Cybercrime and Punishment: Security, Information War, and the Future of Runet

Elizaveta Gaufman

7.1 INTRODUCTION

Cybersecurity is notoriously hard to define (Salminen 2018), especially given the possible macro and micro incarnations from cyber war to individual password theft (Nissenbaum 2005). This chapter operates from the assumption that digital security is a complex process of intertwining of practices and technology that ensure the undisturbed functioning of information and communication technologies for the everyday needs of individuals, protected from breaches of confidentiality and anonymity. While most countries' daily functions depend on their invulnerability to cyber disruptions, a state's potential to discipline and punish its citizens through digital surveillance has hardly been underestimated as well (Dupont 2008; Teboho Ansorge 2011; Morozov 2011). This chapter explores the influence of digitalization on security in Russia, touching upon the issues of governmental control, surveillance, information war, as well as the issue of (Russian) internet sovereignty. This chapter aims to show the discrepancies in Russian cyber politics at home and abroad, highlighting its struggle for more internet regulation that is seen by the Russian government as a panacea against perceived external attempts at regime change. At the same time, this chapter shows that despite seemingly formidable "cyber army" capabilities for external use, domestic surveillance and attempts to build a Great Russian Firewall are still lacking even though the law on the isolation of the Runet has been passed in April 2019 (for more, see Chap. 2).

E. Gaufman (✉)
University of Groningen, Groningen, Netherlands
e-mail: e.gaufman@rug.nl

An image of a hacker with a thick Russian accent hastily typing something into the computer has become a staple trope in popular culture from James Bond movies to Late Night Comedy shows. Despite the fact that cybernetics was considered for a long time a “reactionary pseudoscience that appeared in the United States of America (USA)” (Peters 2016), Soviet Union and later Russia discovered “possible military applications for computers.” Since then, Russia has been consistently ranked as one of the dominant cyber powers around the world (Clarke and Knake 2014) ostensibly capable to disrupt democratic elections, organize a protest movement, or shut down a government. As in many cases in Soviet Union, military needs propelled the development of an industry that soon spilled over into civilian use with unexpected consequences. Russian Internet, or Runet, has become a threat to “regime stability” in Russia to such a degree that Soviet practices of dissident citizen surveillance and banning of anti-regime statements have found their way back to Russia today.

Externally, Russia enjoys a status of a cyber superpower (Musgrave 2016), but domestically it is still struggling to create a fully national, digitally sovereign Runet (Ristolainen 2017) reinforcing the digitized reason of state regime (Bauman et al. 2014). So far, governmental attempts at policing and censoring the digital space have made its infrastructure more vulnerable to traffic disruption for private users and have slowed down the development of Russia’s internet industry. Moreover, increased government control that aims to rid the Russian cyberspace of “servers hosted in California,” has negative consequences for civil society, freedom of speech and privacy that would potentially restrict the services and flow of information to regular Russian internet users. This is, however, so far of little concern to the Russian government that aims at creating a fully Russian Net by the end of 2021 that would be completely independent from international internet infrastructure (Vedomosti 2016).

Even though destruction of critical infrastructure has always been a staple part of military strategy, it has been gradually conceptualized as a matter of national security during the Cold War and especially after 9/11 (Collier and Lakoff 2008; Aradau 2010). In the digital age, the notion of critical infrastructure has been expanded to mean not just power plants and bridges, but also banking systems and e-government with both “old” and “new” infrastructure susceptible to outside threats that, in turn, take the form of not only missiles and troops, but also computer malware and the proverbial hackers. If in the times of Lenin, one had to physically take over the telegraph station in order to organize a successfully revolution (Lenin 1969), nowadays a person with a messenger app like Telegram or WhatsApp installed in a smartphone far away from the social movement can seemingly do as much damage (Kow et al. 2016).

Third World War, according to numerous Russian scholars, is supposed to be informational-psychological (Samokhvalova 2011; Vladimirov 2013; Markov and Nevolina 2018; Kiselev 2015), which stands in sharp contrast with the Western fears of “Digital Pearl Harbors” and “Weapons of Mass Disruptions” (Hansen and Nissenbaum 2009). Russian Military Doctrine has

emphasized the need to develop armed forces and means for an “information confrontation” since 2010 (Kremlin 2010). This belief is partially rooted in various conspiracy theories that argue that “the West” is on a quest to destabilize Russia through corrupting Russian core values and its society (Gaufman 2017; Yablokov 2018). Russian conspiracies have their counterpart conspiracy in the West—the already-retracted Gerasimov Doctrine that is supposed to explain Russian information warfare as part of long-standing Soviet origin “active measures” that are supposed to undermine Western countries (Sanovich 2017; Galeotti 2018). The US Defense Intelligence Agency’s report on Russian Military Power even talks of how “Information Confrontation” is “strategically decisive and critically important to control its domestic populace and influence adversary states,” encompassing “Informational-Technical” (defense, attack, and exploitation) and “Informational-Psychological” (changing people’s behavior or beliefs in line with Russian’s government agenda) strategies (Defense Intelligence Agency 2017).

Moreover, continuous securitization of terrorist attacks has paved the way for governmental overreach in surveillance and the expansion of cyber capabilities—and not only in Russia (Eriksson and Giacomello 2007). Encryption technology and the Internet in general have been framed as a cesspit of, for example, terrorists and pedophiles—a rhetoric remarkably similar among surveillance proponents in the United States and in Russia (Gaufman 2017; Monsees 2019). Discursively linking the Internet with crime has worked remarkably well across the world, justifying the surveillance and policing of “trembling creatures” who use it. No wonder that the notion of security has become inextricably linked with the cyberspace. This chapter outlines the digital turn in the Russian government’s understanding of security that is primarily concerned with regime stability and curbing outside influence. Hence, its focus is on governmental control of the Internet, surveillance, cyber war, and the struggle for global internet governance à la Russe.

7.2 FREEDOM OF SPEECH VS. THE GOVERNMENTAL CONTROL OF THE RUNET

Most analysts contend that the Arab Spring was a driving force behind the Russian government’s attempts to put the Russian Internet under more stringent control emulating a Chinese model (Soldatov and Borogan 2015). Images of toppled dictators whose grip on their countries seemed unwavering must have sent shockwaves through the Kremlin, where it was now obvious that the Internet could be more than just kitchen talk 2.0. Evidence of massive resources that have been invested in regulating and penetrating the Russian blogosphere since 2010–2011 shows that the Russian leadership was also keenly aware of the influential role played by new media in shaping public opinion and wasted no time trying to “manage” them. The government’s attitude toward new media would appear to be encapsulated by the famous phrase used in early

2012 by Stanislav Govoruhin, then head of Putin's reelection campaign staff, who described the Internet as "a rubbish-dump controlled by *GosDep* (the US State Department)." And yet, the Russian government wastes no time making sure that the "dump" is under control.

