Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond

Joe Cheravitch
Doctoral Student
King's College London

Bilyana Lilly
Policy Researcher
Frederick S. Pardee RAND Graduate School
RAND Corporation

Abstract: While Moscow's willingness to launch cyber operations depends in no small part on how the Russian leadership interprets geopolitics, resources and personnel determine the ability to conduct them. Russia has demonstrated a capacity to craft sophisticated malware to support operations that range from espionage to disrupting critical infrastructure, to interfering in states' internal affairs through cyber-enabled influence campaigns, but the government still faces difficulties recruiting and retaining the needed technological talent to keep pace with its rivals. While some of the factors inhibiting the growth of Moscow's cyber programme are internal to the organisations tasked with executing them, such as a culture-clash between specialist recruits and the bureaucracy, the most significant impediments are exogenous to them and include brain-drain and the health of Russia's economy. Moscow's litany of perceived adversaries in cyberspace ensures continuous efforts by the state to prevent the emigration of computer science and IT specialists and expand the ranks of those serving Russia's offensive and defensive cyber capabilities. As evolving technologies like artificial intelligence and quantum computing carry implications for future cyber operations, Moscow's ability to marshal its resources to remain competitive in a furtive digital arms race similarly depends on many of these factors.

This chapter aims to address key questions arising from the probable gap that separates Russian cyber personnel and capabilities, especially technological innovation, from its ambitions and what effect this disparity might have on future state-backed cyber campaigns. It starts by accounting for different factors that affect the ability of Russia's military and security services to successfully expand recruiting and support technological innovation related to cyber operations. This is followed by an examination of various initiatives and strategies that Russian agencies have introduced to address Russia's cyber limitations and cultivate technological innovation. Finally,

it discusses how Russia's current official policies and informal practices are likely to affect the nature of its cyber operations in the future and to what extent NATO and its members can leverage these limitations to achieve desired effects in the Alliance's cyber security efforts.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

1. INTRODUCTION

As states seek to build a capacity to defend against cyber operations and, to varying extents, conduct their own, virtually all face considerable hurdles when staffing and resourcing their cyber forces.[1] In many cases, the challenges are universal: disproportionate salaries and benefits between public organisations and private enterprise, or vast cultural differences between government and private employment that typically pushes freethinking and autonomous programmers toward the private sector. States are forced to cultivate offensive and defensive capabilities within the confines of budgets and personnel quotas amidst an ever-changing and largely unpredictable operational environment. While pooling resources among allies could improve their ability to better manage these developments, such opportunities are few as the sheer level of trust needed to share effective and unattributable malware or aspects of cyber security surrounding critical infrastructure drives partners to err on the side of classification. Some of the challenges in developing proprietary capabilities are distinct to certain governments with aspirations to compete in this space. For instance, countries peripheral to global technological innovation that nonetheless hope to protect national networks, if not exploit those of their adversaries, must consistently access technology and components developed beyond their borders. Cyber and traditional espionage provide at least an intermittent avenue to acquire an adversary's capabilities, though access can end abruptly and the discovery of these efforts may beget a response. Some countries including Russia and China must reconcile the operational boon provided by incorporating criminal elements into the state's agenda while ensuring these partnerships keep contracted, co-opted or coerced hackers from targeting the same networks the government seeks to defend, usually through tacit arrangements that promise incarceration for doing so while tolerating criminals' unsanctioned operations against external targets (Maurer, 2018; Marks, 2020).

Moscow has faced a plethora of challenges in building the kind of offensive and defensive cyber capability deemed necessary to thwart and reciprocate perceived activity from Russia's rivals, chiefly NATO member states. Some of these obstacles are among the seemingly universal ones mentioned earlier, while others are distinct. Probably foremost among them is the persistent

[1] For instance, the US military's Cyber Command (CYBERCOM) as of late 2018 faced recruiting challenges despite enhanced recruiting measures and a larger budget. A particular lack of 'coders' and 'developers' stunted the growth of CYBERCOM's Cyber Mission Force at the time, while a US defence department report found that existing specialists lacked the necessary experience to make a 'credible strategic cyber capability' (Pomerleau, 2018).

emigration of technological expertise from Russia, a trend that has existed in ebbs and flows since the collapse of the Soviet Union. Other factors exogenous to Russia's national security structure such as the state of Russia's economy and the ongoing global Covid-19 pandemic likely intermittently serve as a brake on developing the technology and personnel needed to compete with peers and adversaries in cyberspace, at least in absolute terms. The Russian government has addressed these challenges by creating a dedicated cyber force and using the support of a variety of non-governmental actors and agencies. The government has also established institutions and initiatives aimed to stimulate technological innovation. Despite its efforts, these limitations continue to shape how Moscow pursues the development of its cyber capabilities and the strategy guiding their use, suggesting that analysis of these trends, including state efforts to circumvent or alleviate them, would help to discern future Russian cyber operations, most importantly the campaigns targeting everything from Western elections to global critical infrastructure.

Research for this paper includes a mix of scholarly, journalistic and non-traditional sources that collectively offer valuable open source insights into Moscow's cyber limitations and how they might affect future activity. It concentrates on Russian state organisations, primarily the military and intelligence services and their connections to Russian academia, the IT industry, criminal hackers and other third parties. The opacity surrounding Russian and other states' cyber capabilities, however, affords the analysis and judgments in this paper a moderate level of confidence, as operational security prevents the fidelity needed to definitively assess the strengths and weaknesses facing relevant programmes.

2. Factors Limiting the Growth of Russia's Cyber Programmes

Russia can count on few if any allies in terms of cyber operations that have increasingly supported Russian foreign policy and military objectives that stretch from Syria to the US. The resources Moscow can allocate to cyber programmes are almost certainly eclipsed by those available to its principal rival in cyberspace, the NATO Alliance.[2] Despite ongoing debates about the actual size of Russia's defence budget, NATO military spending—even excluding the US—exceeds Russia's several times over (Wezeman, 2020), though unclassified budgetary comparisons fail to account for clandestine expenditures under which most states almost certainly place their offen-

[2] Although there are extremely few public cases of states cooperating in offensive cyber operations, at least some evidence suggests Russia's chief rivals have done so. The US, for example, allegedly collaborated with Israel in creating the Stuxnet virus that targeted Iran's nascent nuclear programme (Nakashima and Warrick, 2012). Additionally, NATO members in late 2017 agreed on a more aggressive approach to Russian cyber aggression that reportedly included offensive activity, according to a former NATO official, though the level to which offensive capabilities were actually shared or integrated into the Alliance structure remains unclear (Ali, 2017).

sive cyber efforts. In response to US plans in early 2015 to increase spending on cyber, including almost $17 billion partly dedicated to boosting US Cyber Command's capabilities,[3] Moscow reportedly mustered as much as $250 million, part of which was dedicated to offensive capabilities (Gerden, 2016). A 2017 assessment published by a Russian IT firm that ranked states' cyber capabilities, which included 'espionage, offensive cyber operations and information warfare' ranked Russia fifth in global 'cyber power', with roughly less than five per cent of the budget for cyber programmes as the US supposedly had and slightly over ten per cent of its reported manpower (Korotaev, 2017). Granted, the kind of cyber operations long conducted by Russian state actors, one of the cost-effective means of asymmetrically outflanking quantitatively superior adversaries prescribed by Putin in 2006,[4] almost certainly require a fraction of the spending on cyber made by Moscow's rivals, at least while at peace. Larger ambitions, however, such as establishing cyber capabilities and forces that move closer to parity with Russia's perceived adversaries, or initiatives to reduce software and hardware import dependencies on many of those same states, require a higher level of resourcing. Keeping pace with these rivals as emerging technologies such as quantum computing play a larger role in future cyber operations similarly necessitates increased funding and personnel.

A drought in state resources following the collapse of the Soviet Union all but crippled Moscow's nascent efforts to keep pace with observed Western developments in cyber capabilities. Sergey Aleksandrovich Modestov, a current vice-president of the Russian Academy of Military Science, claimed in 1997 that the 'widespread opinion' that Russia lagged the West in computing technology by as much as a decade necessitated a redoubling of Moscow's efforts to 'control and create a new class of weapons' (Modestov, 1997). Even as Russia underwent fiscal and economic stabilisation and as Russian society increasingly accessed the internet at exponential rates, Moscow struggled to connect advances in computer science and information technology to state goals surrounding national security, in part because of distinct cultural and bureaucratic impediments to government innovation. A 2005 RAND report found that a 'cult of secrecy' inhibited Moscow's efforts to integrate information technology into state functions including national security as state entities often used 'privileged information' to boost their interests at the

[3] According to official sources, the US intelligence community's Military Intelligence Programme (MIP) budget for fiscal year 2015 amounted to $16.6 billion (ODNI, 2020). The Deputy Director of the National Security Agency testified to the US House of Representatives Armed Services Subcommittee on Intelligence, Emerging Threats, and Capabilities and claimed that the MIP in 2015 would 'focus on the development of a strong cyber workforce and intelligence gathering in cyberspace' focused on US Cyber Command (US Government Publishing Office, 2014).

[4] Putin in 2006 in an address to Russia's federal assembly stated: "We must take into account the plans and directions of development of the armed forces in other countries; we must know about perspective developments. But do not chase quantitative indicators, do not 'burn' money in vain. Our answers must be founded on intellectual superiority. They will be asymmetric, less expensive." (Kremlin.ru, 2006).

expense of one another, a practice exacerbated by President Putin's placing intelligence officers in prominent positions (Peterson, 2005). While Moscow has since adopted measures to mitigate some of these problems, with mixed success, several shortcomings continue to hold back the state's effort to bolster its cyber capabilities.

