National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Comparative Analysis of Canada's Cyber Policies and Capabilities in a New Digital Environment

Major Dohyun Shin

JCSP 49

Master of Defense Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 49

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Master of Defense Studies – Maîtrise en études de la défense

Comparative Analysis of Canada's Cyber Policies and Capabilities in a New Digital Environment

Major Dohyun Shin

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.

I would like to express my heartfelt gratitude to several individuals who have played pivotal roles in the completion of this research paper. First and foremost, my deepest appreciation goes to Vic, whose unwavering support, encouragement, and understanding have been invaluable throughout this journey.

I am also immensely grateful to my academic advisor, Dr. Rebecca Jensen, for her guidance, expertise, and valuable insights. Her dedication, constructive feedback, and support has been critical in shaping the ideas and refining the work. Her mentorship has been an inspiration, and I am truly fortunate to have had the privilege of working under her supervision. Furthermore, I would like to extend my thanks to colleagues Brad and Jason for their discussions that have contributed significantly to the development and progression of this research.

To all those mentioned above and to countless others who have contributed to the research in ways big and small, I extend my utmost appreciation. Without your support and encouragement, this research paper would not have been possible. Thank you.

Leave it to Beaver: Comparative Analysis of Canada's Cyber Policies and Capabilities in a New Digital Environment

ABSTRACT

This research paper offers a comparative analysis of cyber security policies and capabilities in Canada, with a focus on the threats from adversarial states of Russia and China, as well as malicious non-state entities. The paper also compares the policies of Canada's allies within the Five-Eyes communities, namely the United States (US), United Kingdom (UK), and Australia. Through the comparative analysis, it highlights vulnerabilities within the cyber domain where Canada should alter course with respect to its policies as well as offer support to the areas where it is succeeding.

In a global society that is becoming more connected than ever, cyber threats from malicious entities pose an existential threat to the emerging digital society. Cyber-attacks from adversarial actors affect not just the government or the military, but the entire spectrum of a nation. As such, Canada must ensure its federal agencies promote private-public sector collaboration at all levels, mandate higher levels of online authentication and safety for individuals, re-evaluate the role of the military in cyber operations, and expand the available work force for the new digital economy.

INTRODUCTION

Cyber space is a relatively new non-physical domain which encompasses "all interconnected communication, information technology and other electronic systems, networks and their data."[1] In the Canada's Cyber Security Strategy of 2010, cyber space is further described as "the electronic world created by interconnected networks of information technology and the information on those networks…where more … people are linked together to exchange ideas, services and friendship."[2] With the rapid adoption of computers and informational technology (IT) in all aspects of society, cyber space has become a forum facilitates more than 4.3 billion people[3] in business, education, health, relationships, and more. However, the interconnected nature of the cyberspace also provides a vector for malicious actors to operate in areas of espionage, theft of intellectual properties, financial crime, terrorism, and state-sponsored actions.[4] Inversely, Canada and its allies are also able to leverage the reach of operating in the cyberspace to target. In fact, recent history has been filled with examples of actions in the cyberspace by both state and non-state actors.

---

[1] The Official NATO Terminology Database, "cyberspace", https://nso.nato.int/natoterm/Web.mvc.
[2] Canada. Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada. Her Majesty the Queen in Right of Canada, 2010. 2
[3] Cyber Centre Learning Hub, Discovering Cyber Security, Module 1.
[4] Add reference

ADVERSARIAL THREATS

Although there are multitude of potential adversaries for Canada within the cyber domain, this paper will focus on the main actors of Russia, China, and non-state organizations. This is backed up in the Canadian Centre for Cyber Security's report on the *National Cyber Threat Assessment: 2023-2024* which specifically listed Russia and China's cyber programs, in addition to Iran and North Korea, as posing the "greatest strategic cyber threat to Canada."[5] As Ukraine found out in its recent war against Russia, if they are "aware of the enemy's motivation and tools, [they] can forecast quite confidently which segments and sectors are most threatened by Russian hackers."[6]

To better understand the state-sponsored cyber programs of Russia and China, an examination of their policies and regulations will need to be conducted. This will provide a baseline understanding of the framework for their programs to recognize their approach to cyber actions and cyber security. In addition, the organizational structure will need to be studied to appreciate their capabilities and respective roles within their cyber programs and how they contribute to the goals of their strategic interests, both in offensive and defensive roles.

Russia has emerged as the focal point of media attention considering their recent full-scale invasion of Ukraine and how their cyber organizations, including the Federal Security Service (FSB), the military intelligence agency (GRU), and the Russian Foreign Intelligence Service (SVR), furthered the government's goals. This is with the backdrop of the widespread media coverage of Russia's interference in foreign elections, targeting of critical infrastructures, and influencing the global population to become more sympathetic to their national interests.

Like Russia, China's cyber program has received attention on how it is being employed to further their national goals. Incidents such as the cyber-attacks against western countries, cyber espionage military technology, and theft of intellectual and trade secrets of companies, have made headlines. These actions were supported by their cyber agencies. The Ministry of State Security (MSS), the People's Liberation Army's Strategic Support Force (PLASSF), and the Ministry of Public Safety (MPS) provide effective tools for the central government to leverage in furthering the economic advancement and in the development of their cyber program capable to challenging the US hegemony in the domain.