Even before the protest wave of 2011–2012, there has been evidence of the government's involvement in Runet albeit not on a grand scale. During the 2011–2012 elections, Distributed Denial-of-Service (DDoS) attacks on oppositional websites, seemingly with state involvement, were registered by numerous independent organizations (Mikhaylova 2012). The 2012 "Kremlingate" scandal also showed that the Russian authorities had in fact gone much further than merely obstructing oppositional media, and that millions of rubles had been spent by the government with the aim of channeling online discussions in the desired direction (Karimova 2012; RFE/RL 2015; for more on history of this period of Runet, see Chap. 16).

The hacked correspondence between then head of the Agency for Youth Affairs Vasily Yakemenko and his deputy Kristina Potupchik demonstrated as early as 2011 and 2012 that a significant amount of budgetary funds was being spent on paying an "army of bots"—people paid to write online comments and posts on themes of interest to the government. These online warriors reportedly took their cue at least in part from the current discourse on *Russia Today* (RT) and *Pervyj kanal* (Delovoi Peterbrug 2014). An ad hoc 50-ruble commentary has transformed into a large company—the now-infamous Internet Research Agency—that employs people on a regular basis and supplies pro-Kremlin content at home and abroad. Pro-Kremlin-paid internet commentators are the frequent butt of jokes. For example, a cartoon by an oppositional caricaturist Ėlkin shows an internet user measuring his online speed based on the number of "Kremlin-bot" comments appearing on a particular post (Radio Svoboda 2014). The amount of financing that went and is still going into paying for pro-Kremlin commentators and bloggers shows that the Kremlin considers online public sphere an important battlefield. Only the battlefield has also moved outside of Russia as well, with the so-called Kremlin trolls "invading" other countries (see below Cyber War).

The Russian government has been steadily trying to tighten the grip on the Internet for the fear of violent regime change reminiscent of the Arab Spring. The Federal Service for Supervision of Communications, Information Technology and Mass Media or Roskomnadzor that is tasked with implementation and enforcement of laws on mass media is the Russian federal executive body that in practice carries out censorship in media and telecommunications, encompassing electronic media, information technology (IT), and telecommunications. Technically, Roskomnadzor is also supposed to be overseeing compliance with the law protecting the confidentiality of personal data, but, in reality, it cooperates with state law enforcement agencies such as FSB (*Federal'naâ služba bezopasnosti*, Federal Security Service) in order to carry out surveillance tasks (Soldatov and Borogan 2013; Ermoshina and Musiani 2017), often under the guise of anti-terrorism measures.

However, a more radical to date attempt to enforce the “anti-terrorist” concerns on the Runet was far from successful. “Telegram” is a cloud-based instant messaging app developed by the creator of Russia’s most popular social network VKontakte Pavel Durov. Telegram is one of the most popular messaging services in Russia and especially in Moscow, with many media personalities and celebrities having their own “channel.” On April 13, 2018, Telegram was banned in Russia by a Moscow court, due to its refusal to grant the Federal Security Service access to encryption keys needed to view user communications as required by federal anti-terrorism law. On the morning of April 16, Roskomnadzor began sending out requests to providers to block Telegram.

At first, the department demanded to stop access only to the Internet Protocol (IP) addresses of the servers of the messenger itself. In the first days, millions of Amazon and Google cloud services IP addresses were added to the registry of banned websites, which Telegram ostensibly used to bypass blocking. Gradually, these addresses were unlocked, but Roskomnadzor’s attempts created a lot of disruptions in the everyday life of ordinary Russian businesses from flower delivery to online education and had a “Barbra Streisand effect” on the popularity of Telegram itself: Telegram’s traffic increased by a third in the first month, while the number of app downloads for Android jumped twice (Meduza 2019a). The Telegram ban debacle has shown that Russia is deeply integrated into the global digital ecosystem, and because international finance and commerce rely heavily on automated solutions that generate cross-border traffic, it would be difficult and costly to create an Internet kill switch. Moreover, with a wide availability of Virtual Private Network (VPN) technology, it is easy to circumvent the ban by getting access to transnational traffic, thus making Runet far from being behind a great wall.

From a governmental point of view, however, this represents a major security risk. Most of the legislation aimed at tightening the regulation of the Runet is presented as a means to protect the public from dangerous information or counter terrorist activity; for instance, the 2012 laws “*O zâsite detej ot informacii, pričînâjušej vred ih zdorov’û i razvitiû*” (On Protecting Children from Information Harmful to Their Health and Development and Other Individual Legislative Acts of the Russian Federation on the Issue of Limiting Access to Unlawful Information on the Internet). The same packaging was applied to the so-called Yarovaya law of 2016, a set of Internet regulations that took effect in July 2018. According to the new regulations, Internet and telecom companies are required to disclose communications and metadata, as well as “all other information necessary,” to authorities, on request and without a court order. However, amid the attempts of Roskomnadzor to ban Telegram, even some governmental officials and the head of *Russia Today* Margarita Simonyan kept using the messenger. Ordinary citizens have quickly realized that noncompliance with Internet laws has led to selective “like” and “share” persecution (Verkhovsky 2018, for more on digital law, see Chap. 5).

Several court cases highlight a selective application of punishment for digital “crimes.” Aleksandr Gozenko was convicted for “inciting hate speech” after

posting four comments in VKontakte, where he allegedly wanted to “organize a *vata*¹ Holocaust.” Other convictions, which information and analysis center SOVA for the monitoring of xenophobia deemed as “Inappropriate enforcement of anti-extremist legislation,” included posts or memes that contained political messages opposing the annexation of Crimea or proclaiming independence of some Russian subjects of federation (Verkhovsky 2018). One of the examples of “Like, Share, Repost, Prison” became particularly prominent when famous Russian rapper Oxxxymiron publicized a case against a 23-year-old Maria Motuznaya, who posted several anti-religious memes (Novaya gazeta 2018). It is also notable that the overwhelming majority of cases of “digital extremism” that are being prosecuted were committed in VKontakte, which is obligated by law to share private information with the law enforcement agencies. At the same time, social networks (Facebook and Twitter) presumably do not cooperate with Russian security forces and are being prosecuted for non-compliance with the Federal Law No. 242-FZ, which obligates foreign companies to store data of Russian users on servers within Russia (Burgess 2019).