The most significant impediment is likely the consistent 'brain drain', the emigration of IT and computer science specialists from Russia to other countries, especially the West. Nataliya Kasperskaya, chair of the board of the association 'Fatherland Soft' (*Otechestvenniy soft*) and ex-wife of renowned Russian cyber security mogul Eugene Kaspersky, recently submitted a letter to Prime Minister Mikhail Mishustin warning that Russia could lose between 10 to 15 thousand IT specialists in the next year (Skobolev, 2020). But dissatisfaction with salaries is longstanding; in 2017, a survey by Russoft found that Russian programmers were unhappy with their pay even as wages rebounded from their precipitous decline between 2014 and 2016 (Russoft, 2017a). According to a 2019 survey conducted by the Atlantic Council, IT specialists and software engineers comprised the third-most prominent category of Russian professionals choosing to live and work in other countries (Herbst and Erofeev, 2019). The effects on Russia's IT and computing industries by the coronavirus pandemic exaggerate an already dire trend for Moscow regarding the flight of technological specialists. Comparing May this year and the same period in 2019, Russian software developers' average revenue fell by almost half and ten per cent of firms claimed earnings declined by more than 90 per cent (Kozlov, 2020).

Prime Minister Dmitriy Medvedev in 2017 and Deputy Prime Minister Dmitriy Rogozin in 2018, described brain drain as a significant problem for Russia's development and future competitiveness (RBC.ru, 2017; 2018). The low salaries for specialists in Russia compared to those offered in the West, plus the internationally recognisable quality of Russia's leading scientific academic institutions, create an outward flow of specialists. In 2018, another survey revealed that as much as 65 per cent of Russian IT specialists planned to work abroad for higher salaries, though most surveyed stated they would eventually return to Russia after gaining 'international experience' (Romanova, 2018). As the military strove to build an 'information operations force' and as Rostec expended more funds on securing Russia's critical networks, the dearth of specialists became apparent as mounting evidence showed their preference to leave Russia for the West (Khodarenok and Zatari, 2017). Moreover, the interference of the state in private enterprise has contributed to the departure of specialists, including the IT sector. Pavel Durov, the founder of Russia's foremost social media platform 'VKontakte', left Russia in mid-2017 at least ostensibly because of demands from Russia's Federal Security Service (FSB) to provide information on his platform's users (Heller, 2018). The departures of key figures like Durov have a disproportionate impact on Russia's IT industry. As Russoft described in its 2019 survey of Russia's IT industry, 'even the loss of one key employee who is leaving the country is a problem for a specific company, particularly when this person is the most

competent developer who knows foreign languages' (Russoft, 2019: p. 144).

Whatever Moscow's personnel and resource limitations, Russia's hackers have given little sign that these shortcomings affect operations, at least during peacetime, which have ranged from attacking the 2018 Winter Olympic Games to probing electric grids in the US.[5] Nevertheless, in an unlikely scenario involving impending overt conflict between Russia and NATO, the limitations facing the former would probably affect its ability to conduct concurrent and sustained efforts against at least a quantitatively superior foe. When Russian state-sponsored actors launched waves of fairly simple yet massive distributed denial of service (DDoS) attacks against largely unprepared networks in Estonia in 2007 and Georgia in 2008, Western intelligence services and allies purportedly developed malware unparalleled in its sophistication and purpose: the Stuxnet malware used to temporarily disrupt Iran's nuclear programme required the work of multiple teams for development and extensive facilities for testing (Zetter, 2014). While DDoS served Moscow's purposes at the time and as it continues to occupy a prominent spot in state and non-state cyber arsenals, the examples of Stuxnet and the Estonia and Georgia cases to some extent highlight the probable gulf in capabilities between Russia and the West at the time.[6] Time also probably influenced these operations: while Stuxnet is described as being planned and developed years in advance of its use, Russian operators tasked with attacking Estonian and Georgian networks had far less lead time to prepare offensive cyber operations, given the comparative abruptness of the events that precipitated the 'bronze soldier' incident in Estonia and the war with Georgia a year later. The earliest available samples of the 'Regin' malware, considered by cyber security experts as the most advanced malware ever created and reportedly the work of the US's National Security Agency (NSA), date from 2011 (Cimpanu, 2019), a time when Russian military intelligence (GRU) officers resorted to spontaneously contacting cyber security researchers to hand over exploits (Satter and Bodner, 2018). Undoubtedly, Russian

[5] While much has been written about the blurring of peace and war from the Russian military perspective, several Russian military authors nonetheless distinguish between peace and theoretical wartime cyber operations. These authors typically distinguish between the types of operations that shape peacetime cyber, or 'information confrontation' efforts, like cyber efforts directed at strategic deterrence and wartime cyber operations, which generally aim to achieve information predominance over the enemy and aid kinetic military operations (Sayfetdinov, 2014; Lata, Annenkov and Moiseev, 2019; Dylevskiy, Komov and Petrunin, 2013).

[6] The gap in cyber espionage capabilities between Russia and its rivals at the time, however, was likely narrower than that separating offensive cyber operations. For instance, malware components that constituted what would eventually become APT28, attributed to Russia's GRU, date back to 2004 and continuously evolved alongside successful hacks against a wide array of targets (FireEye, 2014). Similarly, Turla, a threat group attributed to Russia's Federal Security Service (FSB), predates APT28 and has consistently impressed cyber security researchers through sophisticated breaches of targeted networks, including the 'agent.btz' exploitation of classified US military networks in 2008 (Council on Foreign Relations, 2020).

cyber capabilities drastically improved between then and the more notable and recent operations following Russia's annexation of Crimea in 2014. But some of these successes were predicated on malware likely developed by its rivals, such as the repurposing of alleged NSA intrusion sets for the 'BadRabbit' ransomware and 'NotPetya' wiperware attacks in 2017 (Stubbs, 2017), suggesting Russian malware development continued to lag behind that of its foremost adversaries. These capabilities are certainly enough to match Moscow's goals of engaging in information warfare along various fronts during uncertain peace and Russian actors have even recently demonstrated the ability to create original tools to advance these campaigns.[7] But to lead the international community in emerging technologies relevant to cyber capabilities, as prescribed by Putin in 2017, Russia needs more than current limitations allow.

Perhaps one of the most salient technological pursuits for offensive cyber operations is quantum computing, particularly its application to decrypting digital codes used by an adversary. As described by US Army Cyber Institute researchers in 2020, an adversary could use this technology to 'efficiently break the universally adopted public-key cryptographic schemes' in place today (Beshaj and Hall, 2020: p. 351). While Moscow hopes to develop unique capabilities in this field, including an ongoing effort by the Foundation for Advanced Research Projects (TASS, 2020), it continues to lag far behind leaders in the field, chiefly the intense competition internal to the US private sector. Additionally, artificial intelligence promises to advance both defensive and offensive capabilities, such as automatic defensive systems capable of formulating and deploying patches or social media automated phishing and reconnaissance on the offensive side of operations (Howells and Kalfoglou, 2020). Experts, however, describe Russia as a laggard in this field as Nikolai Markotkin of the Russian International Affairs Council and Elena Chenenko of Kommersant claimed in August 2020:

> Even if artificial intelligence (AI) development becomes Russia's highest priority, Moscow has no chance of catching up with Washington and Beijing in this field. Under favourable conditions, however, it is quite capable of becoming a serious player and even a local leader in certain areas (Markotkin and Chernenko, 2020).

These developments in Russia occur against a backdrop of serious deficiencies in national cyber security. While Moscow has demonstrated a clear and consistent interest in improving this, efforts to boost critical infrastructure cyber security are under-resourced and mired in stalled initiatives to reduce dependence on foreign software and hardware. The extensive use of pirated software to shore up cyber security and an ageing computing infrastructure

[7] For instance, the US National Security Agency and Federal Bureau of Investigation in August 2020 released a report detailing malware used by the GRU's 85th Main Special Service Center (GTsSS), the GRU's leading cyber espionage unit, called 'Drovorub' that deployed 'previously undisclosed' malware to target Linux systems (NSA/FBI, 2020).

also hinder the state's drive to improve these capabilities (Kottasova, 2017). The WannaCry ransomware attack in 2017 affected Russian networks more than those of any other state, extending even to its central bank (Reuters, 2017) as the attack offered a fleeting glimpse into a woefully unprepared cyber security sector.

3.RUSSIA'S INITIATIVES TO ADDRESS ITS CYBER LIMITATIONS

Emerging technologies relevant to cyber capabilities require intensive research and a given state's ability to harness various private and public entities to support these developments is perhaps not as far removed from arms-races of the previous century. That capacity hinges on the state's ability to marshal personnel and resources through collaboration, expropriation, coercion or otherwise to meet research goals. While Moscow has been able to seemingly keep its adversaries on the back foot in recent years through brazen offensive cyber operations and a distinct ability to merge hacks with digital psychological operations, its ability to remain competitive as communications and computing technologies become more sophisticated is less clear.

To manage or mitigate its shortage of talent, the Russian government has adopted various formal and informal methods. These include: 1) soliciting or coercing individuals and organisations to conduct operations on Moscow's behalf; 2) cultivating technical innovation relevant to state cyber capabilities; 3) expanding direct recruiting programmes; 4) bureaucratic deconfliction; 5) espionage targeting other states' cyber capabilities; and 6) concentrating on 'information-psychological' effects.

A. Soliciting/Coercing Civilian IT Experts and Organisations

The Russian services have a long history of co-opting a variety of cyber experts including criminals and IT specialists from the private sector or 'patriotic' hackers to collaborate with the government in various operations (Maurer and Hinck, 2018; Turovskiy, 2019). As early as the 1980s, Soviet intelligence services made use of an independent German hacker, Peter Karl, who offered to steal secret documents containing technology blueprints for the USSR that could enable the latter to 'overtake the West' (Turovskiy, 2019: p. 125). Today, the relationship with criminal hackers residing in the former Soviet states is based on the tacit agreement that they can conduct their activities unprosecuted by the state as long as they do not target any .ru websites and assist when called to engage in an operation 'for patriotic purposes' (Turovskiy, 2019: p. 148; Maurer and Hinck, 2018). In describing Moscow's control over non-state cyber groups, Russian expert Anton Nosik asserted: 'Each [Russian] hacker, who is not in prison, has a curator. Either in FSB or in Directorate 'K' of Russia's Ministry of Internal Affairs' (Lysenko and Brooks, 2018:p. 4). Such partnerships can help to fill any gaps by developing relation-

ships with independent hackers, some of whom eventually don a uniform.[8]

Even Russia's military, which probably represents the most rigidly hierarchical and subordinated offensive Russian cyber actor, at least occasionally elicits support from independent sources. Alexandra Elbakyan, a programmer from Kazakhstan who founded a website that has leaked thousands of proprietary academic publications, reportedly works occasionally on behalf of Russian military intelligence (Harris and Barrett, 2019).

