FANCY BEARS'

Hack Team

#OpOlympics

About us

2016-09-13

Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team. We stand for fair play and clean sport.

We announce the start of #OpOlympics. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw.

ANALYSIS

HACKING FOR INFLUENCE

FOREIGN INFLUENCE ACTIVITIES AND CYBER-ATTACKS

| PIRET PERNIK |

FEBRUARY 2018

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: Hacking for Influence— Foreign Influence Activities and Cyber-attacks
Author: Pernik, Piret
Publication date: February 2018
Category: Analysis

Cover page photo: A screenshot of the Fancy Bears website after its hacking into a World Anti-Doping Agency’s (WADA) database and posting confidential medical data of the US Olympic team members online, Tuesday Sept 13, 2016 (AP Photo/Alexander Zemlianichenko).

Keywords: cybersecurity, cyber-attacks, cyber espionage, information warfare, influence operations, United States of America, Russia

Disclaimer: The views and opinions contained in this paper are those of its author only and do not necessarily represent the official policy or position of the International Centre for Defence and Security or any other organisation.

ISSN 2228-2076

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Introduction

In recent years much academic, policy and journalistic research has been conducted about authoritarian countries' influence activities (whose purpose is to achieve foreign and security policy objectives) in liberal democratic countries.[1] The majority of work primary concerns China and Russia, but also explores countries in Asia, the Middle East and Africa.[2] All nation-states – democratic and authoritarian – have traditionally used cyber capabilities to gather intelligence (cyber-espionage) in foreign countries, but today low-intensity political warfare in cyberspace has become more prominent.[3] Unfortunately for democratic countries, cyberspace is an ideal environment in which to undermine democratic processes and institutions by diverse covert activities.

> *It is unlikely that China's and Russia's strategies will change remarkably any time soon and their evolving practices should be studied in the West.*

This paper focuses on grey zone cyber-attacks by authoritarian states and their proxies in support of other influence activities against liberal democracies. In the contested cyberspace the major state-adversaries to democratic countries are China, Russia, Iran, and North-Korea. However, of these five countries only China and Russia have developed mature information warfare and information operation strategies and tactics. This paper provides an overview of the Russian theory and practice in using cyber-attacks for soft subversion. While the scope of the paper is limited to the examination of only one country, it should be emphasized that China's approach is similar to Russia's. Both countries see free information and foreign technologies as threats, and try to achieve "cyber sovereignty" in order to control cyberspace and information contained in it. Similarly, both countries make no distinction between peacetime and wartime information-related activities. They have long tradition of strategic thinking about the role of information in projecting national power and holistic understanding of information space.

It is unlikely that China's and Russia's strategies will change remarkably any time soon and their evolving practices should be studied in the West. In order to do so more case studies should be undertaken, applying both quantitative and qualitative methods.[4] This paper recommends lines of action to the EU and NATO countries that will enable to better understand and counter state-initiated cyber-attacks against democratic countries as part of grey zone influence activities.

[1] Thorsten Bennen, "An Era of Authoritarian Influence?", *Foreign Affairs*, September 15, 2017 (accessed January 29, 2018); Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How authoritarian states project influence", *Foreign Affairs*, November 16, 2017 (accessed January 29, 2018). Western authors and institutions that have researched Russia's strategy include James Sherr, Mark Galeotti, Keir Giles, Kenneth Geers, Clint Watts, Ben Nimmo, Michael McFaul, Peter Pomerantsev, Michael Weiss, NATO Strategic Communications Centre of Excellence, NATO CCD COE, the RAND Corporation, the European Values think-tank, the EU East StratCom Task Force, the German Marshall Fund, the European Council on Foreign Relations, the Atlantic Council, the Harvard Kennedy School, the US Army War College, the Chatham House, etc.

[2] For example, see Anne-Marie Brady, "Resisting China's Magic Weapon," *The Interpreter*, September 27, 2017; Alan Chong, "Information Warfare. The Case for an Asian Perspective on Information Operations", *Armed Forces and Society* 40(4) (2014): 599–624; U.S.-China Economic and Security Review Commission, *Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy*, Washington DC, May 4, 2017: 179-181, accessed January 29, 2018; Scott W. Harold et al., *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains* (Santa Monica: RAND Corporation, 2017) (accessed January 29, 2018). Other authors include Adam Segal, Mikk Raud, Robert Lai, Timothy Thomas.

[3] In this paper, the concept of cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R), Washington DC, February 5, 2013, accessed January 29, 2018.

[4] This paper treats the terms "information warfare" and "information counter-struggle" as synonymous. Since the paper focuses on Russian practice, the Russian term "information counter-struggle" is preferred throughout the text. Different nations use different cyberspace-related concepts that have different meanings. In Russian academic writing and strategic documents, the term "information counter-struggle" (*informatsionoye protivoborstvo*) is commonly used. It is usually translated into English as "information confrontation", but in this paper "information counter-struggle" is used, as it refers to the presence of an activity ("struggle") rather than a more passive word ("confrontation"). The concept implies a continuous application of tools, including in peacetime, by a wide range of state and non-state actors. The term is used in: Juha Kukkola, Mari Ristolainen, and Juha-Pekka Nikkarila, "Confrontation with Closed Network Nation: Open Network Society's Choices and Consequences," *IEEE MILCOM 2017 Conference Proceedings*, Baltimore, October 3-25, 2017 (accessed January 28, 2018). By contrast, the US Joint Staff and Army Doctrine refers to "information operations" as activities conducted only during military conflict by strictly designated authorities (military and intelligence services), whose activities are constrained by legal frameworks. Information operations occur at the operational level, whilst information counter-struggles are at the strategic level. See: Joint Chiefs of Staff, "Information Operations," Joint Publication 3-13, Washington DC, 2012, accessed January 28, 2018.

1. Political Influence Activities in Cyberspace

Nation-state political influence activities in an online environment can be understood as "coordinated and deniable activities that are initiated by a state actor and which are aimed at influencing decisions, perceptions and behaviour of political leaders, the population or particular target groups (such as experts and the media) with the objective of achieving the state actor's security policy objectives, mainly through the dissemination of misleading or incorrect information, often complemented with other actions tailored for the purpose that is being pursued."[5] Cyber-attacks have been by used nation-state-affiliated actors to steal private information that is then publicly broadcasted ("doxing") to embarrass an individual or organisation.[6] Examples are the cyber-attacks against Sony Pictures Entertainment in 2014 and against the US and French presidential elections in 2016. These types of political influence activities are conducted in the grey zone between war and peace and are usually not prohibited under international law. Cyber-attacks that do not reach "the use of force" threshold in international law are considered hybrid threats, along with other types of non-military threat such as disinformation, propaganda and diplomatic, economic or military pressure.[7] Hence, cyber-attacks constitute one tool among diverse subversive activities carried out during peacetime.

Cyber-attacks constitute one tool among diverse subversive activities carried out during peacetime.