Persecution and punishment of digital “crimes” are in part made possible due to cooperation between the Russian government and the internet infrastructure owners (Sivets 2018) such as hosting providers or other large IT companies. A similar infrastructure connection was observed during the crisis in Ukraine, when no sophisticated information warfare tools could be necessary given that Russia could gain physical control over the internet infrastructure in Crimea (Giles and Geers 2015). Most importantly, Russian government’s hold on the Runet is administered through control on three infrastructural levels. Firstly, Rostelecom, one of the main providers of broadband internet, already cooperates with Roskomnadzor, which means that Rostelecom would filter and block the content that violates Yarovaya law for instance. Secondly, given that local companies and platforms such as Yandex or VKontakte are much more popular than Google and Facebook, Roskomnadzor can regulate access to information through the Netoscope project, a database of unlawful websites on the Runet, in which both Yandex and VKontakte and a host of other Russian IT giants participate. Netoscope markets itself as a database of “malicious” websites and offers the service of “checking” a domain name to establish whether it can harm a user or not. Lastly, Roskomnadzor also has secured the cooperation of Technical Center “Internet,” which operates Main Registry of Runet’s Domain Name System (DNS) (Sivets 2018), which would be morphed into a national one under the new “sovereign internet law” (Stadnik 2019). But even without the sovereign internet, Roskomnadzor can already have a say in the information flows as DNS translates Uniform Resource Locators (URL) into IP address and acts as a type of “phonebook” that Roskomnadzor is allowed to edit. Thus, governmental control of the Runet is much more tangible, and “surgical strikes” of digital speech prosecution create a lot of press coverage, but at the same time the Russian government lacks the resources so far for comprehensive digital surveillance.

7.3 SURVEILLANCE

During the Soviet era, a seemingly omnipotent ability of the state to spy on the population became a source of numerous precautions and jokes. Soldatov and Borogan (2015) even preface their book *The Red Web* with the Russian saying “It’s not a telephone conversation”; this reflected a Soviet-era fear of surveilled device communication and general distrust of technology that was operated by the state. Jokes about microphones hidden in ashtrays and electric plugs where “Comrade Major” is listening to the conversations people have in the privacy of their kitchens have survived to this day. It turned out, however, that “Comrade Major” has been listening not only in the Soviet Union.

In 2013, Edward Snowden leaked a cache of documents to the media that documented the existence of classified surveillance programs run by the US National Security Agency (NSA) in cooperation with secret services of other major Western powers. Snowden revelations became a turning point in the discourse on digital security and surveillance (Bauman et al. 2014). Proponents of the “net delusion” argument (Morozov 2011; Paltemaa and Vuori 2009; Dupont 2008; Golkar 2011), who argued that the Internet represents an easy tool for the government to surveil and control the population, were vindicated given the scope and reach of the surveillance programs and their potential for governmental overreach, including opposition repression as opposed to “Twitter Revolution” techno-optimists who believed in the purely emancipatory power of the Internet.

Soldatov and Borogan note that the Russian state does not have the capabilities to carry out mass surveillance that would be comparable to the scope of the NSA’s reach (Soldatov and Borogan 2015). Russian “SORM” (*Sistema tehničeskikh sredstv dlja obespečeniâ funkcij operativno-razysknyh meropriâtij*, System for Operative Investigative Activities) is the system designated for lawful interception interfaces of telecommunications and telephone networks that enables the targeted—but not mass—surveillance of both telephone and Internet communications in Russia. SORM was first implemented in 1995 to allow access to surveillance data for the FSB, but during Vladimir Putin’s first week in office on January 5, 2000, the law was amended to allow seven other federal security agencies (apart from the FSB) to access to data gathered via SORM, including Ministry of Internal Affairs, Border patrol and customs, Police and Russia’s tax police. The legality of the SORM legislation has always been questioned, and in December 2015 the European Court of Human Rights ruled unanimously that that Russian legal provisions “do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance,” especially given that this risk “is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications,” thus violating Art. 8 of the European Convention on Human Rights that stipulates a right to respect for one’s “private and family life, his home and his correspondence” (European Court of Human Rights 2015).

Nevertheless, even the aforementioned “Yarovaya Law” and the expansion of the grounds for addition to the list for blocked Internet sites in Russia were supplemented with further legislation and measures. The national project “*Cifrováá ékonomika*” (Digital Economy) is yet again framed as an initiative that would ensure that the Runet does not contain dangerous sites for children, and at the same time identify customers of communication services and protect the users of the Internet of Things devices. An innovation in the trillion ruble national project is an obligatory installation of domestic antiviruses on personal computers manufactured and imported to Russia that already raises concerns that this measure would further commercial interests of select few governmentally approved companies that would most likely cooperate with security services (Zhukova et al. 2018). In the course of the project, a national traffic filtering system with a “white list of Internet-friendly resources for children” is supposed to be created by December 31, 2021, executed by Roskomnadzor and security agencies such as the Ministry of Internal Affairs and the FSB.

Also, according to the state program “*Informacionnoe obščestvo*” (Information Society), the goal is to have 90% of Internet traffic transmitted domestically (as opposed to 70% in 2014). Russian Minister of Culture Medinsky even stated that in the future, he guarantees that people will have to show their passport to “enter Internet,” not just in Russia, but around the world as well (Kommersant 2019). Medinsky offered the one option for the Internet policing that is being developed in the Digital Economy national project that would potentially work like parental control on devices—only the Russian government and Roskomnadzor being the “parents.” Another option, however, remains, which is the Chinese “Great Firewall”—completely encapsulating and monitoring the Runet, creating a Russian digital panopticon with endless possibilities for governmental overreach (Veeraraghavan 2013; Teboho Ansoorge 2011). Experts agree that both options seem to be on the table in the Kremlin (Soldatov and Borogan 2013; Zhukova et al. 2018). In either case, these measures will increase the possibilities and capabilities for mass surveillance.

7.4 CYBER WARFARE VS. INFORMATION WARFARE

An apocalyptic vision of cyber war that involves financial market crashes, power plant meltdowns and financial collapse came to be as a warning tale from military experts amid the overwhelming enthusiasm about the Internet (Clarke and Knake 2014). This vision, however, has been amended in the policy world by the notions of “hybrid war” and “active measures” (Charap 2015; Johnson 2018; Seely 2017; Biscop 2015). The latter one references a Soviet-era term for the actions conducted by Soviet security services such as KGB (*Komitet gosudarstvennoj bezopasnosti*, Committee for State Security,) by means of media manipulation and various degrees of violence (Johnson 2018). Most scholars contend that “hybrid war” is not new or unique to Russia (Galeotti 2016; Renz 2016; Polese et al. 2016) and should not lead to panic over

YouTube cartoons about girls and bears² that can somehow indoctrinate its audience to love Putin (Galeotti 2017). While cyber warfare has been viewed in Clausewitzian terms of critical security infrastructure strikes (Rid 2012), information warfare or its more Russia-specific designations such as “hybrid war” and “active measures,” common among Kremlin critical journalists, had had much less coverage until 2007.