Russia's intelligence and security services will almost certainly continue to pursue relationships with independent organisations and specialists to boost its cyber capabilities beyond those provided solely by uniformed and official staff. This tactic afforded Moscow a cyber capability even during its post-Soviet nadir in the 1990s when state-backed hackers successfully compromised several US government networks belonging to the military, National Air and Space Administration (NASA), Department of Energy and others (Greenberg, 2019). Incorporating independent sources into these operations received the highest possible endorsement in 2017 when Putin compared patriotic hackers to independent 'artists' acting in the state's interests, though supposedly without its direct backing (RFE/RL, 2017). Given the reliability of independent sources to supplement state-sanctioned cyber operations, the veneer of plausible deniability they afford Moscow and the international community's struggle to address it, their use could even expand in a future in which the gap in cyber capabilities between Russia's official actors and its adversaries widens. Nonetheless, the case of 'Vyarya', a pseudonymous programmer who left Russia after threats from probable security services after he refused to cooperate in offensive cyber research, illustrates that an even heavier hand in soliciting external support can potentially accelerate the flight of qualified specialists (Kramer, 2016). Developing the technologies likely to drive future cyber operations, however, falls outside the purview of independent hackers. Adapting to this future necessitates robust links to an IT sector capable of intensive research and optimising work with state-funding that is a fraction of the resources put forth by Russia's perceived adversaries.

B. Efforts to Cultivate Technical Innovation

Moscow needs a vibrant IT sector to compete with its adversaries and rivals if it hopes to remain at the cutting edge of offensive and defensive cyber capabilities, especially in the unlikely—yet conceivable—scenario in which Russia needs sustained operations against a sophisticated opponent. Russia

[8] The case of Dmitriy Dokuchaev, a renowned Russian hacker gradually integrated into one of the FSB's offensive cyber departments, exemplifies the path from independent hacking to direct state subordination and employment. (Kramer 2017; Turovskiy 2019: p. 139) Dokuchaev, an independent hacker in the mid-2000s, was coopted into working for the FSB's Center for Information Security and eventually became a major in that unit. Similarly, Maksim Yakubets, the leader of a prominent criminal hacking group, in 2017 began working closely for the FSB and – as of early 2018 – awaited a license to work with classified information from the former, though whether Yakubets received a rank and official position within the FSB remains unclear (US Department of the Treasury, 2019).

lacks an equivalent to the Silicon or Shenzhen Valleys and state-directed efforts to cultivate an analogue in Russia have met with, at best, mixed results. Medvedev in 2010 inaugurated an effort to build 'Skolkovo Valley', which he described as 'something along the lines of Silicon Valley' and which by 2020 would host as many as 50,000 specialists (Appell, 2015). The initiative rapidly fell victim to rampant corruption and eventually led Russian officials to re-evaluate its potential. For instance, Viktor Vekselberg, the chairman of the Skolkovo Board of Directors, claimed in June this year that 'Skolkovo is not a counterpart of the Silicon Valley' and comparing them was 'inappropriate and even absurd' (TASS, 2020).

Skolkovo's fate demonstrates that trends in emigration and limited resources are worsened by prevailing corruption, which almost certainly limits Moscow's ability to optimise research and development for projects relevant to cyber capabilities. For example, a military officer who headed a department in the 18th Central Scientific Research Institute (TsNII), which, according to the Russian press, develops 'special radio-electronic technology' on behalf of the GRU, was stripped of his rank and sentenced to six years in prison in 2017 for stealing equipment worth 40 million roubles (Lenta.ru, 2017).[9] That same year, the head of the FSB's Information Security Centre resigned as FSB sources claimed his dismissal due to corruption charges was imminent (Kolomychenko, 2017), though his ouster could have at least partly been political.

Russia's military and security services use the Russian Foundation for Advanced Research (Fond Perspektivykh Issledovaniy, FPI), known as Russia's equivalent to the US Defence Advanced Research Projects Agency (DARPA), to stimulate innovative research and projects that can enhance Russia's cyber capabilities. FPI conducts regular nationwide competitions for innovative technological solutions to national security problems (Moscow Times, 2015) and cyber warfare which as of 2018 constituted one of the three main foci of FPI's research (Uppal, 2019). The winning projects may receive funding to build a prototype of their research and their solutions can then be implemented in the respective agencies of the Defence Ministry (International Military-Technical Forum 'Army-2018', 2018). In 2019, FPI together with Skolkovo Security Challenge launched a competition for the best solution for the 'preventive detection of network attacks.' The participants who won the contest applied machine learning methods to effectively identify 'complex patterns and network anomalies' (FPI, 2019a). The interest of the security services in the ideas developed in these competitions is suggested by the fact that one of the judges of the competition was A. V. Korolkov, chairman of

[9] The 18th Central Scientific Research Institute, or Unit 11135, to some extent likely conducts cyber research. For instance, the unit hosted an unspecified scientific conference in 1995 that helped research related to 'raising the effectiveness of automated operational control systems from the impact of malicious software' (Vyalykh, 1999). The 18th also benefitted from research in 2004 for a contract related to 'Research and development of mathematical and software tools for effective parallelisation of applied problems on high-performance computing systems' (Levin, 2004).

Unit 43753 (FPI, 2019b), the FSB's Communications Security Centre, part of the Eighth Service Directorate (Villalon, 2016).

Nonetheless, the flight of specialists from Russia continues to threaten the overall health of Russia's IT sector and ultimately state actors' ability to tap into it to further their goals related to developing offensive and defensive cyber capabilities. The continued effect of the coronavirus pandemic on Russia's economy has exacerbated the issues driving emigration, suggesting a prolonged effect on the IT sector. Other issues, such as Russia's impending adoption of a law that requires digital assets be purchased in Russia and declared by whoever buys them are likely to spur more emigration. As the head of Russia's cryptocurrency and blockchain associated stated, 'The adoption of the digital financial asset law in its current state is likely to speed up an exodus of IT professionals' (Kozlov, 2020).

C. Expanding Direct Recruiting Programmes

While the Soviet military and intelligence services enjoyed a direct pipeline to highly qualified graduates of technical institutions, these services' post-Soviet descendants must compete with the allure of the private sector when recruiting computer science and IT specialists in modern Russia. Despite the shock of the Soviet collapse, many of the institutions used to train intelligence and military specialists in cyber operations survived into the 21st century, though many initiatives are new. Russia's military, for example, has launched several such efforts since 2013 ranging from 'military science units' to cyber security education programmes at specific universities and schools; for example, the St. Petersburg-based Military Academy of Communications in 2015 launched a cyber security training programme that offered classes on network technology, multimedia hardware, software and robotics (Bodner, 2015). At least some of these programmes seek to inculcate a culture of patriotism among prospective recruits, galvanising them against supposed information and cyber threats emanating from states hostile to Russia. The GRU, for instance, has sponsored 'cadet classes' that provided extra computer lessons alongside patriotic education (Troianovsky and Nakashima, 2018). Another tactic involves direct partnerships with academic institutions or training programmes, sometimes by placing officials connected to Russia's military or intelligence services into positions of leadership. For instance, the former chief of the Federal Agency of Government Communications and Information (FAPSI) and current Director of the National Association for International Information Security, Vladislav Sherstyuk, also serves as the Director of the Institute for Information Security at Moscow State University (NAIIS, 2020).

Since the creation of the military science units, the military has been soliciting applications for mathematicians, cryptographers, engineers and programmers among technical universities (Turovskiy, 2019). President Putin's 2018 visit to the 'ERA' (Elite of the Russian Army) Technopolis, which is partly based on that recruiting initiative, exemplified the importance of harnessing Russia's technical talent for defence research (Shurygin, 2018) and

he also inspected the ERA's work at the 'Army 2019' exposition near Moscow that year (Vesti, 2019). Although those entering the science companies are only obligated to serve a year of military service, the standard conscription term for Russia's military, they are encouraged to become officers after their mandatory service (Lysenko and Brooks, 2018).

According to Turovskiy (2019), since 1991 the FSB has been conducting Olympiads on cryptography in Russian schools. The services have continued to use various practices to seek young hackers. In 2015, a course titled 'Young programmers of Russia's FSB' appeared in a Moscow-based academy for children in secondary education, which prepared students to become IT experts and taught them how to launch DDoS attacks and exploit wireless networks, all while attending meetings with FSB officers. He reports that the curriculum included political lectures with a heavy anti-Western bias, which led one of the students to suggest to his classmates that they 'unite and attack America' (Turovskiy, 2019: p. 184) and in 2017, the course organisers officially signed a contract for collaboration with the FSB Academy and the FSB administration in Moscow.

Various government agencies may also be using events such as online hackathons and large-scale conferences to identify cyber talent. An online contest called 'Digital Breakthrough', a product of Russia's 'Education' and 'Land of Opportunities' national initiatives, began in 2019 and included 40 regions and 66,000 participants (Zakharov, 2020). Both the FSB and GRU probably recruit from 'Positive Hack Days', which in 2014 hosted round-table discussions attended by FSB representatives on information security, the possibilities of network espionage and different countries' approaches to information security (Positive Hack Days, 2014). Dmitriy Badin, a GRU officer identified by the US and Germany for election-related hacking, very likely attended this event, probably at least in part to spot and recruit talent (RFE/RL, 2018).