Nation-states have used cyber-attacks against each other in peacetime for many purposes. In addition to military, political or economic intelligence collection, high-intensity/damaging attacks on critical infrastructure have also been attributed to state actors (e.g. Stuxnet is believed to have been developed by the US and Israel). Some destructive cyber-attacks against critical infrastructure have been identified as most likely state sponsored, but were not publicly attributed to a particular state actor (e.g. cyber-attacks against a German steel mill).[8] Low-intensity cyber-attacks appearing to attempt to exert political influence on an opponent are more frequent than few destructive cyber-attacks. In the West, they are referred to with terms such as "cyber-influence operations", "influence cyber operations", "cyber-enabled information operations", "cyber-enhanced disinformation campaigns" and "cyber-abetted inference", as well as "cyber propaganda" and "hybrid cyber operations."[9] Definitions of these terms are not usually provided, and they do not distinguish between, on the one hand, disinformation campaigns that may be executed fully or partially in and through cyberspace, and, on the other, cyber-attacks that apply cyber capabilities with the purpose of causing certain effects in cyberspace.[10] A good example of this

[5] This definition is provided by the Swedish Military Intelligence Service. See Anke Schmidt-Felzmann, "More than Just Disinformation: Russia's information operations in the Nordic region", in *Information Warfare – New Security Challenge in Europe,* ed. by Tomáš Čižik (Bratislava: Centre for European and North Atlantic Affairs, 2017).

[6] "Doxing" (or "doxxing") is the broadcast of personal data to embarrass or damage the reputation of a person or organisation, including when the data is obtained by hacking. The term also includes legal means of obtaining private information (e.g. searching public databases and social media sites) for benign purposes (e.g. law enforcement or for business analysis purposes). See "Doxing", Wikipedia, accessed January 29, 2018.

[7] The EU defines hybrid threats as "a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological, information), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organised hostilities". European Commission, *Joint Framework on countering hybrid threats – a European Union response*, JOIN (2016) 18, Brussels, April 6, 2016, accessed January 28, 2018.

[8] Industrial Control Systems, "German Steel Mill Cyber Attack", December 30, 2014, accessed January 29, 2018.

[9] Keir Giles, "Countering Russian Information Operations in the Age of Social Media", Council on Foreign Relations, November 21, 2017 (accessed January 29, 2018); Glenn Crowther, "The Cyber Domain", *The Cyber Defense Review* 2(3) (Fall 2017): 63–78; 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. by N. Pissanidis, H. Rõigas and M. Veenendaal (Tallinn: NATO CCD COE Publications, 2016): 113–26; "ICIT Introduces: Center for Cyber-Influence Operations Studies (CCIOS)", Institute for Critical Infrastructure Technology, accessed January 29, 2018; Nadiya Kostyuk and Yuri Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution*, November 10, 2017 (accessed January 29, 2018).

[10] The term "disinformation campaign" as used in academic and policy writings occurs in peacetime. The US military defines "information operations" as "the integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own". Disinformation campaigns are at the strategic level, whilst information operations, including cyber-attacks, are at the operational level, and during military conflicts.

mixture is the report "Freedom on the Net 2017", which observes that "online manipulation and disinformation tactics" have taken place against election processes in 18 countries. According to the report, "online manipulation tactics" include activities that constitute the use of the internet (e.g. pro-government online commentators, media and propaganda, "fake news around elections") and cyber-attacks (the use of social media bots and hijacking social media accounts by hacking).[11]

An analogy can be drawn with ISIL/Daesh's use of the internet, which clarifies the distinction between (1) the use of cyberspace (mainly the internet) to carry out core activities and (2) cyber-attacks. Daesh has not acquired high-end cyber capabilities that would enable it to launch large-scale destructive cyber-attacks against critical infrastructure. The vast majority of terrorist activity online consists of using cyberspace to boost its traditional agenda: distribution of propaganda, intelligence collection, recruitment, fundraising, and radicalisation of potential supporters, as well as the communication and planning of attacks. Terrorists have only been able to deface websites and break into social media accounts, which require low-end cyber capabilities. Similarly, the vast majority of nation-states' activity in cyberspace has remained below the level of high-end cyber-attack. Much cyberspace activities that nation-states have used to exert political influence in democratic countries are technically legal (e.g. big data, purchase of political advertisements in social media). To curb the spread of disinformation Germany has enacted new regulations, the US intends to make social media advertising more transparent, Google and Twitter have restricted the appearance of Russian government broadcasters RT and Sputnik on their channels, and Facebook plans to inform users if they liked or followed posts or pages by the Russian Internet Research Agency troll farm.[12]

However, a clear distinction between content-related activities (disinformation, trolling, political ads, etc.) and cyber-attacks is important for two reasons. First, the first group of activities is often legal, but cyber-attacks usually qualify as crime (for example, intrusion into a computer system for the purpose of espionage is illegal under both domestic law and the Budapest Convention on Cybercrime). The choice of state response to political influence activities will depend on, among other things, the legality or illegality of the act. For example, the US has responded to nation-state-initiated cyber-attacks with various measures: economic sanctions, criminal prosecution and diplomatic expulsions. It chose financial sanctions against ten North Korean officials accused of cyber-attacks against Sony Pictures Entertainment; indictment of five Chinese PLA officers in response to the theft of intellectual property from US companies; indictment of seven Iranian hackers in response to intrusions against financial sector and IT companies; and financial sanctions and the expulsion of 35 Russian diplomats in response to the hacking of the US elections. Second, different attacks require different protection measures. Disinformation can be countered by better media literacy and critical thinking, and educational programmes can be carried out by schoolteachers without specialist training. By contrast, the detection of Advanced Persistent Threats (APT) that move laterally in the network requires highly specialised expertise and investment in technology.

The vast majority of nation-states' activity in cyberspace has remained below the level of high-end cyber-attack.

In sum, the first category can be denoted as "cyberspace-enabled political influence activities", and the second as "cyber-attacks in support of political influence activities".

[11] Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp and Jessica White, *Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy* (Washington DC: November 2017) (accessed January 29, 2018).
[12] Katy O'Donnell, Joanna Plucinska and Mark Scott, "Germany's new online hate speech code pushes big fines and debate," *Politico*, October 2, 2017 (accessed January 29, 2018); Adam Sharp, "'Honest ads' on social media one step to an honest political system", *The Hill*, October 31, 2017 (accessed January 29, 2018).

1.2 Cyber-attacks in support of political influence activities

For the purposes of this paper cyber-attacks are understood as deliberate activities in cyberspace that cause harm by compromising communications, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.[13] Harm can be caused by violating confidentiality, integrity, availability, authenticity or non-repudiation of systems or information. Cyber-attacks are executed by the application of cyber capabilities. Cyber capabilities are devices, computer programmes or techniques designed to create degradation, disruption or destruction effects and manipulation of information, information systems and/or networks in or through cyberspace.[14]

In contrast to cyberspace-enabled political influence activities cyber-attacks have effects on one or more layers of cyberspace: the physical layer (hardware and physical infrastructure such as cables, routers and servers), the syntactic layer (software instructions and rules) or the semantic layer (information in cyberspace).

