348f4b85350e96b78f6a8

[8] Jethro Mullen and Ivana Kottasova, "Russian Hackers Release Secret Data of 25 More Olympic Athletes", *CNNtech*, September 15, 2016, https://money.cnn.com/2016/09/15/technology/wada-olympic-athletes-russian-hackers/index.html

The third level of operations targets critical political and economic infrastructure in physical space or cyberspace. Russia's cyberattacks have covered a variety of targets, from voter lists and digital mass-media outlets to government websites, banks, electricity distribution networks, hospitals, airports and maritime transport systems. While Russia has not yet crossed the threshold of cyber destruction (e.g., complete destruction of computer networks, sabotage or physical destruction of pipelines, intentionally provoked industrial incidents involving casualties) its offensive operations in cyberspace have temporarily disrupted services provided by banks, ATMs and airports, as well as electricity supplies, the retail sector, and maritime transportation.[9] Again, Russia is not the only cyber actor that has used cyber tools to target physical infrastructure. Stuxnet – the virus designed to sabotage the Iranian nuclear centrifuges – is also one such tool. But no other power seems to have used cyberattacks as massively and indiscriminately to disrupt real-world processes as Russia did over the past 15 years in Estonia, Georgia or Ukraine.

Russia is undoubtedly one of the world's great cyber powers, armed with a lot of technical skill and expertise, plus the willingness and readiness to act aggressively in cyberspace. This has certainly helped Russia boost its global profile. But in the process Russia has pushed cyber concerns onto the top of decision-makers' agendas in the EU and the US, making cyberspace an ever-more contested domain and thus forfeiting the competitive and strategic advantage that it has hitherto enjoyed in this arena.

---

[9] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Annex

Abbreviations

AI	Artificial Intelligence
ANSSI	French National Cybersecurity Agency (*Agence nationale de sécurité des systèmes d'information*)
APT	Advanced Persistent Threat
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
AU	African Union
BRICS	Brazil, Russia, India, China and South Africa
CBMs	Confidence-building measures
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCNEP	National Commission for the monitoring of the electoral campaign for the presidential election (*Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle*)
CDMA	Cyber Defence Management Authority
CDMB	Cyber Defence Management Board
CERT	Computer Emergency Response Team
CERT EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CIA	Central Intelligence Agency
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CSTO	Collective Security Treaty Organisation
DDoS	Distributed Denial of Service
DNC	Democratic National Committee
DNS	Domain Name System
DoS	Denial of Service
EEAS	European External Action Service
ENP	European Neighbourhood Policy
EW	Electronic Warfare
FAPSI	Federal Agency for Government Communications and Information (*Federalnoye Agentsvo Pravitelstvennoi Svayazi I Informatsii*)
FBI	Federal Bureau of Investigation
FSB	Federal Security Service (*Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii*)

FYROM	Former Yugoslav Republic of Macedonia
GDP	Gross Domestic Product
GGE	Group of Government Experts
GRU	Russian military intelligence agency (*Glavnoye Razvedyvatelnoye Upravlenie*)
HOSG	Heads of State and Government
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
KGB	Committee for State Security (*Komitet gosudarstvennoy bezopasnosti*)
NATO	North Atlantic Treaty Organisation
NCIA	NATO Communications and Information Agency
NCS	NATO Command Structure
NIS	Network Information Security
NSA	National Security Agency
OSCE	Organisation for Security and Cooperation in Europe
R2P	Responsibility to Protect
R&D	Research and Development
RBN	Russian Business Network
RBTH	Russian Beyond The Headlines
RT	Russia Today
SCO	Shanghai Cooperation Organisation
SHAPE	Supreme Headquarters Allied Powers Europe
TAIEX	Technical Assistance and Information Exchange Instrument of the European Commission
UN	United Nations
UNGA	United Nations General Assembly
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Notes on the contributors

Siim Alatalu joined the NATO Cooperative Cyber Defence Centre of Excellence in January 2015 as Head of International Relations. In 2018 he joined the Centre's Strategy Branch, where he is in charge of cyber strategy and policy research and training related to NATO and the EU, as well as providing subject matter expertise to the Centre's other flagship projects. His prior professional career includes several advisory and managerial positions at the Estonian Ministry of Defence since 2001.

Irina Borogan is a Russian investigative journalist, co-founder and deputy editor of *Agentura.ru*, a watchdog that monitors the activities of the Russian secret services. She has co-authored (with Andrei Soldatov) *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (PublicAffairs, 2010) and *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, published in the autumn of 2015 and updated in 2017.

Elena Chernenko is Deputy Head of the international desk at *Kommersant* newspaper (Russia). She is a member of the board of the PIR Center and also a member of the board of the Council on Foreign and Defence Policy (SVOP). Her areas of research interest include cyber diplomacy, non-proliferation and arms control. She holds a PhD in History from the Moscow Lomonossow State University, and has worked in journalism since 2003.