Efforts to recruit capable computer science and IT specialists into Russia's military and security services probably offered lukewarm results and some evidence suggests direct outreach fails in certain cases. For example, insider accounts of the 'military science units' describe a lacklustre attempt at integrating technical talent into the ranks of Russia's military and accounts from 2015 from two science units describe inept leadership, ineffectual scientific work and frequent distractions that ranged from moving furniture to attending lectures on Stalin, which led some to conclude that the science units were largely a propaganda effort (Topwar.ru, 2015; Dobrynin, 2017). A separate account from 2017 claimed that most of the work performed by the Ministry of Emergency Services' science company was useless and its recruits even faced occasional physical hazing during their initial processing (Krasnaya Vesna, 2018). Additionally, the patriotic education that seemingly accompanies many efforts to directly recruit students into the military and security services probably dissuades a significant portion of potential recruits from joining. For example, a military veteran and former instructor for the KGB

in 2019 taught courses on 'psychotronic warfare' at one of Russia's largest technological universities that claimed social media 'was a weapon designed to destroy Russia' and the US High-Frequency Active Auroral Research Programme based in Alaska was a 'secret US mind-control project' (Yapporova, 2019). While the university's engineering and programming students largely bemoaned the mandatory courses, information security students praised their university's growing ties to the FSB and Federal Technical and Export Control Service, which offered internships and employment opportunities. Even beyond the propagandistic curricula, only 15 per cent of the 25,000 graduates of IT programmes in Russia are ready for immediate work, largely due to a shortage of professors with relevant skills, suggesting recruits to the military and security services probably require extensive training before they can contribute to operations or research (Izvestiya, 2019).

D. Bureaucratic Deconfliction

Inarguably, Moscow is incapable of controlling the wide range of exogenous factors that affect the health of its computing and IT industries, such as unanticipated phenomena like the coronavirus pandemic and fluctuations in oil prices, or the competitiveness of other states' hardware and software exports. The Russian government could, however, improve on many of the internal problems that affect the state's ability to optimise the resources and personnel at its disposal. Deconflicting missions between highly competitive Russian actors tasked with defending the country's networks and breaking into those of other states is an internal impediment to cyber operations that partly lies within Moscow's control. According to Kimberly Zenz, the Head of Threat Intelligence of the German Cyber Security Organisation (*Deutsche Cyber-Sicherheitsorganisation*), infighting among Russia's cyber actors has increased since 2014, resulting from factors that include geopolitical pressures, economic uncertainty, elite conflicts and shifting power from formal institutions (Zenz, 2019). In its most benign form, infighting results in duplicative and redundant efforts between actors and expending resources Moscow can ill-afford to waste. More significantly, infighting leads actors to leak information to undermine rival organisations, resulting in attribution or arrests. A leading theory behind the arrest by Russian authorities of the FSB's Centre for Information Security officers in late 2016 involves a plot by the centre's officers to undermine the GRU by leaking information about their 2016 operations to interfere in the US presidential election (Eckel, 2019).

Bureaucratic competition has long stifled Moscow's efforts to develop cyber capabilities. Even during the Soviet period, a zero-sum approach by state actors to fiscal and personnel resources ensured insurmountable bureaucratic hurdles for initiatives to enhance the nascent field of 'cybernetics' to further Moscow's goals related to defence and economic management (Peters, 2017). Within the modern FSB, at least occasional conflicts between the Centre for Information Security, a unit that conducts offensive operations, and the Communications Security Centre, largely responsible for ensuring cyber security, demonstrate the almost inevitable nature of bureaucratic friction even when official mandates and responsibilities avoid direct overlap (Rozh-

destvenskiy and Alekhina, 2017). The consistently independent operations by malware associated with Russia's military and intelligence services evidences a probable lack of collaboration. According to Check Point Research, a cyber security firm that investigated Russian state-sponsored malware in 2019, Russian state actors refrain from sharing their code with other actors and each maintained a team of malware developers working for years on 'parallel or similar' toolkits, that allowed researchers to 'spot redundancy in this parallel activity' (Cohen and Bassat, 2019). While compartmentalising these efforts may boost operational security, redundancy is something Moscow can ill afford considering how quantitatively outmatched Russian actors are by their rivals. By pooling resources between actors, or at least establishing rough divisions of labour, Moscow could improve offensive and defensive cyber operations.

To some extent, Russian officials have enacted means of reducing bureaucratic strife related to cyber capabilities. At a time when Moscow sought to rapidly build its cyber-capable cadres, the FSB and GRU overcame their deep-seated rivalry to secure an agreement in 2017 between the GRU's foremost cyber espionage unit, the 85th Main Special Service Centre (Unit 26165) and the FSB's prestigious cryptography academy, in which the latter would help train specialists for the former (RFE/RL, 2018). Often, firms contracted by state actors act as connective agents between various ministries and organisations, providing an at least unofficial and indirect path to cooperation between Russian actors.[10] Nevertheless, historical rivalries between the actors responsible for conducting cyber operations probably necessitate presidential mediation if Moscow hopes to foster lasting, collaborative relationships between them. Informal summits like the 2018 Siberian outing attended by FSB head Aleksandr Bortnikov, Minister of Defence Sergey Shoygu and President Putin offer a secure setting for such an inter-organisational parlay.

E. Espionage Targeting Other States' Cyber Capabilities

Of course, digital or traditional espionage offers a means of circumventing Russia's problems in developing its own capabilities by stealing the technology of other, more advanced states. Soviet intelligence has dedicated significant resources to science and technology espionage, such as the 'ente-erovtsy' (the phonetic pronunciation of the Russian acronym for science and technology intelligence, NTR) of the interwar period (Haslam, 2015). Probably no case serves as a better example of using espionage to gain offensive cyber capabilities than that of the Shadow Brokers, which reportedly involved probable Russian actors leveraging access to Kaspersky antivirus software and an NSA contractor's negligence to acquire malware that would eventually feed Russian and other state-backed offensive cyber operations (Harris, Lubold and Sonne, 2018). Although disconnected from state-sponsorship, the recent US Department of Justice (DOJ) indictment of a Russian

[10] Bloomberg's 2015 investigation into Kaspersky Labs provides a succinct, yet thorough snapshot of the interconnectedness of Russian state-backed cyber actors and the firms that support them (Matlack, Riley and Robertsom, 2015).

national who sought to extract sensitive information from a US company by using an inside agent to introduce malware into the company's network shows the continued vulnerability to espionage of the private sector which the West relies on to develop cyber capabilities (DOJ, 2020). Human-enabled cyber operations also lower the kind of offensive capabilities required to penetrate and exploit adversarial networks, either by providing sensitive details on cyber security infrastructure or by directly implanting malware into a targeted network. Herman Simm, a former Estonian intelligence officer who worked for Russia's Foreign Intelligence Service (SVR) until his arrest in 2008, provided Moscow with intimate details on NATO cyber security, leading the Alliance to conclude that Simm's leaks made NATO partners 'more vulnerable to cyber threats and attacks' (Schmid and Ulrich, 2010).

Nevertheless, there are obvious drawbacks in leaning too heavily on espionage to bolster Russia's lacklustre technological development. Even the best intelligence operations come to a usually abrupt end for various reasons, like an agent's reassignment, discovery by authorities or cessation in supporting their handlers, which limits intelligence services' insight into a particular field. The discovery of an agent network in a targeted country leads to diplomatic fallout, national embarrassment and typically strengthens counter-intelligence efforts among affected states and their allies. But the West has continuously shown its vulnerability to furtive computer espionage conducted remotely by China and Russia, a veritable backdoor into classified projects related to national security. The resemblance of Chinese fighter aircraft to US ones, for example, shows what prolonged access to these networks can yield for states engaging in cyber espionage (Daniels, 2017). Advanced Persistent Threats attributed by the cyber security community to Russian state actors have similarly gained access to sensitive information resting on NATO networks, such as APT28's longstanding targeting of US defence contractors (CISOMAG, 2020). The current environment in which Russian operators attempt to breach these networks, however, is somewhat different to many of these actors' past and largely undetected intrusions; an unprecedented level of international attention is now focused on malware attributed to Russia's military and intelligence services, which likely inhibits at least to some extent their ability to conduct cyber espionage. Underground or criminal malware, nonetheless, can provide original exploits disassociated with state-backed threat groups and intrusion sets. For example, malware widely attributed to a criminal group was possibly used in a campaign to illicitly acquire sensitive information on Ukrainian diplomacy and naval affairs shortly before the Kerch Strait incident in 2018, when Russian naval vessels apprehended and imprisoned Ukrainian mariners on the Black Sea (Tucker, 2018).

F. Concentrating on 'Information-Psychological' Effects

Russia is perhaps unique among contemporary cyber powers in its conceptualisation of the indivisibility of technical and psychological computer network operations, which range from offensive cyber operations on critical infrastructure to using false social media personas to disseminate messaging that supports Russian foreign policy or military objectives. As seamless as

this integration is among Russian security officials, operations like the use of Triton malware to shut down a Saudi energy facility in 2018 require far more technical development than the kind of digital psychological operations represented by, for instance, the GRU's limited use of Facebook in 2014 to sow social and political discontent in post-Maidan Ukraine. By concentrating on the latter, Russia's intelligence services and its military could employ more officers with less technical capabilities to conduct more less-technically intensive influence operations. One of Russia's longest-running influence campaigns on social media, dubbed by cyber security researchers 'Secondary Infektion', involves little more than registering single-use accounts on social media to amplify narratives published on alternative news websites and forums and posting simple forgeries of documents ostensibly written by Western or Ukrainian officials (Nimmo et al., 2020a). While concentrating on digital influence might come at the expense of developing emerging technologies needed for sophisticated offensive cyber operations, like those possibly needed in an unlikely wartime contingency with a conventional foe, Russian officials might be satisfied with an 'information-psychological' focus during a continued uneasy peace between Russia and the West. The riots in Novi Sanzhary, Ukraine, in early 2020 served as a stark example of the potential for Russian influence operations to inspire physical effects, however, few and circumstantially specific these cases may prove. The increasing social and political polarisation among states that Russian commonly targets with digital influence efforts might also reduce the need to illicitly procure sensitive documents, like those used by Russian actors to influence Western elections, as target audiences readily accept less credible forgeries that are easier to fabricate than obtaining actual sensational materials through cyber espionage.[11]