This definition of cyber-attacks includes low-end attacks that do not reach the threshold of the use of force or an armed attack. We do not use the definition suggested in the Tallinn Manual 2.0, which defines cyber-attacks as attacks that are reasonably expected “to cause injury or death to persons or damage or destruction of objects”.[15] In the event of such high-end attacks, the law of armed conflict would apply, but here we focus on the activities in the grey zone, where mostly low-end attacks are used. Thus, in this paper “cyber-attack” denotes both low- and high-end attacks during peacetime. Examples of low-end cyber-attack vectors are website defacement, and Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, and takeover of computers as part of botnets. Medium-level attacks include for instance the use of malware (trojans, viruses, worms, rootkits) or unauthorised access to computers through cyber capabilities. High-end cyber-attack vectors include APTs, customised malware, logic bombs, zero-day exploits, and the like.[16]

In contrast to cyberspace-enabled political influence activities cyber-attacks have effects on one or more layers of cyberspace: the physical layer (hardware and physical infrastructure such as cables, routers and servers), the syntactic layer (software instructions and rules) or the semantic layer (information in cyberspace).[17] An example of a physical effect is the destruction of a laptop or its functionality; a syntactic effect is the disruption of information stored on the laptop. In addition, cyber-attacks may have a cognitive effect (e.g. the modification of the information in a way that affects the adversary’s decision-making).[18]

As will be discussed in this paper later they can additionally cause cognitive and strategic effects. It should be underlined that this definition excludes activities that do not apply cyber capabilities affecting the cyberspace layers. Examples of such activities are the creation of inauthentic social media accounts, the purchase of political ads in social media, the use of technological innovations (big data analytics, machine learning, artificial intelligence) for spreading disinformation, and the use of paid commentators (trolls) to dominate and sway online conversations. These activities do not affect the physical and logical layers, and they do not affect the semantic layer by cyber capabilities.

[13] Brangetto and Veenendaal, op. cit.

[14] Joint Chiefs of Staff, “Cyberspace Operations”: II-5.

[15] Michael Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edn (Cambridge: Cambridge University Press, 2017): 415.

[16] Malware that allows privileged access to a computer to be maintained; malware designed to initiate a malicious sequence of actions if specified conditions are met.

[17] There are many models of cyberspace. For the purposes of this article Martin Libicki’s model has been chosen: Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007).

[18] Larry Welch, “Cyberspace – the Fifth Operational Domain,” Institute of Defense Analysis, Research Notes, 2011 (accessed January 29, 2018).

Cyber-attacks may have cognitive effects. For example, cyber-attacks in 2015 against three regional electric power distribution companies in Ukraine, which caused blackouts for several hours to 225,000 consumers, might have led to some degree of uncertainty. However, the effect on Ukrainians' minds was probably marginal compared to that of the ongoing disinformation and propaganda campaign. DDoS and other types of cyber-attack against Estonia in 2007 similarly had some effects on decision-makers and the population at large, even though they had a negligible effect on the individual decisions of the Estonian government. Due to methodological difficulties, it is generally problematic to ascertain cognitive effects of cyber-attacks with high degree of certainty. It may be possible to measure changes in opinion or behaviour (or determine shifts in government policy) resulting from a particular disinformation activity targeted to specific audiences, but there will be a negligible cause-and-effect relationship between a particular cyber-attack and public opinion, because cyber-attacks are ambiguous. While the use of bots and inauthentic accounts in social media can be identified relatively easily, attribution of cyber-attacks with high-level confidence is more difficult. Analysis of their effects, the possible intentions of the perpetrators, and reading the intended message is subjective and hard to prove with solid evidence (among other things because intelligence agencies do not reveal sources and methods).

Due to methodological difficulties, it is generally problematic to ascertain cognitive effects of cyber-attacks with high degree of certainty.

Yet, there are cyber-attacks whose primary objective seems to be intimidation of an organisation or an individual. For example, the release of National Security Agency (NSA) hacking tools by the Shadow Brokers embarrassed the agency and played into public criticism that Western intelligence agencies should disclose vulnerabilities to commercial ICT companies.[19] An example of an allegedly Western-initiated influence operation is the release of the Panama Papers. Some experts note that Russian president Vladimir Putin believes that this was a Western influence operation directed against him personally.[20] Researchers at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) have described "cyber influence attacks" in which, in their opinion, the objective has been to influence decision-making or public opinion. These include Chinese cyber espionage against the US Office of Personnel Management (OPM) in 2015, cyber-attacks against the Central Election Committee in Ukraine in 2014, APT28 "false flag" cyber-attacks against French television station TV5Monde in 2015, cyber-attacks against Estonia in 2007, and several cases of personal doxing in 2014 and 2015.[21] It is plausible that the objective in these cases was to embarrass, coerce or intimidate a nation-state, an organisation, or an individual, but to show the intention and the effect is not easy. For example, the OPM attacks have been attributed to China, but figuring out the objective (was it a preventive attack, retaliation, coercion, deterrence or espionage?) is subjective because no solid proof of intention exists.

The empirical quantitative research of cyber-attacks in Ukraine in 2014-6 shows that there is no correlation between the number and intensity of cyber-attacks (executed by various non-state actors) and military fighting in the Donbass.[22] This is not surprising, because coordination of non-state low-level cyber-attacks with regular and irregular armed attacks would in practice be difficult and not feasible. This study revealed additionally that there was no reciprocity between actions of pro-Ukrainian

[19] Some experts believe that Shadow Brokers are Russian security agencies-affiliated. Other groups/campaigns such as APT28, CyberBerkut, Sandworm, Turla and Gamaredon have been attributed by several cyber security companies to Russian interests, or are at least identified as state-sponsored campaigns. Ukrainian security services, politicians and experts have attributed various cyber-attacks in Ukraine in 2013-6 to the Russian security services.

[20] Jason Healey, "What Might Be Predominant Form of Cyber Conflict?", in *IEEE International Conference on Cyber Conflict U.S.*, ed. by Edward Sobiesk, Daniel Bennett and Paul Maxwell (Washington DC, 2017). According to Andrei Soldatov, the Russian interference in the US elections in 2016 was in retaliation for the release of the Panama Papers. See: Vanessa Sauter, "The Lawfare Podcast: Andrei Soldatov on Russian Intel Ops and Surveillance", *Lawfare*, November 12, 2017 (accessed January 29, 2018).

[21] Brangetto and Veenendaal, op. cit.

[22] Kostyuk and Zhukov, op. cit.

and pro-rebel/pro-Russian groups of hackers. Cyber-attacks were not conducted in order to respond, retaliate or deter the adversary's actions, but for practical reasons. This result is also not surprising, because cyber-attacks take time to prepare, and non-state hackers conduct cyber-attacks when they have the time and resources to do so, and immediate reciprocity is thus difficult.[23] Thus, retaliation and deterrence seem not to be primary factors, at least in the case of non-state hackers during military conflict. Even though academic reasoning might sound plausible, empirical evidence that proves that nation-states have used cyber-attacks to deter, retaliate against or coerce an opponent, is scarce.

Even though academic reasoning might sound plausible, empirical evidence that proves that nation-states have used cyber-attacks to deter, retaliate against or coerce an opponent, is scarce.