Sven Herpig is the project director of the Transatlantic Cyber Forum (TCF), founded by the German think tank Stiftung Neue Verantwortung in Berlin. His research currently focuses on international cybersecurity policy, including government hacking, vulnerability management, resilience policies and the protection of election infrastructures. He previously worked for Germany's Federal Office for Information Security (BSI) and the information security staff at the Federal Foreign Office.

Oscar Jonsson is a PhD candidate at the Department of War Studies, King's College, London. The subject of his thesis is the Russian understanding of modern warfare. He previously worked as an expert on Russia for the Swedish Armed Forces Headquarters, specialising in 'hybrid warfare' and strategic planning.

Xymena Kurowska is Associate Professor of International Relations at Central European University, Hungary and Marie Skłodowska-Curie Fellow at Aberystwyth University, UK. She received her doctorate on European security from the European University Institute in Florence. Her current research interests include security theory and practice, Russian society and foreign policy, digital propaganda, and norm contestation in cyberspace.

Jarno Limnéll is Professor of Cybersecurity at Aalto University, Finland, and an adjunct professor in three other Finnish universities. He is also the CEO of the IoT infrastructure security firm Tosibox. He has been working on security issues for over 20 years, and has a profound understanding of the global threat landscape. He has published extensively on security issues.

Patryk Pawlak heads the Brussels office of the EU Institute for Security Studies (EUISS). He is currently involved in several projects focused on the EU's external cyber capacity building and cyber diplomacy. Since February 2018, he has managed the EU Cyber Direct project aimed at supporting the EU's cyber diplomacy and resilience-building efforts in six major partner countries (Brazil, China, India, Japan, South Korea, and the United States). In April 2018, he was appointed as a Co-Chair of the Advisory Board of the Global Forum on Cyber Expertise.

Piret Pernik is a Research Fellow at the International Centre for Defence and Security (ICDS). Her research focuses on cybersecurity and cyber defence, digital policy and transformation, societal security, and comprehensive security and defence. She has published on national, NATO, and EU cybersecurity policies and strategies. Before joining ICDS in 2013, she worked at the Estonian Ministry of Defence and served as an adviser to the National Defence Committee of the Estonian Parliament.

Nicu Popescu is Director of the Wider Europe programme at the European Council on Foreign Relations. He was a Senior Analyst at the EUISS from July 2013 until July 2018, where he specialised in Russia and the EU's eastern neighbours. He previously worked as advisor on foreign policy and EU affairs for the prime minister of Moldova (2010, 2012-2013), dealing with foreign policy issues as well as domestic reforms. Prior to this, he worked as head of programme and Senior Research Fellow at the European Council on Foreign Relations in London (2007-2009, 2011-2012), and as a Research Fellow at the Centre for European Policy Studies in Brussels (2005-2007).

Thomas Reinhold is a fellow of the Institute for Peace Research and Security Policy (IFSH) and member of the Research Advisory Group of the Global Commission on the Stability of Cyberspace. He studied computer science and psychology and his main areas of specialisation are software and hardware security in computer networks, software vulnerability and software security concepts as well as software threat analysis. His research has focused in recent years on cybersecurity, threats in cyberspace, and the rising problems of cyberwar and arms control in this domain.

Anatoly Reshetnikov is a PhD researcher and a lecturer at the Department of International Relations of Central European University. His broader research interests include identity politics, conceptual history, linguistic approaches to social analysis, contemporary Russian politics, the concept of responsibility in international relations, and the new institutionalised techniques of political control and resistance, such as political trolling.

Stanislav Secrieru is a Senior Analyst at the EUISS. He was previously a policy analyst at the Open Society European Policy Institute in Brussels, a Partnership for Peace Research Fellow at the NATO Defence College, a Research Fellow with the Study Programme on European Security at the Institute for European Politics in Berlin, and a Senior Research Fellow at the Polish Institute of International Affairs (PISM). He has also worked on research projects addressing political and security developments in the eastern neighbourhood for the European Council on Foreign Relations (ECFR) and Freedom House.

Andrei Soldatov is a Russian investigative journalist, co-founder and editor of *Agentura.ru*, a watchdog that monitors the Russian secret services' activities. He has been covering security services and terrorism issues since 1999. He has co-authored (with Irina Borogan) *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (PublicAffairs, 2010) and *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, published in the autumn of 2015 and updated in 2017.

Jean-Baptiste Jeangène Vilmer is the director of the Institute for Strategic Research (IRSEM, French Ministry for the Armed Forces), after having served as policy officer working on Security and Global Affairs at the Policy Planning Staff (CAPS) of the French Ministry of Foreign Affairs, and in various academic positions (McGill University Faculty of Law, King's College London Department of War Studies). He co-authored the CAPS-IRSEM report on *Information Manipulation* (September 2018).

European Union Institute for Security Studies
100, avenue de Suffren | 75015 Paris | France | www.iss.europa.eu

Publications Office