But evidence suggests that emerging technologies will affect digital influence operations as well, possibly blocking Russian techniques and capabilities that supported previous efforts. Despite, for example, the GRU's probable emphasis on using machine-translations to support digital psychological operations, the fact that linguistic mistakes have been frequently used to detect and identify their operations indicates technology has fallen short

[11] For instance, an early 2019 poll conducted by Gallup revealed that US President Donald Trump's job approval rating that year marked the most entrenched political polarisation within the US than previously recorded (Jones, 2019). At the same time, academic research has demonstrated a positive correlation between polarisation and receptivity to 'fake news', such as individuals' propensity to overrate the accuracy of news consistent with their political views (Sindermann, Cooper and Montag, 2020).

of ambition.[12] While Russian influence actors have recently demonstrated the ability to use 'deep fake' technology to create false social media profiles, such as the Internet Research Agency's (IRA) effort to support a covert website through a handful of inauthentic profiles (Macaulay, 2020), cyber security firms were able to quickly identify them. Indeed, emerging technologies thus far have probably benefitted NATO efforts to counter Russian digital influence operations than these technologies have forwarded Russian actors' ability to covertly conduct them. The Lithuanian website 'Demaskuok' (debunk), for instance, cooperated with Google in developing artificial intelligence capabilities to identify disinformation (President of the Republic of Lithuania, 2019). Given that both sides' implementation of emerging technologies to conduct and defend against digital influence campaigns is nascent, assessments about Russian capabilities allow for little more than low confidence estimations of their successful use. Nonetheless, Russia's fixation on conducting online influence operations, the proliferation of new and relevant technology, plus the apparent ability of other actors – particularly non-state ones – to use emerging technologies to influence audiences over the internet suggests Moscow is possibly better positioned to take advantage of these developments than those defending against its digital malign influence. As experts from the U.K.'s Conflict Studies Research Centre asserted:

> The introduction of machine learning and potentially artificial intelligence (AI), will vastly enhance capabilities for automating the reaching of mass audiences with tailored and plausible content. Consequently, they will render malicious actors even more powerful (Hartmann and Giles, 2020).

Just as human agents can advance cyber espionage and offensive cyber operations, they can help to overcome hurdles facing Russian digital influence campaigns such as a lack of cultural or linguistic expertise and the increasing ability of social media platforms to identify coordinated inauthentic behaviour. Both the GRU and SVR, for example, continue to solicit native authors to generate content on covertly run websites that aim to influence US audiences, including messaging about the upcoming presidential election, disinformation surrounding the coronavirus pandemic and exacerbating societal unrest (Barnes and Sanger, 2020). Similarly, Evgenniy Prigozhin's IRA as of September 2020 sought genuine American authors with partisan political viewpoints to write content for a website the IRA furtively managed,

[12] An official assigned to the GRU's main psychological warfare training programme at the Ministry of Defence's Military University (VUMO) sometime after the Georgian war claimed that his curriculum recently added classwork on 'machine-translations of literary texts into foreign languages' that would allow operators to quickly create 'high quality' translations of materials into foreign languages (Cheshuin, 2009). For examples of how linguistic mistakes have undermined GRU online influence operations, see the Atlantic Council's Digital Forensic Research Lab's report on 2016 operations, titled '#TrollTracker: Russia's Other Troll Team,' or Graphika's 2018 report on GRU use of blogs, including the 'non-native English' found in posts supporting the GRU's 'Inside Syria Media Centre' (Nimmo and Yap, 2018; Nimmo, Francois, Eib and Tamora, 2020b).

'peacedata.net'. The use of false social media accounts alerted Facebook and Twitter to the operation and eventually leading the social media platforms to disable the accounts and pages (BBC, 2020).

4. RECOMMENDATIONS AND CONCLUSION

The limitations affecting Moscow's drive to build a peer-worthy cyber force among its military and security services are unlikely to prevent them from continuing the cyber espionage, digital influence campaigns or even infrequent yet brazen attacks against critical infrastructure that have constituted their repertoire for at least the past two decades, though escalated amidst rising international tensions surrounding Russia's annexation of Crimea in 2014. Russian state actors behind these efforts will almost certainly find enough graduates of computer science and IT programmes to maintain current staffing and state actors will still be able to rely on support from independent IT and cyber security firms even as these sectors face growing challenges resulting from economic and demographic factors. In the highly unlikely event that Moscow faced imminent and overt conflict with NATO, these limitations would become more pronounced, as Russian services probably would be unable to match their adversary in terms of sustained and simultaneous offensive cyber operations, all while attempting to protect their own networks. Perhaps more importantly, Russia's cyber limitations will likely affect its ambitions to harness emerging technologies relevant to offensive and defensive capabilities.

In the meantime, Moscow will continue its cyber efforts in the face of quantitatively predominant adversaries, as one military author asserted, following renowned Russian military strategist Aleksandr Suvorov's axiom, 'not by number, but by skill' (Nesmeyanov, 2017). The countries targeted by Russian cyber operations at the same time can adopt measures to possibly exacerbate Russia's cyber limitations, such as depriving Russian actors of the skill prescribed by Suvorov. Most of Russia's young programmers, computer scientists and IT specialists hope to work abroad at least temporarily, primarily in the West. A 2018 poll by Gallup found that, among a record level of Russians hoping to emigrate, respondents named Germany and the US as their most-desired destinations (Moscow Times, 2019).[13] Indictments issued by the West against Russian state-backed hackers may do little to curb ongoing activity, but they probably dissuade at least some would-be military or intelligence officers from joining an agency that could permanently prevent their ability to travel to desirable countries. US Cyber Command's furtive messaging effort against Russian actors involved in digital influence operations, which revealed Cyber Command's awareness of Russian actors' personal information, presents a low-risk effort to exacerbate this issue. As much as Russian officials rely on the skill of their programmers, engineers

[13] A separate poll that year found that half of Russia's IT specialists wanted to emigrate, while Germany, the US and the U.K. were top choices for relocation (Strack et al., 2018).

and IT specialists to boost cyber capabilities,[14] they likely worry about their susceptibility to this kind of messaging. A long-serving Russian psychological operations officer warned as much in 2013, claiming that 'information-psychological' attacks on cyber operators constituted one of the three main types of cyber operations (Popov, 2013).

Sanctions offer an approach to limit Russian actors' ability to procure software and hardware, probably hindering state-backed efforts to conduct research related to emerging technologies, though possibly unnecessarily damaging private enterprise in Russia, including firms that are mostly unassociated with state programmes. Despite Moscow's intent to shift toward domestic software production, fuelled by sanctions levelled against Russia following its annexation of Crimea and by officials' fears that foreign software could benefit hostile cyber warfare aims, initiatives to spur domestic production quickly stalled, leading presidential spokesman Dmitriy Peskov to declare in 2016 that an effort to replace state agencies' use of Microsoft products was 'impossible for the time being, especially because local companies haven't yet developed worthy alternatives' (Popa, 2016). Around half of Russia's IT companies in 2017 felt that sanctions harmed their industry (Russoft, 2017b). While little evidence suggests that sanctions have an immediate effect on Russian state-sponsored cyber operations, with some experts claiming they actually spur more operations,[15] sanctions could provide a means of affecting Russian actors' long-term ability to adapt to an increasingly sophisticated operational environment. US sanctions, for instance, catalysed the downfall of a Russian tech company in 2018 that developed microprocessors as part of a state effort to reduce dependence on Western technology (Kolomychenko, 2018). Nevertheless, some experts state that sanctions imposed on Russia have benefitted its economy (Twigg, 2019), indicating that lasting sanctions could eventually spur enough domestic production to possibly support Moscow's cyber agenda. Moreover, the prolonged inability by Moscow to access needed foreign software and hardware could force Russian officials to overcome their entrenched suspicions of cooperating with Beijing on technological development, eventually forging a relationship that surpasses the existing programmes and bilateral initiatives. China and Russia this year took steps to reinforce their joint research on emerging technologies, such as a new research lab focused on artificial intelligence at the Moscow Institute of Physics and Technology sponsored by Huawei and mutual concerns—like antipathy toward the US—and benefits are likely to deepen technological ties between them (Bendett and Kania, 2020).

---

[14] As Dmitriy Mikhailov, the head of the Centre for Cybersecurity at the Russian National Research Nuclear University, explained in 2016, 'Russia has experienced some IT security problems, however our hackers are among the best in the world. In the case of cyber attacks, the most important thing is not related to material assets, but the skilful use [of] mathematical algorithms' (Gerden, 2016).

[15] According to Dmitri Alperovitch, the Chairman of the Silverado Policy Accelerator and former Chief Technology Officer of Crowdstrike, Russian state cyber actors as of 2015 used more brazen and frequent cyber espionage operations to compensate for Western sanctions levelled against Russia (Bennett, 2015).

Considering Russian actors' demonstrated ability to repurpose an adversary's malware to use in their own offensive operations, Western militaries and intelligence services should weigh the risks in using sophisticated malware in offensive operations. While Russian actors probably lack the personnel and resources needed to craft as many zero-day exploits as their rivals, they have consistently made use of malware purportedly developed by the US to conduct many of their operations, including the GRU's use of EternalBlue, attributed to the NSA, to carry out the NotPetya wiperware attack in 2017 (Hay Newman, 2018). Although US Cyber Command, for example, has shown a willingness to execute offensive operations as part of a new strategy to deter Russian offensive cyber operations, it could conceivably benefit Moscow by defending too far forward in cyberspace through the use of original malware that Russian actors can quickly reverse engineer and reuse. Similarly, Western militaries and intelligence services can help guard against Russia's ability to acquire proprietary exploits by enhancing operational security and access to relevant programmes, given Russian actors' consistent ability to take advantage of leaked or poorly secured offensive tools and malware developed by its rivals.

With the production of sophisticated tools available to NATO nations, member states need to ensure they incentivise reporting of vulnerabilities through, for example, bug bounty programmes across their industries. Such programmes, if properly compensated, could provide an alternative to selling such information underground. This can have a long-term crippling effect on illicit markets for vulnerabilities and restrict the ability of Russia state-supported cyber threats to access and exploit them (Supreme Headquarters Allied Power Europe (SHAPE) representative 2018, pers. comm., 12 August).