Nevertheless, cyber capabilities display attractive features for nation-states' influence operations. Cyber capabilities are versatile, ubiquitous and uniquely secretive.[24] As discussed earlier, they are attractive tools of covert influence activities in the grey zone, and they balance the power of conventional capabilities by enabling asymmetric advantage through cyberspace. They have been used before the start of kinetic battle to prepare the battleground (e.g. the Russo-Georgian war of 2008). They can support and, in certain cases, substitute conventional and unconventional capabilities. Cyber-attacks can be used as standalone or support operations, and turned on and off according to need.[25] They can be used for intelligence, reconnaissance, surveillance and psychological operations, as well as for signalling deterrence, for discreet sabotage and for widespread disruption.[26]

In contrast to kinetic weapons, cyber capabilities are non-lethal and less likely to cause casualties. The quality of reduced collateral damage makes cyber capabilities attractive if the objective is to avoid a strong response or escalation. Moreover, the effects of cyber-attacks can be temporary or reversible, which is again preferable if the aim is not to escalate the conflict.[27] Their effects can be, at least theoretically, as precise as firing precision-guided munitions.[28] The same malware and exploits can be used for multiple purposes (e.g. for intelligence collection and for disruption or destruction). The same malware can also be developed into multiple improved versions (for instance, the BlackEnergy series of trojan software). Cyber-attacks are also more ambiguous than kinetic attacks because their effects may be not obvious (at least not immediately), and it is difficult to infer the intentions of attackers from their actions.[29]

Another attractive trait of cyber-attacks is that they can be launched over great geographic distances. The majority of cyber capabilities (e.g. malware) are affordable and easily available. The difficulty in attributing attacks offers plausible deniability for the attacker.[30] Attackers can operate undetected for long periods (the average detection time is over 200 days). Further, cyber capabilities are more persistent than kinetic attacks in that the risks of the operating personnel (e.g. non-state hackers, military cyber troops, intelligence agencies) being caught are very low. Lastly, early warning and indications of cyber-attacks have not yet proven to be useful in preventing or detecting nation-state attacks.[31]

[23] Nadiya Kostyuk, "Hacking Power Grids: New Tactic of War or Wave of the Future?", *Russia Matters,* November 3, 2017 (accessed January 29, 2018).

[24] George Perkovich and Ariel E. Levite, "Conclusions", in *Understanding Cyber Conflict. Fourteen Analogies,* ed. by George Perkovich and Ariel E. Levite (Washington DC: Georgetown University Press, 2017): 250-60.

[25] Stephen Blank, "Cyber War and Information War à la Russe," in *Understanding Cyber Conflict. Fourteen Analogies,* ed. by George Perkovich and Ariel E. Levite (Washington DC: Georgetown University Press, 2017): 81-98.

[26] Ibid.

[27] Martin C. Libicki, "The Convergence of Information Warfare," S*trategic Studies Quarterly*, Spring 2017: 49-65.

[28] Perkovich and Levite, op. cit.

[29] Libicki, op. cit.

[30] Many experts hold that "the attribution problem" has been solved by state-of-the-art digital forensics and by combining technical attribution with all-source intelligence, but there are also convincing opposing views. For example, see Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs*, 70(1) (Winter 2016): 75-136.

[31] Libicki, op. cit.

In the grey zone between war and peace, cyber-attacks can be used to support objectives of information warfare.

In the grey zone between war and peace, cyber-attacks can be used to support objectives of information warfare in several ways. The possibilities include collecting intelligence, doxing, infecting digital devices and webpages to spread propaganda, social media bots, and knocking websites offline by DDoS attacks. New attack vectors that have knowingly not yet been used, but can be used by nation-state actors to influence populations, include attacks against the internet of things and, if radio-frequency technology devices become widely used, jamming and spoofing these.[32] On the cyber defence side, cyber capabilities can be used to deter adversaries (deterrence by denial and deterrence by punishment), but the nuclear deterrence analogy cannot be applied without amending it to cyberspace. An example of the use of cyber-attack for deterrence by punishment is when critical infrastructure is attacked in order to signal to the victim an ability of the attacking state to inflict greater costs.[33]

However, there are certain limitations to using cyber capabilities in hybrid and kinetic conflicts. Standalone cyber-attacks cannot entirely replace non-military and conventional operations because their effects are uncertain and the timing of success often unpredictable.[34] For example, malware can spiral out of control, or an adversary can replicate, reverse-engineer or proliferate it. Another disadvantage is that it is hard to limit cyber effects to specific targets – after an attack is launched it can result in unintended consequences, go viral, and cause unexpected damage. There is also the risk of escalation:

> *There are no clear thresholds, mechanisms for signalling, or methods for escalation control and so a conflict in cyberspace might quickly become kinetic because of misperception or miscalculation.*[35]

Some experts believe that the risk of escalation has led to self-restraint by major cyber powers who have opted not to use high-end attacks.[36]

In terms of the ability to yield strategic effects, cyber espionage can clearly be used for this purpose. However, in kinetic conflicts cyber-attacks so far have only had short-term operational- and tactical-level effects and did not change the overall course of kinetic fighting. During the conflicts in Georgia and Ukraine, Russia demonstrated its ability to harm critical infrastructure by cyber-attacks, but these attacks did not play a critical role in the military conflict.[37] Apart from battleground effects, cyber tools can be used to manipulate information and decision-making, which, according to some authors, "is more likely to produce strategic effect" than high-intensity cyber-attacks against critical infrastructure.[38]

In kinetic conflicts cyber-attacks so far have only had short-term operational- and tactical-level effects and did not change the overall course of kinetic fighting.

It has been proposed that cyber-attacks can produce effects at five levels of severity: (1) on specific data sets or devices by compromising their confidentiality, integrity and availability; (2) on a cyber system when information is compromised or not available; (3) on a decision-maker, algorithm, or connected cyber-physical system; (4) on larger, physical systems at the level of people, organisations, government and society; and (5) on a strategic

[32] Libicki, "The Convergence of Information Warfare".

[33] Robert E. Schmidle, Michael Sulmeyer and Ben Buchanan, "Nonlethal Weapons and Cyber Capabilities", in *Understanding Cyber Conflict. Fourteen Analogies,* ed. by George Perkovich and Ariel E. Levite, (Washington DC: Georgetown University Press, 2017): 31-44.

[34] Ibid.

[35] Adam Segal, "An Update on U.S.-China Cybersecurity Relations", Council on Foreign Relations, November 17, 2017 (accessed January 29, 2017).

[36] Perkovich and Levite, "Conclusions".

[37] Peter Feaver and Kenneth Geers, "'When the Urgency of Time and Circumstances Clearly Does Not Permit …': Pre-delegation in Nuclear and Cyber Scenarios", in *Understanding Cyber Conflict. Fourteen Analogies,* ed. by George Perkovich and Ariel E. Levite (Washington DC: Georgetown University Press, 2017): 211-230.

[38] James Lewis, "Fighting the Wrong Enemy, aka the Stalemate in Cybersecurity," *The Cipher Brief*, November 26, 2017 (accessed January 28, 2018).

goal.[39] In this conceptual framework, a grey zone cyber-attack against information can affect behaviour of a decision-maker if information is rendered incorrect (level three effect). This can result in a greater effect which disrupts life cycles at the level of an individual, organisation or society (level four effect). The level four effect can degrade trust in society, national will and the ability to fight, provision of critical civil functions, or the national economy (level five effect). The level five effects constitute strategic effects that are manifested as degrading national security.[40]

According to this framework a moderate-level (level three) cyber-attack that alters information, makes it unavailable or deletes it may in the end result in a strategic-level national security effect.