The Estonian Bronze Soldier controversy has become patient zero in the modern cyber war discussion (Hansen and Nissenbaum 2009). In 2007, Estonian authorities decided to remove *Alšša*, a bronze statue in the center of Tallinn that commemorated the Soviet soldiers who fought against Nazi troops in World War II. The statue was widely seen as a symbol for Soviet occupation by many Estonians (Brüggemann and Kasekamp 2008). After the statue was relocated to a military cemetery, there were several waves of protest, both in Estonia and in Russia (Herzog 2011). Demonstrations in front of the Estonian embassy organized by the pro-Kremlin youth movement *Nashi* (Our people), an attack on the Estonian ambassador in Moscow, and finally a cyberattack on the Estonian government showed a certain degree of popular outrage, in which the role of the Russian government was seen as encouraging, if not sponsoring (Ottis 2008; Herzog 2011).

Ottis identified a clear political angle of the malicious traffic that was the core of cyberattack (Ottis 2008). For instance, malformed queries directed at the Estonian government included Russian-language swearwords calling the Estonian prime minister a “faggot” and a “fascist.” At the same time, instructions of how to attack Estonian governmental websites were scattered across Russian-language websites and even relatively primitive denial of service attack (the so-called ping flood) could have caused considerable trouble. While Ottis did not identify Russian government’s direct involvement into the attacks, he also notes that it did nothing to mitigate them, that is, to dial down the public outrage about Estonia and condemn the “patriotic” cyberattacks. Herzog also emphasizes that the Estonian cyberattack milestone showed that virtually untraceable “hacktivists” may now possess the ability to disrupt or destroy government operations. Alternatively, Rid (2012) has pushed against the designation of Estonian cyberattacks as “cyber war” as it fails to meet Clausewitz’s war criteria of being violent, instrumental, and politically attributed. Balzacq and Cavelti (2016) also offer the conceptualization of “cyber incidents” instead of “cyber war” with the latter notion being the result of a securitization process of deliberate disruptions of normalized cybersecurity practices.

While other cyberwarfare weapons, such as Stuxnet,³ have significantly changed the way policy and academia discuss cyber war (Langner 2011; Collins and McCombie 2012), it is Russian “disinformation campaigns” that have made headlines all over the world, spurring the development of different working groups and projects that assess the impact of pro-Russian narratives in Western countries, such as North Atlantic Treaty Organization’s (NATO), NATO Strategic Communications Centre of Excellence (StratCom COE), Center for European Policy Analysis, Australian Renewable Energy Agency

(ARENA), and numerous computational propaganda projects. The most widely publicized ones had at best murky methodology (such as Hamilton 68) or were quickly discredited (such as PropOrNot). However, as Sanovich notes,

tools like bots and trolls were developed ... to jam unfriendly and amplify friendly content and the inconspicuousness of trolls posing as real people and providing elaborate proof of even their most patently false and outlandish claims. The government also utilized existing, independent online tracking and measurement tools to make sure that the content it pays for reaches and engages the target audiences. Last but not least, it invested in the hacking capabilities that allow for the quick production of compromising material against the targets of its smear campaigns. (Sanovich 2017)

According to several journalistic investigations (Delovoi Peterburg 2014; Seddon 2014; RFERL 2015), there is a special “troll army,” that is, a team of fake internet bloggers who are hired to promote pro-Kremlin discourse. After the leak of the “bot manuals,” even a regular internet user is able to track identical comments that pollute social networks (Gunitsky 2015). Kremlin trolls are not “classic” trolls identified in the literature: even though Kremlin trolls may end up emotionally provoking the audience, their main purpose is an ideological one, while regular trolls are usually devoid of ideology (Hardaker 2010). Kremlin trolls are real people who are paid to promote Kremlin-friendly discourse.

NATO StratCom COE identifies six criteria for Kremlin trolls (2016), including being consistently pro-Russian and posting repetitive messages and not purpose-made context. Some of these criteria are helpful, but again require close-reading, which is usually impossible in large-scale data sets and still employ are rather high level of bias (NATO StratCom COE 2016). Moreover, these criteria are not applicable to targeted advertising on Facebook that was allegedly part and parcel of the Russian interference in the American presidential elections in 2016. Apart from IP data that StratCom COE used, it is hard to determine whether the person is a paid troll or not definitively. This was one of the caveats that was problematic for PropOrNot and partially for Hamilton 68. Moreover, the cited study analyzed specifically comments to popular Latvian news agencies, such as DELFI, and this methodology is not always applicable to the analysis of social networks due to design of these platforms.

Attribution in cyberspace remains one of the main challenges. It normally follows the “cui bono” (“to whom is it a benefit?”) logic, but one would always be uncertain about the identity of the perpetrator(s) (Baezner and Robin 2017), especially given that some cyber activists do not act on governmental orders—which has been the official line of the Russian government when accused of acts of cyber war. “Patriotic Hacking” is not unique to Russia as evidenced by #OPvijaya cyberattack on Pakistani governmental websites and governmental initiatives in several Asian countries to promote cyber privateering (Hare 2017). However, it was an issue related to Russian foreign policy that put cyber war on international security and NATO’s radar.

The “hacktivist” defense was used also in the case of alleged Russian interference in the US elections in 2016. US intelligence agencies and several private cybersecurity firms identified two groups with alleged ties to FSB and GRU (*Glavnoe razvedyvatel'noe upravlenie*, Main Intelligence Directorate), that were involved in the hacking of the Democratic National Committee (DNC). Two groups, Advanced Persistent Threat (APT) 29, aka Cozy Bear, and APT 28, aka Fancy Bear, penetrated the servers of the DNC and leaked private communications that had a damaging effect on Donald Trump’s rival in the presidential campaign—Hillary Clinton (Polyakova and Boyer 2018). During the 2018 Helsinki summit between President Trump and President Putin, Russian president insisted that the Russian state has never interfered and does not interfere in elections in other countries. Further, he admitted that some Russians could have sympathized with Trump, since during his election campaign he was in favor of improving ties with Moscow, and those people acted on their sympathies (Khimshiashvili 2018).