There is little reason to doubt Russian actors' capability to continue offensive cyber operations, digital influence operations and cyber espionage operations in the near-term future. There is sufficient evidence, however, to doubt Moscow's ability to adapt to emerging technologies that require intensive research and investment that exceed the state's capacity. Although Moscow could overcome some of the challenges affecting cyber development such as bureaucratic competition, reducing corruption or alleviating the culture shock that programmers and IT specialists face when entering the military or security services, Russian officials can do little to influence the exogenous factors likely to affect the health of Russia's IT and computing industries on which the state relies to advance its capabilities. These limitations provide only narrow openings for countries affected by Russian cyber activity to affect Russia's future capabilities, like dissuading potential recruits from joining Russia's military or security services by barring them from the countries in which many Russian IT and computer science specialists hope to work or travel. Efforts such as this will almost certainly fail to prevent the next NotPetya attack, a type of behaviour that can only be resolved through deterrence, diplomacy or a drastic change in tensions between the West and Mos-

cow. But indictments and sanctions could to some degree inhibit Moscow's ability to use emerging technologies like quantum computing and artificial intelligence for future offensive operations. At the same time, Western cyber planners should pay more attention to economic and demographic factors, such as the outflow of technological talent from Russia, which will shape how Moscow approaches cyber competition with its perceived adversaries throughout the next decade.

5. REFERENCES

Ali, R. (2017) NATOs Little Noticed but Important New Aggressive Stance on Cyber Weapons. *Foreign Policy*. 7 December. Available from: https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/ [Accessed 21st October 2020].

Appell, J. (2015) The Short Life and Speedy Death of Russia's Silicon Valley. *Foreign Policy*. 6 May. Available from: https://foreignpolicy.com/2015/05/06/the-short-life-and-speedy-death-of-russias-silicon-valley-medvedev-go-russia-skolkovo/ [Accessed 21st October 2020].

Barnes, J. E. & Sanger, D. E. (2020) Russian Intelligence Agencies Push Disinformation on Pandemic. *The New York Times*. 28 July. Available from: https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html [Accessed 21st October 2020].

BBC News. (2020) Facebook and Twitter 'dismantle Russian network'. 2 September. Available from: https://www.bbc.com/news/world-us-canada-53980979 [Accessed 21st October 2020].

Bennett, C. (2015) Russia's cyberattacks grow more brazen. *The Hill*. 12 April. Available from: https://thehill.com/policy/cybersecurity/238518-russias-cyberattacks-grow-more-brazen [Accessed 21st October 2020].

Bendett, S. & Kania, E. (2020) The Resilience of Sino-Russian High-Tech Cooperation. *War on the Rocks*. 12 August. Available from: https://warontherocks.com/2020/08/the-resilience-of-sino-russian-high-tech-cooperation/ [Accessed 21st October 2020].

Beshaj, L & Hall, A.O. (2020), Recent developments in cryptography. In Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky, G. (eds.), *12th International conference on cyber conflict, 20/20 vision: The next decade*. NATO CCDCOE Publications, Tallinn, pp. 351-368.

Bodner, M. (2015) Russian Military Launches Cybertraining Programme for Youth. *The Moscow Times*. 1 September. Available from: https://www.themoscowtimes.com/2015/09/01/russian-military-launches-cybertraining-program-for-youth-a49276 [Accessed 21st October 2020].

Cheshuin, S. A. (2009) *Osobennosti sovremennovo informatsionnovo protivoborstva i ikh uchod pri podgotovke spetsialistov zarubezhnoy voennoy informatsii v voennom universitete* [The Features of Modern Information Confrontation During the Training of Specialists of foreign Military Information at the Military University]. Available from: http://www.milpol.ru/sgs/sgs.html [Accessed 21st October 2020].

Cimpanu, C. (2019) The world's most famous and dangerous APT (state-developed) malware. *ZDNet*, 8 July. Available from: https://www.zdnet.com/pictures/the-worlds-most-famous-and-dangerous-apt-state-developed-malware/ [Accessed 21st October 2020].

CISOMAG. (2020) Russian Hackers Attempting Cyber Espionage Against Middle East Defence Firms. 24 March. Available from: https://cisomag.eccouncil.org/russian-hackers-attempting-cyber-espionage-against-middle-east-defense-firms/ [Accessed 21st October 2020].

Cohen, I. & Bassat, O. B. (2019) Mapping the connections inside Russia's APT Ecosystem. *Check Point Research*. 24 September. Available from: https://research.checkpoint.com/2019/russianaptecosystem/ [Accessed 21st October 2020].

Council on Foreign Relations. Turla. Available from: https://www.cfr.org/cyber-operations/turla [Accessed 21st October 2020].

Daniels, J. (2017) Chinese theft of sensitive US military technology is still a huge problem, says defence analyst. *CNBC*. 8 November. Available from: https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html [Accessed 21st October 2020].

Dobrynin, S. (2017) Rosgiki dlya Rosgvardiya [Rosgiki for the Russian National Guard]. *Radio Svoboda/Radio Liberty*, 27 July 27. Available from: https://www.svoboda.org/a/28643436.html [Accessed 21st October 2020].

Dylevskiy, I. N., Komov, S. A., & Petrunin, A.N. (2013) Ob Informatsionnykh Aspektakh Mezhdunarodno-Pravovo Ponyatiya Agressiya [On the Informational Aspect of the International-Legal Understanding of Aggression]. *Voennaya Mysl*. 10, 3-12.

Eckel, M. (2019) In Moscow Treason Trial, A Major Scandal for Russian Security Agency. *RFE/RL*. 27 February. Available from: https://www.rferl.org/a/russia-hacker-mikhailov-stoyanov-fsb-scandal-for-russian-security-agency/29794092.html [Accessed 21st October 2020].

FireEye, Inc. (2014) APT28: A Window into Russia's Cyber Espionage Operations? Available from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf [Accessed 21st October 2020].

Fond Perspektivykh Issledovaniy. (2019a) *Konkursy [Contests]*. Available from: https://fpi.gov.ru/tenders/184/ [Accessed 21st October 2020].

Fond Perspektivykh Issledovaniy. (2019b) *Protokol No. 2 zasedaniya konkursnoy komissii [Protocol No. 2 of the Contest Commission Session]*. 31 May. Available from: https://fpi.gov.ru/upload/iblock/de3/de33a1a0b32c2b2abbe2c9013eb853a3.pdf [Accessed 21st October 2020].

Gerden, E. (2016) Russia to spend $250m strengthening cyber-offensive capabilities. *SC Media*. February 4. Available from: https://www.scmagazineuk.com/russia-spend-250m-strengthening-cyber-offensive-capabilities/article/1477698 [Accessed 21st October 2020].

Greenberg A. (2019) *Sandworm*. New York: Doubleday.

Hay Newman, L. (2018) The Leaked NSA Spy Tool That Hacked the World. *WIRED*. 7 March. Available from: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ [Accessed 21st October 2020].

Harris, S., Lubold, G. & Sonne, P. (2018) How Kasperskys Software Fell Under Suspicion of Spying on America. *The Wall Street Journal*. January 5. Available from: https://www.wsj.com/articles/how-kasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888 [Accessed 21st October 2020].

Harris, S. & Barrett, D. (2019) Justice Department investigates Sci-Hub founder on suspicion of working for Russian intelligence. *The Washington Post*. 19 December. Available from: https://www.washingtonpost.com/

national-security/justice-department-investigates-sci-hub-founder-on-suspicion-of-working-for-russian-intelligence/2019/12/19/9dbc-b6e6-2277-11ea-a153-dce4b94e4249_story.html [Accessed 21st October 2020].

Hartmann, K. & Giles, K. (2020) The Next Generation of Cyber-Enabled Information Warfare. In Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky, G. (eds.), *12th International conference on cyber conflict, 20/20 vision: The next decade*. NATO CCDCOE Publications, Tallinn, pp. 233-249.

Haslam, J. (2015) *Near and Distant Neighbours: A New History of Soviet* Intelli*gence*. New York: Farrar Strauss and Giroux.

Heller, M. (2018) Durov refuses to hand over Telegram encryption keys to FSB. *TechTarget*. 21 March. Available from: https://searchsecurity.techtarget.com/news/252437323/Dorov-refuses-to-hand-over-Telegram-encryption-keys-to-FSB [Accessed 21st October 2020].

Herbst, J. & Erofeev, S. (2019) *The Putin Exodus: The New Russian Brain Drain*. The Atlantic Council, Eurasia Center. Available from: https://publications.atlanticcouncil.org/putin-exodus/The-Putin-Exodus.pdf [Accessed 21st October 2020].

Howells, L. & Kalfoglou, Y. (2020) Security Think Tank: AI cyber attacks will be a step-change for criminals. *Computer Weekly*. 2 July. Available from: https://www.computerweekly.com/opinion/Security-Think-Tank-AI-cyber-attacks-will-be-a-step-change-for-criminals [Accessed 21st October 2020].

International Military-Technical Forum 'Army-2018'. (2018) A Strategy for the Development of Technologies in the Sphere of Artificial Intelligence for the National Security of the Russian Federation. 24 August 2018. Moscow region. Russia (held at the Patriot Expo).

Izvestiya. (2019) Nazvany zarplaty IT-spetsialistov v Rossii [The salaries of IT-specialists in Russia have been announced]. *Izvestiya*. 13 September. Available from: https://iz.ru/920869/2019-09-13/nazvany-zarplaty-it-spetcialistov-v-rossii [Accessed 21st October 2020].

Jones, J. M. (2019) Trump Job Approval Sets New Record for Polarisation. *Gallup*. 16 January. Available from: https://news.gallup.com/poll/245996/trump-job-approval-sets-new-record-polarisation.aspx [Accessed 21st October 2020].

Katwala, A. (2018) Why Chinas perfectly placed to be quantum computing's superpower. *WIRED*. 14 November. Available from: https://www.wired.co.uk/article/quantum-computing-china-us [Accessed 21st October 2020].