2. Information Warfare in the Russian and in the US view

Russia's strategic documents (Military Doctrine 2014, National Security Strategy 2015) identify the use of information and communications technology (ICT) for political and military purposes as one of the main security threats to and military dangers for Russia. The official documents depict Russia's information counter-struggle as a defensive measure, and a strategic priority in peacetime and wartime alike. Moscow perceives EU and NATO enlargement and—allegedly West-instigated—"coloured revolutions" as threats to Russian geopolitical interests and national security. Information of Western origin is consequently perceived as a security threat and the information environment as a domain of operations. Against this backdrop Russia regards its information warfare against the West "as threat-neutralising measure" to deter what it perceives as hostile activities against itself. In this way, information freedom and the free and open internet as its medium become targets of Russia's policy.[41] This view, which may seem paranoid to some, is expressed frequently by senior Russian government officials and key leaders. For example, Putin's spokesperson Dmitry Peskov claimed that Russia is "in a state of information warfare with the trend-setters in the information space, most notably with the Anglo-Saxons, their media".[42] Sergey Kislyak, the former Russian ambassador to the US, claims that the US runs "a massive propaganda campaign … with the purpose of undermining the internal political atmosphere in Russia".[43] According to journalist and author Andrei Soldatov, the Kremlin genuinely believes it is under attack from the West, and in his opinion, Russia's strategic activity is therefore always reactive.[44]

The Russian concept of information warfare is "information counter-struggle" (*informatsionoye protivoborstvo*). Its purpose is "to inflict damage on [an] opponent by means of information in [the] information sphere".[45] The main mechanisms to cause harm are divided into information-psychological and information-technical tools. Technical tools are low-level cyber-attacks (unauthorised access to information resources), as well as "protection of own information environment". The end goal is a change in the strategic behaviour of an adversary, which is achieved by manipulating their picture of reality and consciousness by technological and psychological components of the counter-struggle.[46]

Psychological measures encompass anything that can be used to influence the general

[39] David Ormrod and Benjamin Turnbull, "The cyber conceptual framework for developing military doctrine", *Defence Studies* 16(3) (2016): 270–98 [290–1].

[40] Ibid.

[41] Stephen Blank, "Russian Information War as Domestic Counterinsurgency", *American Foreign Policy Interests* 35(1) (2013): 31–44 (accessed January 29, 2018).

[42] "'Russia at war with Anglo-Saxon media' – Putin spokesman", *RT*, March 27, 2016 (accessed January 29, 2018).

[43] "Legendary Russian Ambassador Kislyak Explains How He Personally Helped Steal US Elections," *Vesti*, November 18, 2017 (accessed January 29, 2018).

[44] Sauter, "The Lawfare Podcast: Andrei Soldatov on Russian Intel Ops and Surveillance". The Estonian Foreign Intelligence Agency similarly observes that "Russia's leaders appear to fall for the lies spouted by its own propaganda machine. Misled by its own propaganda, the Kremlin has assigned a paranoiac interpretation on the Western position and has concluded that [the] West is driven by Russophobic sentiment." Estonian Information Board [now Estonian Foreign Intelligence Agency], "International Security and Estonia" (Tallinn, 2017) (accessed January 29, 2018).

[45] *Informatsionnoe protivoborstvo* includes the use of information and physical means of influence to achieve information superiority over an adversary. *Russian Military Encyclopaedic Dictionary*, cited in Trotsenko, "Information Warfare at the Operational-Tactical Control Level", *Military Thought* 26(2) (2017).

[46] Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy", *Proliferation Papers* 54, November 2015, IFRI Security Studies Centre (accessed January 29, 2018).

population and armed forces personnel. For Russia, the objective of psychological activities is to affect the will, behaviour and morale of the adversary and also more subtle emotions that in turn impact rational thinking.[47] This activity is sometimes known as "reflective control", referring to a state predetermining an adversary's decisions in its favour in such a way that the adversary believes it is behaving in its own interests.[48] In the Russian view, information warfare in modern conflicts does not target solely adversary's key decision-making, but uses extensively "the protest potential of the population."[49] US military doctrine is much less nuanced in the area of psychological influence on the population – it states simply that the aim of information operations is to create doubt, confuse and deceive, and influence decision-makers, militaries and various other audiences, and is silent on the need to manipulate with sentiments of population.[50]

The Russian view is that the main battlefield is human consciousness, perceptions and strategic calculations.

The Russian view is that the main battlefield is human consciousness, perceptions and strategic calculations.[51] According to a prominent Russian information warfare expert, there are no borders in the battlefield of the cognitive domain. The borders between war and peace, internal and external, tactical, operational and strategic levels of operations, and forms of warfare (offence and defence) and of coercion are blurred.[52]

Two key aspects distinguish the Russian understanding of information counter-struggle from the US military's view of information operations.[53] In the Russian view, the information counter-struggle is first conducted constantly during peacetime, and second, it is a strategic-level activity executed by a "whole-of-society" response that recalls in a way the Soviet-era concept of "total defence", according to which all the resources of civil society were used for national defence. Russia expert Mark Galeotti has described how the Kremlin carries out this holistic approach by outsourcing the fulfilment of Russia's policy to volunteers, organised-crime groups, business, the Russian Orthodox Church, government-organised non-governmental organisations (GONGOs), the media and other actors in the deployment of various "active measures".[54] By contrast, the US military perceives information operations as wartime activities executed by designated authorities whose action is constrained by their mandates stipulated by law. For the US, this activity is at operational level.

In several respects, the US and Russian views display also similarities. For Russia, violent physical acts such as "kidnapping adversary officials" and "physical destruction of adversary assets and targets" are also psychological tools.[55] Likewise, the US includes physical destruction among information operations tools. Accordingly, actions in the domains of operations (land, air, sea, space and cyber) can have psychological effects.[56] Both countries reckon that cyber-attacks are part of information warfare tools, and that information-related activities are to be conducted simultaneously in the cyber and physical spaces. Both countries include defensive activities (e.g. operational-level "operations security", and protecting own infrastructure, networks and forces) as part of information warfare, and they agree that the ultimate objective of information warfare is information superiority. As will be discussed in

[47] V.A. Kiselyov, "What Kind of Warfare Should the Russian Armed Forces Be Prepared for?" *Military Thought* 26(2) (2017).

[48] Adamsky, op. cit.

[49] Government of Russia, "The Military Doctrine of the Russian Federation," December 25, 2014 (accessed February 1, 2018).

[50] Department of the Army, "Field Manual," No. 3-0, October 6, 2017 (accessed February 1, 2018).

[51] Adamsky, op. cit.

[52] Sergei Modestov, "Strategicheskoe sderzhivanie na teatre informatsionnogo protivoborstva" [Strategic containment in the theatre of information counter-struggle], *Vestnik Akademii Voennykh Nauk* 26(1) (2009), cited in Adamsky, op. cit.

[53] "The US military's view" refers to three publications: Joint Chiefs of Staff, "Cyberspace Operations"; Department of the Army, "Field Manual",; and Joint Chiefs of Staff, "Information Operations".

[54] Mark Galeotti, "Putin's hydra: Inside Russia's intelligence services", European Council on Foreign Relations, May 11, 2016, (accessed February 1, 2018).

[55] Kiselyov, op. cit.