The Report by the US Office of the Director of National Intelligence “Assessing Russian Activities and Intentions in Recent US Elections” claimed that it was President Putin who directed the hacking activities, with the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) confirming this with “high confidence” and the NSA with “moderate confidence.” Moreover, the Report went even further and documented not only hacking activities and trolling by the Internet Research Agency, but also some of the articles and reporting by *Russia Today* and *Sputnik* (Defense Intelligence Agency 2017). The report’s assessment of RT’s “Occupy Wall Street” documentary and critique of the US political system as “anti-American rhetoric” played into the hands of Russian interference skeptics: if a country prides itself in its freedom of speech, what kind of damage is a documentary on an anti-establishment movement supposed to do to a democracy? As Sanovich notes, maintaining the reputation of mainstream media and ensuring their objectivity, fairness, integrity and professionalism would be a much more effective defense against any kind of “active measures” (Sanovich 2017).

Sanovich’s argument rings especially true because the Russian government also relies on flooding technique in its information war effort, that is, governmentally affiliated mass media as well as Internet Research Agency trolls provide such an overwhelming amount of contradictory information that is difficult to parse (Roberts 2014). As Farrel and Schneier note, the goal is “to seed public debate with nonsense, disinformation, distractions, vexatious opinions and counter-arguments” (Farrell and Schneier 2018, 2019), and create, in Russian terms, “info-noise” that would fragment social reality and undermine public deliberation with a flurry of “alternative facts.” The problem here is that flooding is not a uniquely Russian or Chinese technique; it has become common place even in established democracies, with the United States being the birthplace of the “alternative facts” catchphrase in the first place. Can flooding on foreign ground be considered a cybercrime that warrants punishment? This is probably the assumption that led the Director of National Intelligence (DNI)

report to include *Russia Today* and *Sputnik* into the report on Russian interference into the American elections. Sanctioning content, however, is an authoritarian technique that most democratic countries cannot afford, and IT giants only recently began filtering outright false information such as anti-vaccine conspiracies (Matsakis 2019).

At the same time, the long arm of the Kremlin is often overestimated. The botched assassination attempt on the former Russian secret agent Skripal, in Salisbury, is a case in point, as the alleged killers' identities were established in a matter of days because of inadequate data protection (Bellingcat 2018). The "information noise" on the assassination attempt was performed in a much more efficient way with some journalists describing no less than 19 theories of the assassination and the head of *Russia Today* conducting an interview with the disclosed alleged assassins who pretended to be fitness coaches and dutifully described the beauty of Cathedral's spear in Salisbury.

While some departments of Russian Secret Services seem to possess a remarkable expertise (or a possibility to outsource it) in cyber warfare techniques including hacking, others have much less impressive record in information security. At the same time, the prosecution of hacker Hell (Sergej Maksimov) in Germany, who hacked and released private emails of the Russian oppositional politician Alexei Navalny, shows that outside of Russia cybercrime often ends in punishment. Similarly, in the United States, former US attorney for the Southern District of New York Preet Bharara prosecuted the infiltration and cyber theft of personal information from the database of J.P. Morgan Chase (Reuters 2015), as well as drug trafficking cases on the so-called dark web. These and several other cases show that despite the need to trace intricate trails of digital evidence across multiple international jurisdictions attribution and punishment for cybercrimes is possible.

7.5 INTERNET SOVEREIGNTY

After Edward Snowden blew the whistle on the scope of American mass surveillance, the US government charged him with theft of government property and two counts of violating the Espionage Act of 1917 through "unauthorized communication of national defense information" (Espionage Act, section 793(d)) and "willful communication of classified communications intelligence information to an unauthorized person" (Espionage Act, section 798(a)(3)). Eventually, he found temporary political asylum in Russia, a country hardly famous for its liberal internet governance, but probably one of the very few countries that does not have an extradition agreement with the United States and granted Snowden asylum. By harboring Snowden, Moscow seemingly had a good hand to renegotiate global Internet governance as he provided first-hand data of governmental surveillance overreach that extended well beyond US borders and threatened other countries' digital security.

The Russian government has a realist state-centric understanding of the cyberspace that is supposed to have its borders, sovereignty, and

nonintervention (Nocetti 2015), a type of digital Westphalia (Zinovieva 2013) with separate “national” Internets and principles of nonintervention. This view is not uniquely held by Russia; the Snowden revelations did indeed push many countries around the world to engage in digitized geopolitics, where cyberspace is a battlefield and each country needs to build up their cyber defenses (Bauman et al. 2014). Hence, it was rather frustrating for the Russian authorities that the United States had a joint responsibility with Internet Corporation for Assigned Names and Numbers (ICANN) to carry out the Internet Assigned Numbers Authority (IANA) overseeing global IP address allocation until 2016. This perception of the Internet was vocalized by Putin, who called it a “CIA project” and by numerous Russian officials who had blamed Russian waves of protest on social networks “whose servers are hosted in California.” With ICANN’s headquarters being indeed in California, its independent nongovernmental status is questioned by other countries as well (Becker 2019).

Runet can, however, potentially do without the overseas servers. Most researchers note that Runet is a self-contained linguistic and cultural environment with its own well-developed search engines, social networks, and messenger services and software products often imported to other countries (Price 2017; Asmolov and Kolozaridi 2017). Introduction of Cyrillic domain addresses was a notable breakthrough after years of Latin script domination. The preparation and testing of the .рф domain started in 2007 by registrar RU center and proceeded as an application to ICANN. In January 2010, ICANN announced that the domain was one of the first four new non-Latin country code top-level domains to have passed the Fast Track String Evaluation and the domain became operational on May 13, 2010, with two websites: for the president of Russia and for the government of Russia. As of the moment of writing, the .ru domain is still approximately five times more popular than its Cyrillic counterpart. While the introduction of Cyrillic domain names could be seen (and framed) as an emancipatory move to decolonize the Internet (Leslie 2012; Farivar 2011), so far it just implemented a higher level of Russian state influence that does not necessarily have an emancipatory agenda.

Moreover, Russian government tried to forge alliances with China, Saudi Arabia, Egypt, and United Arab Emirates in order to promote a more centralized and controlled vision for the global Internet, specifically trying to introduce global Internet governance at an International Telecommunications Union (ITU) conference in 2012. This attempt was unsuccessful given the opposition from most Western countries including the United States, whose representative insisted that the conference was not supposed to deal with the issue of internet governance or the fact that it was supposed to be carried out through ITU, because that would potentially open the door to content censorship (Fitzpatrick 2012). Even further, when Russian Minister of Communications Nikiforov provided remarks in Brazil’s NETmundial conference calling to hand over the power from ICANN to ITU in light of the Snowden revelations about American mass surveillance, his speech was not even included into the conference documents. Even though several authoritarian countries are eager to

support Russian proposals for a more regulated cyberspace, with the United States so far standing behind an “Internet Freedom” agenda (Price 2017), it is unlikely that Russian suggestions will be implemented. Moreover, Deputy Head of the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation Aleksej Volin remarked during a MediaForum in Shanghai, that Russia and China are looking at creating “alternative” social networks and messengers that would rival its Western analogues (RIA Novosti 2018) if Twitter, YouTube, and Facebook keep on filtering Russian and Chinese media out.