Khodarenok, M. & Zatari A. (2017) Kibervoyna: chem opasny lyudi s noutbukami [Cyberwarfare: why people with notebooks are dangerous]. *Gazeta.ru*. 27 August. Available from: https://www.gazeta.ru/army/2017/08/26/10859996.shtml [Accessed 21st October 2020].

Kolomychenko, M. (2017) U kiberbezopasnosti menyaetsya curator [Cybersecurity is changing its director]. *Kommersant*. 13 January. Available from: https://www.kommersant.ru/doc/3189312 [Accessed 21st October 2020].

Kolomychenko, M. (2018) Exclusive: Russian high tech project flounders after US sanctions. *Reuters*. 17 October. Available from: https://www.reuters.com/article/us-russia-usa-sanctions-technology-exclu/exclusive-russian-high-tech-project-flounders-after-u-s-sanctions-idUSKCN1MR1LF [Accessed 21st October 2020].

Korotaev, V. (2017) V internet vveli kibervoyska [A cyberforce was introduced to the internet]. *Kommersant*, 10 January. Available from: https://www.kommersant.ru/doc/3187320 [Accessed 12th November 2020].

Kottasova, I. (2017) Why Russia's cyber defences are so weak. *CNN*. 15 May. Available from: https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Accessed 21st October 2020].

Kozlov, V. (2020) Russian Tech Industry Faces Coronavirus Brain Drain. *The Moscow Times*. 17 June. Available from: https://www.themoscowtimes.com/2020/06/17/russian-tech-industry-faces-coronavirus-brain-drain-a70607 [Accessed 21st October 2020].

Kramer, A. E. (2016) How Russia Recruited Elite Hackers for Its Cyberwar. *New York Times*. 29 December. Available from: https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html [Accessed 21st October 2020].

Kramer A. E. (2017) Hacker Is a Villain to Russia and the United States, for Different Reasons. *New York Times*. 16 March. Available from: https://www.nytimes.com/2017/03/16/world/europe/russian-hacker-fsb-agent-dmitry-dokuchaev.html [Accessed 21st October 2020].

Krasnaya Vesna. (2018) Bolshaya chast raboty nauchnykh rot ukhodit v stol [The majority of science companies work is useless]. *Krasnaya Vesna.* 24 February. Available from: https://rossaprimavera.ru/news/6cccb188 [Accessed 21st October 2020].

Kremlin.ru. (2006) Poslanie Federalnomu Sobraniyu Rossiyskoy Federatsii [Address to the Federal Assembly of the Russian Federation]. 10 May. Available from: http://kremlin.ru/events/president/transcripts/23577 [Accessed 21st October 2020].

Lata, V. F., Annenkov, V.A. & Moiseev, V.F. (2019) *Informatsionnoe Protivoborstvo: Sistema Terminov i Opredelenniy* [Information Confrontation: A System of Terms and Definitions]. *Vestnik Akademii Voennykh Nauk.* 2 (67), 128-38.

Lenta.ru. (2017) Byvshiy sotrudnik voennovo NII osuzhden za khishchenie radiodetaley na 40 millionov [A former worker of a military research institute was sentenced for stealing radio equipment worth 40 million]. *Lenta*. 31 January. Available from: https://lenta.ru/news/2017/01/31/radiodetali/ [Accessed 21st October 2020].

Levin, I. I. (2004). *Metody I programmno-apparatnye sredstva parallelnykh strukturno-protsedurnykh vychislenniy* [Methods and software and hardware for parallel structural-procedural computations]. Doctor of Technical Science Dissertation. Taganrog State Radio-Technical University.

Lysenko, V. & Brooks, C. (2018) Russian information troops, disinformation and democracy. *First Monday*. 23 (5). Available from: https://firstmonday.org/article/view/8176/7201 [Accessed 12th November 2020].

Macaulay, T. (2020) Russia's most notorious troll farm reportedly used deepfakes to push a fake news outlet on Facebook. *The Next Web*. 2 September. Available from: https://thenextweb.com/neural/2020/09/02/russias-most-notorious-troll-farm-reportedly-used-deepfakes-to-push-a-fake-news-outlet-on-facebook/ [Accessed 21st October 2020].

Markotkin, N. & Chernenko, E. (2020) *Developing Artificial Intelligence in Russia: Objectives and Reality*. Carnegie Moscow Center. 5 August. Available from: https://carnegie.ru/commentary/82422 [Accessed 16th November 2020].

Marks, J. (2020) The Cybersecurity, 202: Chinese hackers could work for the gov-

ernment – or themselves. *The Washington Post*. 22 July. Available from: https://www.washingtonpost.com/politics/2020/07/22/cybersecurity-202-chinese-hackers-could-work-government-or-themselves/ [Accessed 21st October 2020].

Matlack, C., Riley, M. & Robertson, J. (2015) The Company Securing Your Internet Has Close Ties to Russian Spies. *Bloomberg*. 19th March. Available from: https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies [Accessed 21st October 2020].

Maurer, T. (2018) Why the Russian Government Turns a Blind Eye to Cybercriminals. *Slate*. 2 February. Available from: https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html [Accessed 21st October 2020].

Maurer, T & Hinck, G. (2018) Russia's Cyber Strategy. *ISPI Online*. 21 December. Available from: https://www.ispionline.it/it/pubblicazione/russias-cyber-strategy-21835 [Accessed 21st October 2020].

Melkozerova, V. & Parafeniuk, O. (2020) How coronavirus disinformation caused chaos in a small Ukrainian town. *NBC News*. 3 March. Available from: https://www.nbcnews.com/news/world/how-coronavirus-disinformation-caused-chaos-small-ukrainian-town-n1146936 [Accessed 21st October 2020].

Miller, C. (2020) A Small Town Was Torn Apart by Coronavirus Rumors. *Buzzfeed News*. 9 March. Available from: https://www.buzzfeednews.com/article/christopherm51/coronavirus-riots-social-media-ukraine [Accessed 21st October 2020].

Modestov, S. (1997). *SShA gotovy k informatsionnoy voyne s Rossiey* [The US is ready for an information war with Russia]. *Nezavisimoe Voennoe Obozrenie*. 52 (25), pp. 15-23.

The Moscow Times. (2015) Russia's DARPA Working on Underwater Battlebots to Protect Coastline. *The Moscow Times*. 8 July. Available from: https://www.themoscowtimes.com/2015/07/08/russias-darpa-working-on-underwater-battlebots-to-protect-coastline-a48005 [Accessed 21st October 2020].

The Moscow Times. (2019) Record Number of Russians Want to Emigrate – Gallup. *The Moscow Times*. 4 April. Available from: https://www.themoscowtimes.com/2019/04/04/record-number-of-russians-want-to-emigrate-gallup-a65092 [Accessed 21st October 2020].

Nakashima, E. & Warrick, J. (2012) Stuxnet was work of US and Israeli experts, officials say. *The Washington Post*. 2 June. Available from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [Accessed 21st October 2020].

National Association for International Information Security (NAIIS). (2020) *Management of the Association*. Available from: http://namib.online/en/president-of-naiis/ [Accessed 21st October 2020].

National Security Agency (NSA) & The Federal Bureau of Investigation (FBI). (2020) NSA and FBI Expose Russian Previously Undisclosed Malware "Drovorub" in Cybersecurity Advisory. *Press Room*. 13 August. Available from: https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/ [Accessed 16 November 2020].

Nesmeyanov, V. (2017) *Eta tikhaya, smertelnaya voyna* [This quiet, deadly war]. *Flag Rodiny*. 17 (27273), p. 7.

Nimmo, B. & Yap, N. (2018) #TrollTracker: Russia's Other Troll Team. *Digital Forensic Research Lab*. 2 August. Available from: https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5 [Accessed 21st October 2020].

Nimmo, B., Francois, C., Eib, S. & Tamora, L. (2020a). *From Russia With Blogs*. Graphika. Available from: https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf [Accessed 21st October 2020].

Nimmo, B., Francois, C., Eib, S. & Tamora, L. (2020b) *Secondary Infektion*. Graphika. Available from: https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf [Accessed 21st October 2020].

Office of the Director of National Intelligence (ODNI). (2020) *The U.S. Intelligence Community Budget*. Available from: https://icontherecord.tumblr.com/ic-budget [Accessed 16 November 2020].

Peters, B. (2017) *How Not to Network a Nation: The Uneasy History of the Soviet Internet.* MIT Press: London.

Peterson, D. J. (2005). *Russia and the Information Revolution*. Santa Monica: RAND Corporation. Available from: https://www.rand.org/pubs/monographs/MG422.html [Accessed 21st October 2020].

Pomerleau, M. (2018) Here are the cyber staffing issues facing the Defence Department. *Fifth Domain*. August 3. Available from: https://www.fifthdomain.com/dod/cybercom/2018/08/03/can-cyber-command-overcome-its-staffing-shortage/ [Accessed 21st October 2020].

Popa, B. (2016) Russian President Spokesman Says It's Impossible to Give Up on Foreign Software. *Software Russia*. 4 November. Available from: http://www.software-russia.com/in_focus/media/russian-president-spokesman-says-it-is-impossible-to-give-up-on-foreign-software [Accessed 21st October 2020].

Popov, I. M. (2013) Vzglyad na deystviya v kiberprostranstve pod voennym uglom zreniya [A military perspective on actions in cyberspace]. *Nezavisimoe Voennoe Obozrenie*. 13 December. Available from: https://nvo.ng.ru/concepts/2013-12-13/1_war.html [Accessed 21st October 2020].

Positive Hack Days (Phd). (2014) *Best of PHDays*, 2014. Available from: http://2014.phdays.ru/ [Accessed 21st October 2020].

Press Office of the President of the Republic of Lithuania. (2019) *Fight against disinformation is EU priority*. Available from: https://www.lrp.lt/en/media-center/news/fight-against-disinformation-is-eu-priority/32098 [Accessed 21st October 2020].

Radio Free Europe/Radio Liberty. (2017) Putin Compares Hackers to Artists, Says They Could Target Russia's Critics For Patriotic Reasons. *RFE/RL*. 1 June. Available from: https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html [Accessed 21st October 2020].