[56] In US doctrine, cyber capabilities can be used to influence the cognitive dimension (decision-making) through cyber-attacks against the three layers (physical, logical and cyber-persona/social) of cyberspace (respectively, laptop, email, and the information contained in the email). See: Joint Chiefs of Staff, "Information Operations". In this concept of cyberspace, the social layer (users and their online identities) does not equal the semantic layer (i.e. information) of Libciki's model of cyberspace.

the following sections, the Russian view emphasises information-psychological capabilities (in contrast the US view emphasises information-technological capabilities), because the control of information, including internet content and physical infrastructure, is seen as a security warrant for the survival of the regime.[57]

3. Russia's Political Influence Activities

3.1 Foreign and security policy goals

Russia's strategy to influence foreign countries is driven by articulated strategic goals, whilst its modus operandi is flexible.[58] The main goal is to promote its core national interests and create an international environment conducive to its benefit. At the strategic level, democratic regimes, principles and values, as well as the EU integration model, represent an existential threat to the Russian hybrid state based on the opposing model of kleptocracy, autocracy and ideology.[59] Thus the strategic goal is the destruction of the rule of law and an international order based thereon. Russia's mid-term goals are to reduce US leadership in the world, to damage the transatlantic relationship and to split alliances such as the EU and NATO, and to divide their member states. The immediate goals are to conduct specific influence activities (such as interference in electoral processes) with the aim of reducing trust in democratic processes, discrediting institutions and generally sowing uncertainty, doubt, confusion, fear and chaos in Western societies.[60] Some scholars hold that, in the countries that Russia considers its "near abroad" or belonging to its self-declared sphere of interest, Russia conducts hybrid wars "to instil a feeling of constant political and economic insecurity among … population", or even in order to recolonise and imperialise the former Soviet space.[61]

3.2 The use of asymmetric measures

Russian foreign-policy instruments can be divided into six broad categories: governance; economics and energy; politics and political violence; military power; diplomacy and public outreach; and information and narrative warfare.[62] In addition to the traditional tools of national power, Russia has developed a mix of covert influence tools that are commonly referred to as "active measures". These encompass, for example, intelligence operations, organised crime, business lobbies and GONGOs.[63] In a way, the Kremlin has weaponised every factor of modern life at the personal, organisational, nation-state and global level – culture, history, nationalism, information, media and social media, the internet, business, corruption, electoral processes, globalisation, and even "people's power".[64] In this struggle information has been rendered a target, disinformation a weapon, and the internet a battlefield.

In a way, the Kremlin has weaponised every factor of modern life at the personal, organisational, nation-state and global level.

One of the principal threats that a democratic regime and world-view poses to the Russian model of governance and concomitant world-view is the principle of freedom of expression, including its manifestation in a free and open internet. The internet can whip up grass-roots protests and uprisings—the "coloured

[57] A caveat in comparing the Russian and US approaches is that, in Russian thinking and doctrine, the effects of cyber-attacks are not elaborated upon. Psychological effects of cyber-attacks are unfortunately not discussed in Russian writings, but because cyber-attacks are part of the information counter-struggle, it can be deduced that they are perceived to yield psychological effects.

[58] Sherr, op. cit.

[59] Andri Frolov, "Brian Whitmore: Russia Is Waging Non-Kinetic War on West", *Lennar Meri Conference,* May 11, 2017
(accessed February 1, 2018).

[60] Government of Canada, *Cyber threats to Canada's democratic process,* Communications Security Establishment, Ottawa, 2017, accessed January 29, 2017.

[61] Blank, "Cyber War and Information War à la Russe"; Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (London: Rowman & Littlefield: 2016).

[62] Robert Seely, "Defining Contemporary Russian Warfare: Behind the Hybrid Headline", *RUSI Journal* 162(1) (April 2017): 50-9.

[63] Mark Galeotti, "Controlling Chaos: How Russia Manages its Political War in Europe", European Council of Foreign Relations Policy Brief, August 2017 (accessed February 1, 2018).

[64] For example, see Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money", *The Interpreter*, November 22, 2014 (accessed February 1, 2018); Galeotti, "Controlling Chaos".

revolutions"—and the Kremlin fears that an "Arab Spring"-like upheaval in Russia could sweep it from power.[65] The Kremlin's fear of a free and open internet was expressed by President Vladimir Putin in 2014 when he claimed it was a "CIA project" from which Russia needed to be protected.[66] For this reason a multi-stakeholder internet governance model is perceived by Russia (but also by many other authoritarian countries) as inherently dangerous, and these governments intend to increase their control over cyberspace content and physical infrastructure, as well as soft- and hardware. Whether for defensive or offensive purposes, or for a mix of them, Russia has used cyberspace to conduct political influence activities at the strategic level against many EU and NATO member states, and in the Western Balkans, the South Caucasus and Central Asia.[67]

Each country is vulnerable to Russian "active measures" in different ways. Mark Galeotti distinguishes seven types of Russian influence strategies that seek to exploit specific weaknesses and allegiances in individual countries.[68] For example, Bulgaria and Greece have two types of vulnerability: a Russia-friendly political and business elite, and weak democratic institutions. Russia cultivates a strategy of "state capture" by attempting to make these countries "Trojan Horses" within the EU and NATO. Hungary, Romania and Montenegro also have weak institutions, but their affinity to Russian interests is moderate. Russia therefore seeks to influence them only on specific issues (e.g. EU sanctions) by cultivating a strategy of "targeting the state". The remaining strategies are exploitation (in the UK), demonisation (in Estonia and Poland), disruption (in France, Germany, the Netherlands and Sweden), influencing (in the Czech Republic, Italy, Latvia and Lithuania), and social capture (in Slovakia).[69] In the information environment, Russia has likewise cultivated specific memes and narratives to influence different countries.[70] It has used social media bots to influence public opinion in the US, the UK, the Netherlands and Spain. In Hungary, the Czech Republic and Austria it did not deploy social media, but used a multitude of local political, economic and disinformation actors.[71] Russian disinformation practice in Europe shows that specific influence tools are chosen not by default, but after considering particular strengths (e.g. free speech) and vulnerabilities to be exploited, and the expected effects. Russia deemed social media to be an effective medium for covert disinformation activities in the US that enabled it to target selected demographic groups in certain geographic areas over great physical distance with low risk of escalation. In several Central and Eastern European countries, physical influence activities (corruption, and cultural, national and other allegiances) yielded better strategic-level effects than the abuse of social media platforms would have achieved.

Russian disinformation practice in Europe shows that specific influence tools are chosen not by default, but after considering particular strengths (e.g. free speech) and vulnerabilities to be exploited, and the expected effects.

Hence, Russia exacerbates various socio-economic and ideological grievances in Western

[65] Daniel Hoffman, "What Scares Putin? Democracy," *The Cipher Brief*, November 16, 2017 (accessed February 1, 2018); Brian Whitmore, "The Daily Vertical: The Kremlin's Existential Threat (Transcript)", *Radio Free Europe/Radio Liberty,* February 17, 2017 (accessed February 1, 2018).

[66] Ewen MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup", *The Guardian*, April 24, 2014 (accessed February 1, 2018).

[67] For example, the cyber-attacks and disinformation campaigns against the US, Canada, UK, Italy, France, Germany, the Netherlands, Spain, Sweden, Norway, Denmark, Montenegro and many Central and Eastern European countries. See for example, "Moscow is regaining sway in the Balkans", *The Economist*, February 25, 2017; and for a timeline of Russia's influence activity against the US, see "Russian Cyber Attacks," Committee to Investigate Russia, 2017, accessed February 1, 2018. Labelling Russia's strategy as "offensive" or "defensive" is subjective, relative and often politicised. In Russian strategic culture, the two forms of warfare co-exist and are often indistinguishable. See Adamsky, "Cross-Domain Coercion".