7.6 CONCLUSION

Cybersecurity à la Russe is marked by the authoritarian nature of the state that is primarily concerned by the question of regime survival. This logic motivates both external and internal double-pronged strategy of digital security, or, as Yatsyk succinctly puts it, “to hack abroad and ban at home” (Yatsyk 2018). While externally Russia enjoys an image of a cyber superpower, seemingly capable of unseating heads of state, Russian government’s attempts at controlling the cyberspace have not been quite as successful yet; that is why the government relies not only on filtering content, but also on flooding the information space both at home and abroad. Governmental surveillance capabilities are much less formidable, and filtering content is not particularly effective as the recent struggle to ban Telegram showed. Current attempts by the Russian government at making Runet independent from foreign traffic are especially worrisome because without the reliance on the “servers in California,” the ones in Moscow can be switched off albeit with significant political and economic costs. In the end, using the Internet is a matter of national security, according to Putin:

They [the Western intelligence agencies] are sitting there, it’s [the Internet] their invention. And everyone listens, sees and reads what you say, and accumulates defense information. And [once we have sovereign internet] they won’t. (Putin 2019)

This chapter provided the overview of the digital security strategy in Putin’s Russia. The law that is supposed to isolate Runet is officially on “ensuring safe and sustainable functioning of the Internet” on the Russian territory, echoing digital security’s stated main concerns (Meduza 2019b). At the moment of writing, it seems that the main purpose of the Russian government is to emulate the Chinese model and create the self-sustaining sovereign Runet that is independent of foreign infrastructure. This is in part motivated by the considerations of regime stability and the overwhelming perception in the Russian government that the Internet and social media could be used as a “crowbar” for regime change facilitating social mobilization of opposition groups. Viewing the Internet as a tool of criminals is not unique to Russian authorities but, at

the same time, this perception leads to the continuous securitization of cyberspace in Russia and legitimizes acts of information war and cyberattacks. Moreover, existing difficulty in prosecuting digital security offences will likely leave alleged cybercrimes of Russian secret services without punishment.

NOTES

1. Somewhat derogatory term that is supposed to mean the supporters of the Kremlin's Ukraine policy, including Crimea annexation. The court decision "translated" this term as "Russian patriots," thus interpreting "vata" as a social group against said hate speech was used.
2. "*Maša i medved*" (Maša and the Bear) is a Russian fan fiction version of the Goldilocks fairytale, and is extremely popular on YouTube with over 26 million channel subscribers.
3. Stuxnet is a malicious computer worm, allegedly developed by American and Israeli intelligence service and first uncovered in 2010. Stuxnet is believed to be responsible for causing substantial damage to Iran's nuclear program.

REFERENCES

- Aradau, Claudia. 2010. Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 41 (5): 491–514.
- Asmolov, Gregory, and Polina Kolozaridi. 2017. The Imaginaries of RuNet. *Russian Politics* 2 (1): 54–79.
- Baezner, Marie, and Patrice Robin. 2017. *Cyber and Information Warfare in the Ukrainian Conflict*. ETH Zurich.
- Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. A Theory of Actor-network for Cyber-Security. *European Journal of International Security* 1 (2): 176–198.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob B.J. Walker. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8 (2): 121–144.
- Becker, Manuel. 2019. When Public Principals Give up Control over Private Agents: The New Independence of ICANN in Internet Governance. *Regulation & Governance* 13: 561–576.
- Bellingcat. 2018. Full Report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia. Accessed September 21, 2019. <https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/>.
- Biscop, Sven. 2015. Hybrid Hysteria. *Egmont Institute Security Policy Brief* (64).
- Brüggemann, Karsten, and Andres Kasekamp. 2008. The Politics of History and the "War of Monuments" in Estonia. *Nationalities Papers* 36 (3): 425–448.
- Burgess, Matt. 2019. Russia Takes Aim at Facebook and Twitter in a Bid for Online Control. *WIRED*. <https://www.wired.co.uk/article/russia-suing-facebook-twitter>.
- Charap, Samuel. 2015. The Ghost of Hybrid War. *Survival* 57 (6): 51–58.
- Clarke, Richard Alan, and Robert K Knake. 2014. *Cyber War*. Tantor Media, Incorporated.
- Collier, Stephen, and Andrew Lakoff. 2008. The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem. In *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*, 40–62. Routledge.

- Collins, Sean, and Stephen McCombie. 2012. Stuxnet: The Emergence of a New Cyber Weapon and its Implications. *Journal of Policing, Intelligence and Counter Terrorism* 7 (1): 80–91.
- Defense Intelligence Agency. 2017. Russia Military Power. Building a Military to Support Great Power Aspirations.
- Delovoi Peterburg. 2014. Trolli iz Ol'gino pereehali v novyj četyrëhëtažnyj ofis na Savuškina [Olginio Trolls Moved to a New 4-story Office Building on Savushkina]. *dp.ru*. October 28. Accessed March 22, 2015. http://www.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo/.
- Dupont, Benoit. 2008. Hacking the Panopticon: Distributed Online Surveillance and Resistance. In *Surveillance and Governance: Crime Control and Beyond*, 257–278. Emerald Group Publishing Limited.
- Eriksson, Johan, and Giampiero Giacomello. 2007. *International Relations and Security in the Digital Age*. Routledge.
- Ermoshina, Ksenia, and Francesca Musiani. 2017. Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. *Media and Communication* 5 (1): 42–53.
- European Court of Human Rights. 2015. *Roman Zakharov v. Russia*. Strasbourg: European Court of Human Rights.
- Farivar, Cyrus. 2011. *The Internet of Elsewhere: The Emergent Effects of a Wired World*. Rutgers University Press.
- Farrell, Henry, and Bruce Schneier. 2018. Common-Knowledge Attacks on Democracy. *Berkman Klein Center Research Publication* (2018-7).
- . 2019. Democracy's Dilemma. *Boston Review*. <https://bostonreview.net/forum-henry-farrell-bruce-schneier-democracys-dilemma>.
- Fitzpatrick, Alex. 2012. U.S. Refuses to Sign UN Internet Treaty. *CNN Business*. <https://edition.cnn.com/2012/12/14/tech/web/un-internet-treaty/index.html>.
- Galeotti, Mark. 2016. Hybrid, Ambiguous, and Non-linear? How New is Russia's 'new way of war'? *Small Wars & Insurgencies* 27 (2): 282–301.
- . 2017. Masha and the Bear are Not Coming to Invade your Homeland. In *Moscow's Shadows*. <https://inmoscowshadows.wordpress.com/2018/11/17/masha-and-the-bear-are-not-coming-to-invade-your-homeland/>.
- . 2018. I'm Sorry for Creating the 'Gerasimov Doctrine'. *Foreign Policy*, 5.
- Gaufman, Elizaveta. 2017. *Security Threats and Public Perception: Digital Russia and the Ukraine Crisis*. Basingstoke: Palgrave Macmillan.
- Giles, Keir, and Kenneth Geers. 2015. Russia and its Neighbours: Old Attitudes, New Capabilities. In *Cyber War in Perspective: Russian Aggression against Ukraine*, 19–28. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.
- Golkar, Saeid. 2011. Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran. *International Journal of Emerging Technologies and Society* 9 (1): 50.
- Gunitsky, Seva. 2015. Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. *Perspectives on Politics* 13 (01): 42–54.
- Hansen, Lene, and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International studies quarterly* 53 (4): 1155–1175.
- Hardaker, Claire. 2010. Trolling in Asynchronous Computer-mediated Communication: From User Discussions to Academic Definitions. *Journal of Politeness Research* 6 (2010): 215–242.