Radio Free Europe/Radio Liberty. (2018) Investigative Report: On the Trail of the 12 Indicted Russian Intelligence Officers. *RFE/RL*. 19 July. Available from: https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html [Accessed 21st October 2020].

RBC.ru. (2017) Medvedev nazval nedopustimym eksport intellekta iz Rossii [Med-

vedev called the export of intellect from Russia unacceptable]. *RBC.ru*. 27 February. Available from: https://www.rbc.ru/rbcfreenews/58b41aec9a7947ea101ed916 [Accessed 21st October 2020].

RBC.ru. (2018) Rogozin prisval ostanovit vymyvanie mozgov za rubezh [Rogozin urged a stop to brain drain abroad]. *RBC.ru.* 27 February. Available from: https://www.rbc.ru/rbcfreenews/5a9524119a794717e2d20506 [Accessed 21st October 2020].

Reuters. (2017) WannaCry Ransomware Hit Some Russian Banks. *Fortune*. 19 May. Available from: https://fortune.com/2017/05/19/wannacry-ransomware-russia/ [Accessed 21st October 2020].

Romanova, S. (2018) Rekrutery vyyasnili prichiny otezda rossiyskikh IT-spetsialistov za rubezh [Recruiters revealed the reasons for the departure of Russian IT specialists abroad]. *RBC.ru.* 5 June. Available from: https://www.rbc.ru/rbcfreenews/5b168d0e9a7947958ec9dcf3 [Accessed 21st October 2020].

Rozhdestvenskiy, I. & Alekhina, M. (2017) Predatelstvo v FSB: shto izvestno ob arestakh v spetsluzhbe i u Kasperskovo [Betrayal in the FSB: What is known about the arrests in the special service and Kaspersky]. *RBC.ru.* 25 January. Available from: https://www.rbc.ru/society/25/01/2017/58887a2b9a794770370e0d9a [Accessed 21st October 2020].

Russoft. (2017a) Russoft: programmisty nedovolny urovnem svoevo dokhoda [Russoft: programmers are unhappy with their income]. *Russoft*. 13 December. Available from: http://old.russoft.ru/smi/4331 [Accessed 21st October 2020].

Russoft. (2017b) Issledovanie: Okolo 50% Rossiyskikh IT-kompaniy negativno otsenivayut vliyanie sanktsiy na industriyu [Research: About 50% of Russian IT-companies assess sanctions had a negative impact on the industry]. *Russoft*. 7 May. Available from: http://old.russoft.ru/smi/3955 [Accessed 21st October 2020].

Russoft. (2019) *16th Annual Survey: 2019 Russian Software Industry*. Available from: https://russoft.org/wp-content/uploads/2019/12/RUSSOFR-Survey-ENG-2019.pdf [Accessed 21st October 2020].

Sayfetdinov, K. I. (2014) Informatsionnoe Protivoborstvo v Voennoy Sfere [Information Confrontation in the Military Sphere]. *Voennaya Mysl*. 7, 38-41.

Satter, R. & Bodner, M. (2018) Leaked chats show alleged Russian spy seeking hacking tools. *Associated Press*, 1 August. Available from: https://apnews.com/aa719ede3637469a91da829c551fe81b/Leaked-chats-show-alleged-Russian-spy-seeking-hacking-tools [Accessed 21st October 2020].

Schmid, F. & Ulrich, A. (2010) New Documents Reveal Truth on NATOs Most Damaging Spy. *Spiegel International*. 30 April. Available from: https://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-691817.html [Accessed 21st October 2020].

Shurygin, D. (2018) Putin vysoko otsenil tekhnopolis ERA v Anape [Putin highly valued the ERA technopolis in Anapa]. *TV Zvezda.* 22 November. Available from: https://tvzvezda.ru/news/opk/content/201811221606-8wkd.htm [Accessed 21st October 2020].

Sindermann, C., Cooper, A. & Montag, C. (2020) A short review on susceptibility to falling for fake political views. *Current Opinion in Psychology*. 36, 44-8.

Skobelev, Vladislav. (2020) Kasperskaya predupredila Mishustina ob emigratsii IT-spetsialistov za rubezh (Kasperskaya warned Mishustin about the

emigration of IT specialists abroad) *RBC.ru*. 3 June. Available from: https://www.rbc.ru/technology_and_media/03/06/2020/5ed665499a7947fd676d0462 [Accessed 21st October 2020].

Smith-Goodson, P. (2019) Quantum USA Vs. Quantum China: The World's Most Important Technology Race. *Forbes*. 10 October. Available from: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#d91d24072de9 [Accessed 21st October 2020].

Strack, R., Kovacs-Ondrejkovic, O, Antebi, P., Schudey, A., Ignatova, M., & Oblov, A. (2018) *Russia Faces a Talent Conundrum*. Boston Consulting Group. Available from: https://www.bcg.com/publications/2018/russia-faces-talent-conundrum-global-talent [Accessed 21st October 2020].

Stubbs, J. (2017) NotPetya hackers likely behind BadRabbit attack: researchers. *Reuters*. 26 October. Available from: https://www.reuters.com/article/us-cyber-attack-russia/notpetya-hackers-likely-behind-badrabbit-attack-researchers-idUSKBN1CV1TI [Accessed 21st October 2020].

TASS. (2020) Innovation center Skolkovo is not Silicon Valley's counterpart – directors board chair. *TASS*. 2 June. Available from: https://tass.com/science/1163251 [Accessed 21st October 2020].

TASS. (2020) Not Chasing IBM and Google: Russian scientists work on independent quantum computer. *TASS*. 22 January. Available from: https://tass.com/science/1111769 [Accessed 21st October 2020].

Topwar.ru. (2015) Pro sluzhbu v nauchnoy rote [About service in a science company]. *Topwar*. 26 December. Available from: https://topwar.ru/88239-pro-sluzhbu-v-nauchnoy-rote.html [Accessed 21st October 2020].

Troianovski, A. & Nakashima, E. (2018) How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. *Washington Post*. 28 December. Available from: https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html [Accessed 21st October 2020].

Tucker, P. (2018) Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. *Defence One*. 7 December. Available from: https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/ [Accessed 21st October 2020].

Turovskiy, D. (2019) *Vtorzhenie: Kratkaya istoriya Russkikh khakerov (Invasion: A short history of Russian hackers)* Moscow, Inviduum.

Turovsky, D. (2018) It's our time to serve the Motherland: How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. *Meduza*. 7 August. Available from: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland [Accessed 21st October 2020].

Twigg, J. (2019) Russia is Winning the Sanctions Game. *The National Interest.* 14 March. Available from: https://nationalinterest.org/blog/skeptics/russia-winning-sanctions-game-47517 [Accessed 21st October 2020].

Uppal, R. (2019) Russia's Advanced Research Foundation Aims Breakthrough High-Risk Research and Development Like US DARPA. *International Defence, Security & Technology.* February 2. Available from: https://webcache.googleusercontent.com/search?q=cache:Qh3ahoZLDJIJ:Available from: https://idstch.com/industry/russia-s-advanced-research-foundation-advancing-as-an-answer-to-us-darpa/+&cd=1&hl=en&ct=clnk&gl=us [Accessed

21st October 2020].

US Department of Justice. (2020) Russian National Indicted for Conspiracy to Introduce Malware into a Computer Network. *Office of Public Affairs*. 4 September. Available from: https://www.justice.gov/opa/pr/russian-national-indicted-conspiracy-introduce-malware-computer-network [Accessed 21st October 2020].

US Department of the Treasury. (2019) Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. *Press Releases*. 5 December. Available from: https://home.treasury.gov/news/press-releases/sm845 [Accessed 21st October 2020].

US Government Publishing Office. (2014) Hearing on National Defense Authorization Act for Fiscal Year 2015 And Oversight of Previously Authorized Programs before the Committee on Armed Services. *House of Representatives, One Hundred Thirteenth Congress, Second Session.* Available from: https://www.govinfo.gov/content/pkg/CHRG-113hhrg87867/html/CHRG-113hhrg87867.htm [Accessed 16 November 2020].

Vyalykh, S. A. (1999) *Povyshenie effektivnosi zashchity avtomatizirovannykh sistem operativnovo upravleniya ot vredonosnykh programmnykh vozdeystviy* [Raising the effectiveness of automated operational control system defence from the impact of malicious software]. Candidate of Technical Sciences Dissertation. 5th Central Scientific Research Test Institute.

Vesti.ru. (2019) Putin posetil ekspozitsiyu tekhnopolisa Era na forume Armiya, 2019 [Putin visited an exhibition of Era technopolis at the Army, 2019 forum]. *Vesti.ru.* 27 June. Available from: https://www.vesti.ru/article/1321178 [Accessed 21st October 2020].

Villalon, A. (2016) The Russian ICC (V): FSB. *Security at Work*. 20 December. Available from: https://www.securityartwork.es/2016/12/20/the-russian-icc-v-fsb/ [Accessed 21st October 2020].

Wezeman, S. T. (2020) Russia's military spending: Frequently asked questions. Available from: https://www.sipri.org/commentary/topical-backgrounder/2020/russias-military-spending-frequently-asked-questions [Accessed 21st October 2020].

Yapporova, L. (2019) Conspiracy U: A former KGB instructor is winning over students with pseudoscience lectures and FSB internships. *Meduza*. 27 December. Available from: https://meduza.io/en/feature/2019/12/27/conspiracy-u [Accessed 21st October 2020].

Zakharov, R. (2020) V Rossii startoval perviy onlain-khakaton konkursa tsifrovoy proryv [The first online hackathon contest digital breakthrough was started in Russia]. *Zvezda*. 5 June. Available from: https://public.tvzvezda.ru/news/t/2020651844-5qDBr.html [Accessed 21st October 2020].

Zenz, K. (2019) Infighting Among Russian Security Services in the Cyber Sphere [Powerpoint Presentation]. *Black Hat USA*. August. Available at: Available from: https://i.blackhat.com/USA-19/Thursday/us-19-Zenz-Infighting-Among-Russian-Security-Services-in-the-Cyber-Sphere.pdf [Accessed 21st October 2020].

Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.