[68] Galeotti, "Controlling Chaos".

[69] Ibid.

[70] In this paper, the concept of information environment is defined as "any medium through which information is created, transmitted, received, stored, processed and deleted". See James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations* (New York & Moscow: EastWest Institute and the Information Security Institute of Moscow State University, 2014) (accessed February 1, 2018); for example, see "Russian Narratives on NATO's Deployment", Atlantic Council's Digital Forensic Research Lab, April 11, 2017, accessed February 1, 2018.

[71] Lóránt Győri, Péter Krekó, Jakub Janda and Bernhard Weidinger, *Does Russia Interfere in Czech, Austrian and Hungarian Elections?* (Budapest: Political Capital and European Values, in cooperation with Dokumentationsarchiv des österreichischen Widerstandes (DöW), 2017) (accessed February 1, 2018).

societies related to processes such as globalisation, technological innovation, nationalism, fundamentalism, immigration, and climate change. In addition to country-specific vulnerabilities it exploits the openness and freedom of democratic systems. In the words of James Sherr, "attributes of the liberal polity that normally are a source of strength, e.g. 'fairness', can also be used to undermine liberal democracy and advance hostile objectives."[72] He writes that:

> *The beginning of wisdom is to understand that the Russian pursuit of influence is a continuous, background effort not confined to "influence operations". It is labour as well as resource intensive, built on local knowledge, the cultivation of individuals and the long-term development of networks.*[73]

Many experts take the view that Russia's approach to the information counter-struggle has been constantly evolving, developing and adapting, and others believe that in the process it has become refined and tailored.[74]

The Soviet-era experience of the use of "active measures" and intimidation has been adapted and elaborated for modern use.

To sum up, the Soviet-era experience of the use of "active measures" and intimidation has been adapted and elaborated for modern use. Asymmetric tools that can be outsourced to various actors are attractive for projecting Russian national power due to their low cost and wide availability, a degree of anonymity and stealth, low risk of escalation, and great destabilising potential.[75] What perhaps distinguishes Russia is that asymmetric activities are highly integrated with one another, and coordinated with conventional operations in early and defining phases of military conflict (e.g. kinetic operations in Georgia and Crimea).[76]

3.3 The four lines of action

Russia's "defensive approach" in cyberspace is executed across four lines of action: strengthening Russia's "cyber sovereignty"; increasing control of information, including in the internet; exploiting open society, including freedom of expression; and preparing the cyber domain for military activity, including preparing the battleground.[77]

In addition to regulations and other measures that grant to the Kremlin the control over the cyberspace content, Russia plans to invest in cyber resilience and "cyber sovereignty". The Information Security Doctrine of 5 December 2016 states that "in the field of strategic stability" Russia will develop "a national system of the Russian internet segment management". The Russian military intranet already relies on domestic software and hardware and is not connected to the global internet. In line with the aim to decrease technological dependence on other countries, the objective is to foster the production of domestic hardware and software.[78] By 2020 Russia plans to route almost all internet traffic inside the country, and to build "back-ups" and duplicates of critical infrastructure, as well as to increase government control of internet domains and internet traffic exchange points. The aim is to increase "Russian independence within the network and prevent … unfriendly actions against the country undertaken by using the Internet."[79] A joint project is being undertaken by the BRICS countries (Brazil, Russia, India, China and South Africa) to build a high-capacity underwater fibre-optic cable to reduce their dependence on existing global communications infrastructure, which will strengthen their cyber sovereignty. Furthermore, Russia has declared plans to build by 2018 together with the BRICS countries an

[72] Sherr, op. cit.
[73] Sherr, op. cit.
[74] For example, Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016); Emilio Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea", *Parameters* 47(2) (Summer 2017): 51–63.
[75] Alina Polyakova et al., *The Kremlin's Trojan Horses 2.0* (Washington DC: The Atlantic Council, November 15, 2017) (accessed February 1, 2018).
[76] Seely, "Defining Contemporary Russian Warfare".
[77] For discussion on Russia's four lines of effort, see Kukkola et al., op. cit.
[78] Ministry of Foreign Affairs of the Russian Federation, "Doctrine of Information Security of the Russian Federation," approved by Decree of the President of the Russian Federation No. 646, December 5, 2016, accessed February 1, 2018.
[79] Peter Roudik, "Russian Federation: State Control of Internet Proposed," *Library of Congress*, March 1, 2016 (accessed February 1, 2018).

alternative Domain Name System.[80] These steps will reduce Russia's interdependence with global networks fostering its cyber resilience and deterrence by denial.[81] The flip side is that reduced dependence on global networks enables the Kremlin to conduct destructive attacks against the internet's core protocols and infrastructure (e.g. the TCP/IP Protocol Suite, the Domain Name System (DNS), routing protocols, communication cables) if such are deemed by the Kremlin to help them achieve strategic goals.[82]

Some experts believe that Russia is preparing for high-end cyber-attacks in the West. There are reports that Russian hacker-affiliated malware (Havex, BlackEnergy) has been discovered in the US electricity grid, and UK intelligence authorities confirm that Russia has infiltrated Britain's energy, telecommunications and media sector.[83] Implementing malware in critical infrastructure may indicate an attempt to prepare the battleground. Both Russia and China invest large amounts in the development of artificial intelligence and quantum computing that can potentially lead to an increase in the number of cyber-attacks against the West.[84] However, other experts observe that so far Russia has avoided escalation in cyberspace, and opted for cyber-attacks "below the threshold of activity that would justify a forceful response," but with greater strategic autonomy in cyberspace, Kremlin's calculation may change.[85]

A Russian military thinker states that in future conflicts information and cyber warfare will merge into a single whole.[86] The Western experts show that Russia is bringing together information warfare, cyber warfare and electronic warfare approaches. A case of point is that in 2014 Russia used electronic warfare tools to block mobile phone communications and facilitate the spread of disinformation (via text messages) to Ukrainian armed forces personnel in Ukraine.[87] Russia's electronic warfare tools were prominent also in the "Zapad-2017" military exercises. Looking at Russia's military and information warfare activities in Georgia in 2008 and in Ukraine since 2014, Stephen Blank judges that Russia's military has fully integrated cyber and psychological operations with conventional operations.[88] This view is shared also by Martin Libicki, who recommends that also the US should integrate intelligence, surveillance, reconnaissance, psychological operations, cyber operations, and electronic warfare into a whole.[89]

So far Russia has avoided escalation in cyberspace, but with greater strategic autonomy in cyberspace, Kremlin's calculation may change.

Russia has publicly declared that it has added "information warfare troops" to "protect the national defence interests and engage in information warfare" and fend off enemy cyber-attacks to military.[90] However, exact details of their mission, role and functions are not disclosed. It is well known that Russian security agencies have high-end cyber capabilities, and as discussed earlier in this paper, the Russian government outsources cyber-attacks to cyber criminals and IT-companies and other unconventional tools of state power. Many complain that Russia

[80] Patrick Tucker, "Russia Will Build Its Own Internet Directory, Citing US Information Warfare," *Defense One*, November 28, 2017 (accessed February 1, 2018).