- Hare, Forrest B. 2017. Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy? *Asian Security* 15: 1–10.
- Herzog, Stephen. 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* 4: 1–13.
- Johnson, Robert. 2018. Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies* 29 (1): 141–163.
- Karimova, Anastasia. 2012. Kremlëvskaâ blogodel'nâ [Kremlin Blog Maker]. *Kommersant*. Accessed February 3, 2019. <http://www.kommersant.ru/doc/1868022>.
- Khimshiashvili, Polina. 2018. Razminočnyj sammit: kak prošla vstreča Putina i Trampa v Hel'sinki [Training Summit: How the Meeting between Putin and Trump in Helsinki Went]. *RBC, Politika*, July 16. https://www.rbc.ru/politics/16/07/2018/5b4c98d99a794739ea4c2e0a?from=materials_on_subject.
- Kiselev, V. 2015. Gibridnaâ vojna kak novyj tip vojny budušego [Hybrid War as a New Type of a Future War]. *Armejskij sbornik* 12.
- Kommersant. 2019. Medinsky predskazal vseмирnyj perehod na 'Internet po pasportu'. *Kommersant*. https://www.kommersant.ru/doc/3859694?utm_source=facebook.com&utm_medium=social&utm_campaign=amplifir_social.
- Kow, Yong Ming, Yubo Kou, Bryan Semaan, and Waikuen Cheng. 2016. Mediating the Undercurrents: Using Social Media to Sustain a Social Movement. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.
- Kremlin. 2010. Ukaz Prezidenta Rossijskoj Federacii ot 05.02.2010 № 146 O Voennoj doktrine Rossijskoj Federacii [Decree of the President of the Russian Federation from 05.02.2010 №146 On Military Doctrine Of Russian Federation]. <http://kremlin.ru/acts/bank/30593>
- Langner, Ralph. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy* 9 (3): 49–51.
- Lenin, Vladimir. 1969. Sovety postoronnego [Advice of a Stranger]. *Complete Works*, 34.
- Leslie, Christopher. 2012. *Decolonizing the internet*. London, England: SAGE Publications Sage UK.
- Markov, Yevgeniy, and Anna Nevolina. 2018. Rossiâ kak glavnyj ob"ekt sovremennyh informacionnyh vojn [Russia as the Main Target of Modern Information Wars]. *Historia provinciae—žurnal regional'noj istorii* 2 (3): 12–48.
- Matsakis, Louise. 2019. Facebook Will Crack Down on Anti-Vaccine Content. *Wired*. <https://www.wired.com/story/facebook-anti-vaccine-crack-down/>.
- Meduza. 2019a. Telegram v Rossii: kak na nëm otrazilas' popytka blokirovki? Skol'ko čelovek im pol'zuetsâ—i rastët li auditoriâ [Telegram in Russia: How Did the Blocking Affect it? How Many People Use it and Does it Audience Grow]. Accessed December 15, 2019. <https://meduza.io/feature/2018/08/07/telegram-v-rossii-kak-na-nem-otrazilas-popytka-blokirovki-skolko-chelovek-im-polzuetsya-i-rastet-li-auditoriya>.
- . 2019b. Zakonoproekt ob izolácii rossijskogo segmenta interneta predstavili v okončatel'noj redakcii. Vot kak èto budet rabotat' [The Bill on Isolating the Russian Segment of the Internet was Presented in its Final Version. This is How it Will Work]. Accessed December 15, 2019. <https://meduza.io/feature/2019/04/11/zakonoproekt-ob-izolyatsii-rossijskogo-segmenta-interneta-predstavili-v-okonchatel'noj-redaktsii-vot-kak-eto-budet-rabotat>.
- Mikhaylova, Lidya. 2012. Internet as a Battlefield in Russian Elections. *The Examiner*. Accessed August 6, 2019. <http://www.examiner.com/article/internet-as-a-battlefield-russian-elections>.

- Monsees, Linda. 2019. *Crypto-Politics: Encryption and Democratic Practices in the Digital Era* (Routledge New Security Studies), Routledge New Security Studies. Abingdon: Routledge.
- Morozov, Evgeny. 2011. *The Net Delusion: How Not to Liberate the World*. Penguin UK.
- Musgrave, Paul. 2016. If You're Even Asking if Russia Hacked the Election, Russia Got What it Wanted. *The Washington Post*, November 28.
- NATO StratCom COE. 2016. Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia. Full Report. <http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0>.
- Nissenbaum, Helen. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7 (2): 61–73.
- Nocetti, Julien. 2015. Contest and Conquest: Russia and Global Internet Governance. *International Affairs* 91 (1): 111–130.
- Novaya gazeta. 2018. Oksimiron prizval vyjti na miting v podderžku figurantov del iz-za memov vo 'VKontakte' [Oksimiron Urged to Go to a Rally in Support of Defendants in Cases on Memes in VKontakte]. *Novaya gazeta*, August 13. <https://www.novayagazeta.ru/news/2018/08/13/144149-oksiron-prizval-vyyti-na-miting-v-barnaule-v-podderzhku-figurantov-del-ob-ekstremizme-iz-za-memov-vo-vkontakte>.
- Ottis, Rain. 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In *Proceedings of the 7th European Conference on Information Warfare*.
- Paltemaa, Lauri, and Juha A. Vuori. 2009. Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet. *Asian Journal of Political Science* 17 (1): 1–23.
- Peters, Benjamin. 2016. *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. MIT Press.
- Polese, Abel, Rob Kevlihan, and Donnacha Ó. Beacháin. 2016. Introduction: Hybrid Warfare in post-Soviet Spaces, is There a Logic Behind? *Small Wars & Insurgencies* 27 (3): 361–366.
- Polyakova, Alina, and Spencer P. Boyer. 2018. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Brookings – Robert Bosch Foundation Transatlantic Initiative, The New Geopolitics: Europe.
- Price, Monroe. 2017. The Global Politics of Internet Governance. In *Technology and World Politics: An Introduction*. Routledge.
- Putin, Vladimir. 2019. Vstreča s predstaviteľami rossijskich informagentstv i pečatnyh SMI [Meeting with representatives of Russian news agencies and print media]. *Kremlin.ru*. Accessed September 21, 2019. <http://kremlin.ru/events/president/news/59865>.
- Renz, Bettina. 2016. Russia and 'Hybrid Warfare'. *Contemporary Politics* 22 (3): 283–300.
- Reuters. 2015. U.S. Charges three in Huge Cyberfraud Targeting JPMorgan, Others. <https://www.reuters.com/article/us-hacking-indictment/u-s-charges-three-in-huge-cyberfraud-targeting-jpmorgan-others-idUSKCN0SZ1VM20151110>
- RFERL. 2015. Russian Trolls' Vast Library Of Insulting Images. Accessed July 20, 2015. <http://www.rferl.org/content/russian-trolls-vast-insult-cartoon-database/26938435.html>.

- RIA Novosti. 2018. Volin rasskazal o napravleniâh sotrudničestva Rossii i Kitaâ v medi-
asfere [Volin Spoke about Russian-Chinese Areas of Cooperations in Media].
<https://ria.ru/20181104/1532107675.html>.
- Rid, Thomas. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies* 35
(1): 5–32.
- Ristolainen, Mari. 2017. Should ‘RuNet 2020’ Be Taken Seriously? Contradictory
Views about Cyber Security Between Russia and the West. *Journal of Information
Warfare* 16 (4): 113–131.
- Roberts, M. E. 2014. *Fear, Friction, and Flooding: Methods of Online Information
Control*. Doctoral dissertation, Harvard University.
- Salminen, Mirva. 2018. 2.10 Digital Security in the Barents Region. In *Society,
Environment and Human Security in the Arctic Barents Region*, 187–204. Routledge.
- Samokhvalova, Vera. 2011. Specifika sovremennoj informacionnoj vojny: sredstva i celi
poraženîâ [The Specifics of Modern Information Warfare: The Means and Targets of
Destruction]. *Filosofiâ i obšestvo* 3: 54–73.
- Sanovich, Sergey. 2017. Computational Propaganda in Russia: The Origins of Digital
Misinformation. Working Paper.
- Seddon, Max 2014. Documents Show How Russia’s Troll Army Hit America. *BuzzFeed
News*. Accessed September 21, 2019. [http://www.buzzfeed.com/maxseddon/
documents-show-how-russias-troll-army-hit-america#nxEvk1YVWZ](http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america#nxEvk1YVWZ).
- Seely, Robert. 2017. Defining Contemporary Russian Warfare: Beyond the Hybrid
Headline. *The RUSI Journal* 162 (1): 50–59.
- Sivetc, Liudmila. 2018. State Regulation of Online Speech in Russia: The Role of
Internet Infrastructure Owners. *International Journal of Law and Information
Technology* 27 (1): 28–49.
- Soldatov, Andrei, and Irina Borogan. 2013. Russia’s Surveillance State. *World Policy
Journal* 30 (3): 23–30.
- . 2015. *The Red Web: The Struggle Between Russia’s Digital Dictators and the
New Online Revolutionaries*. Hachette UK.
- Stadnik, Ilona. 2019. A Closer Look at the ‘sovereign Runet’ law. *Georgia Tech*. [https://
www.internetgovernance.org/2019/05/16/a-closer-look-at-the-
sovereign-runet-law/](https://www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/).
- Radio Svoboda. 2014. Karikatura dnâ na Radio Svoboda [Caricature of the Day on
Radio Svoboda]. Accessed December 15, 2019. [http://www.svoboda.org/con-
tent/article/26648017.html](http://www.svoboda.org/con-
tent/article/26648017.html).
- Teboho Ansorge, Josef. 2011. Digital Power in World Politics: Databases, Panopticons
and Erwin Cuntz. *Millennium* 40 (1): 65–83.
- Vedomosti. 2016. Runet budet polnost’û obosoblen k 2020 godu [Runet will be
Completely Independent by the Year 2020]. *Vedomosti*. [https://www.vedomosti.
ru/technology/articles/2016/05/13/640856-runet-obosoblen](https://www.vedomosti.ru/technology/articles/2016/05/13/640856-runet-obosoblen).
- Veeraraghavan, Rajesh. 2013. Dealing with the Digital Panopticon: The Use And
Subversion of ICT in an Indian Bureaucracy. In *Proceedings of the Sixth International
Conference on Information and Communication Technologies and Development*, Full
Papers—Volume 1.
- Verkhovsky, Alexander. 2018. Nepravomernoie primenenie antièkstremskogo
zakonodatel’sтва v Rossii v 2017 godu [Improper Use of Anti-Extremist Legislation
in Russia in 2017]. SOVA. Center for Information and Analysis.

- Vladimirov, Aleksandr. 2013. Osnovy obšej teorii vojny. Čast' I: Osnovy teorii vojny [Foundations of Common War Theory. Part I, Foundations of War Theory]. *Kadet.ru*.
- Yablokov, Ilya. 2018. *Fortress Russia: Conspiracy Theories in the Post-Soviet World*. John Wiley & Sons.
- Yatsyk, Alexandra. 2018. To Hack Abroad and Ban at Home: The Kremlin's Cyber Activism. In *PONARS Policy Memo*.
- Zhukova, Kristina, Vladislav Novyi, and Yulia Tishina. 2018. RuNet za stenoi: Kak nacproekt 'Cifrovaâ èkonomika' povliâet na pol'zovatelej interneta [RuNet Behind the Wall: How National Project 'Digital Economics' will Influence Internet users]. *Kommersant*. <https://www.kommersant.ru/doc/3773489>.
- Zinovieva, Yelena. 2013. Cifrovoj Vestfal'? [Digital Westphalia?]. In *MGIMO opinion*.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.