[81] Deterrence by denial operates by convincing an adversary that the benefits it seeks will be denied due to effective defences. Deterrence by cost imposition operates through a credible threat of such a degree of retaliation that the attacking state would find it prohibitively costly to initiate the unwanted activity. See Schmidle et al., "Nonlethal Weapons and Cyber Capabilities".

[82] Transmission Control Protocol/Internet Protocol (TCP/IP) ensures that packets of information arrive at the right destination.

[83] Nell Nelson, "The Impact of Dragonfly Malware on Industrial Control Systems", SANS Institute, January 18, 2016, (accessed February 1, 2018); Andy Greenberg, "Hackers get direct access to US power grid controls," *Wired*, June 9, 2017 (accessed February 1, 2018); "UK cyber-defence chief accuses Russia of hack attacks," *BBC News*, November 15, 2017 (accessed February 1, 2018).

[84] Michelle Cantos, "What Artificial Intelligence in Hands of Adversaries Means for Cyber Defense," *Nextgov*, 24 November 24, 2017 (accessed February 1, 2018).

[85] Lewis, "Fighting the Wrong Enemy".

[86] In this paper, the following definition is used: "Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks." "Cyber Warfare", RAND Corporation, accessed February 1, 2018; Kiselyov, "What kind of Warfare Should the Russian Armed Forces Be Prepared for?".

[87] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn: ICDS, September 2017) (accessed February 1, 2018).

[88] Blank, "Cyber War and Information War à la Russe".

[89] Libicki, "The Convergence of Information Warfare."

[90] Morgan Chalfant, "Russia adds 'information warfare' troops", *The Hill*, February 22, 2017 (accessed February 1, 2018).

surprised the West with its innovative use of information warfare, yielding strategic-level effects (e.g. the US presidential elections).

Stephen Blank holds that Russia used cyber-attacks in Georgia and Ukraine to inhibit reactions by these countries and third parties, and in order to compel and deter them.[91] Other scholars remain sceptical that low-level cyber-attacks can be used as an effective tool of coercion.[92] Yet others believe that long-term low-level cyber-attacks can cumulatively produce large-scale damage. In any case, coercion in cyberspace appears different from the conventional concept of coercion in International Relations literature. In order to compel someone to change their behaviour through a cyber-attack, the target should know that the attack is coming, and they should also be able to avoid the attack by changing their behaviour. These conditions are not fulfilled in cyberspace, where cyber-attacks usually give little early warning and victims cannot avoid them by concessions to an adversary.

Russia's practice confirms that cyber-attacks are attractive tools for authoritarian states to project national power and support other political influence activities.

Be that as it may, it seems that at least some cyber-attacks that have been attributed to Russia affected the cognitive dimension. It has been suggested that the motivation of the hackers who caused blackouts in Ukraine in December 2015 was to demonstrate offensive capabilities, to signal coercion, and to retaliate for the electricity supply to Crimea being cut off a month earlier. It is possible that intimidation was also the main objective behind cyber-attacks against the Ukrainian financial sector in 2015-6 causing delayed payments and economic costs, and behind ExPetya/notPetya and BadRabbit malware that similarly caused financial losses for numerous victims in Ukraine.[93] Russian hacker-affiliated DDoS and other types of low-level cyber-attack against Estonia in 2007 and Georgia in 2008 also fit into the pattern of influence and intimidation.

In regards with attribution, cyber security firms have published reports with technical and operational details about various APT campaigns that they have attributed to Russian interests, but politically- and profit-motivated hackers often use the same malware, and phases of execution (cyber kill chain) are the same in both types of attack.[94] The difficulty in attributing cyber-attacks with high levels of confidence, and the imperfect fit of traditional concepts with cyberspace that were discussed earlier, means the analysis of nation-state-initiated cyber-attacks for political influence purposes remains methodologically difficult. In the future, past cyber-attacks should be analysed more extensively in order to understand their strategic effects, considering who was targeted, what type of attack it was, how and why the attack was executed, what was its impact, and the relationship of the attack to other influence activities and strategic goals. One possibility to improve this type of analysis is to describe at the operational level cyber-attack characteristics and combine this with analysis of International Relations theory (deterrence, coercion, and influence). A better methodology would improve the understating of "the aims, elements and connecting threads of Russian strategy" that will bring greater clarity about its effectiveness.[95]

[91] Blank, "Cyber War and Information War à la Russe".

[92] Kostyuk and Zhukov, "Invisible Digital Front".

[93] In December 2016, the Ukrainian State Treasury, Ministry of Finance and State Pension Fund were subjected to cyber-attacks that delayed payments. ExPetya/notPetya mainly targeted Ukraine, and wiped data in June 2017 causing financial loss. BadRabbit targeted Ukraine and Russia in October 2017, and, according to Kaspersky, two campaigns were executed by the same hackers. The malware affected more computers in Russia than in Ukraine. It is possible that ExPetya/notPetya was reverse-engineered by Russian hackers to target Ukraine, but other explanations are also possible. See: Andy Greenberg, "New Ransomware Linked to NotPetya Sweeps Russia and Ukraine," *Wired*, October 24, 2017 (accessed February 1, 2018).

[94] The main phases of cyber-attacks are preparation, execution and monetisation (i.e. collecting the gains).

[95] Cyber-attack characteristics are: targetability, controllability, persistence, effect, covertness and mitigation. See Duncan Hodges and Sadie Creese, "Understanding Cyber-attacks", in *Cyber Warfare: A Multidisciplinary Analysis,* ed. by James A. Green (New York: Routledge, 2015): 33-60; Sherr, op. cit.

Conclusion

The unique nature of cyberspace makes it an ideal domain for low-end cyber-attacks and other cyberspace-enabled political influence activities. This paper has shown that cyber capabilities differ from kinetic weapons in many respects, and that conventional concepts fail to account for dynamics in this complex domain. Cyber espionage seems to have strategic effects, whilst low-end cyber-attacks tend to produce tactical and operational effects, however, together with psychological operations they can have strategic effects on national security. Cyber capabilities are used as "force multipliers" in military conflicts and in the grey zone between war and peace. In some cases, cyber-attacks likely have psychological effects on their own, but there is still little understanding about the cognitive effects. There is also little understanding about the strategic effects of cyber-attacks for national security and interstate relations. For this reason, past cyber-attacks deserve better scrutiny.

In respect of Russia's practice, this paper has shown that Russia does not apply a uniform cyber-attack strategy across all targets, but considers various opportunities innovatively as they emerge. Russia's practice confirms that cyber-attacks are attractive tools for authoritarian states to project national power and support other political influence activities. They can be used for the purpose of deterrence and coercion, but a better International Relations theory for cyberspace should be developed to should be developed to explain how cyber-attacks translate into deterrent or coercive effects. Quantitative and qualitative methods, and operational and strategic level analysis should be combined to develop a new theoretical and conceptual framework for understanding this fast-evolving domain and how the authoritarian states are exploiting it.

Cyber espionage seems to have strategic effects, whilst low-end cyber-attacks tend to produce tactical and operational effects, however, together with psychological operations they can have strategic effects on national security.

Follow us on:

facebook.com/ICDS.Tallinn
Twitter: @ICDS_Tallinn
linkedin.com/company/3257237

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

ISSN 2228-2076