In addition to state-sponsored programs, non-state actors, such as hacker groups and cyber-criminal organizations, have emerged as significant players in the cyber domain. Thus, it will be important to examine role of non-state actors in the overall cyber security landscape. Although many of them have some level of alignment to governments and governmental organizations, their influence and reach should be considered

---

[5] Canadian Centre for Cyber Security. National Cyber Threat Assessment: 2023-2024

[6] State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned 2022. 7

considering their financial, political, and ideological motivations. They also provide a useful foil in comparing functionality and capability to state actors.

Understanding the policies and organizational structures of Russia, China, and non-state actors' cyber programs will be crucial in evaluating the cyber security strategies of Canada as they are the main actors from which these policies are designed against.

Russia

> *"Hackers are free people, just like artists who wake up in the morning in a good mood and start painting… The hackers are the same. They would wake up, read about something going on in interstate relations and if they feel patriotic, they may try to contribute to the fight against those who speak badly about Russia."*
>
> *- Vladimir Putin, president of the Russian Federation*[7]

National Security Concept of the Russian Federation. There has been an evolution of Russian policies relating to cyber and the information domain over the years as the understanding and integration of them become more understood and adopted. One of the earlier instances of such policy was the "National Security Concept of the Russian Federation", which was formulated in 1997 and released in 2000 outlining the key strategies relating to their national strategy. Although it focused on the issues of the time, such as weapons proliferation, economic threats, and terrorism, it contained evidence of taking certain factors into account which would tie in to subsequent policies on cyber.

First was the realization that the emerging technology will be of national strategic interest. Within the security concept, the idea that Russia's "weakening of the research-technical and technological potential of the country, dwindling research in the strategic spheres of research-technical progress, the exodus of specialists and intellectual property"[8] would eventually lead to vulnerabilities in their defence and create dependencies on outside actors, such as foreign nations. In addition, it acknowledged the role of the Russian defence industries in serving the needs of the country[9] and the necessity to "improve and protect the national information infrastructure."[10] Although the concept of cyber warfare and cyber security was still nascent, there is evidence that Russia saw the essential role that private companies would have in working with governmental organizations to create a cyber environment conducive in more offensive and defensive actions. Furthermore, the security concept crucially recognized the importance of conducting intelligence and counter intelligence operations to not only find threats against Russia, but to correctly attribute those actions to the responsible parties

---

[7] https://apnews.com/article/moscow-donald-trump-ap-top-news-elections-international-news-281464d38ee54c6ca5bf573978e8ee91

[8] Russia. "National Security Concept of the Russian Federation." Medzinárodné Otázky 9, no. 3 (2000): 99-118. 103.

[9] Russia. "National Security Concept of the Russian Federation." Medzinárodné Otázky 9, no. 3 (2000): 99-118. 115

[10] Ibid, 116.

and nations.[11] The concept of attribution in cyber security, and its converse of obfuscating their own actions, would be a key principle in Russia's actions in the contemporary operating environment. In conjunction with the Information Security Doctrine of the Russian Federation of 2000,[12] it laid a foundation for Russia to develop its cyber strategies.

Information Security Doctrine of the Russian Federation (2000). The doctrine is organized by listing four broad categories encompassing the main national interests from a cyber perspective: information security, methods for ensuring the information security, main propositions of Russian State information security policy and measures to realize it, and the organizational base of the information security system.[13]

The Federal Law on Information, Informational Technologies and the Protection of Information (Federal Law No. 149-FZ). The next key evolution in their regulatory framework addressing specific concerns of information and cyber security was the 2006 law passed by the Duma.[14] The Federal Law on Information, Informational Technologies and the Protection of Information (Federal Law No. 149-FZ) outlined the information protection, storage, and transmission requirements for individuals, private organizations, and the governmental agencies. Although it provided the foundation for information security, it also enabled the central government's reach in to.

The policies as they developed from the immediate aftermath of the collapse of the Soviet Union, to the contemporary Russian security environment of Putin's rigid control over country, demonstrates the intertwined nature of their information and cyber domain capability with that of their national strategic interests. As Kevin Riehle of Center for Intelligence and Security Studies (US) points out, Russia's information and cyber capabilities work "in concert with all other levers of national power to achieve a defined list of Russia's national security objective."[15]

Russian Cyber Organizations.

In order to further the national interests of the Russian Federation, Russia employs a mix of both governmental and non-governmental organizations to act within the cyber domain. The state agencies mainly discussed for cyber activities in Russia include the GRU, SVR, and FSB.[16] All three agencies have roots in more traditional

---

[11] Ibid, 116
[12] INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION 2000 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf
[13] INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION 2000 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf
[14] Russia. FEDERAL LAW NO. 149-FZ OF JULY 27, 2006 ON INFORMATION, INFORMATIONAL TECHNOLOGIES AND THE PROTECTION OF INFORMATION.
[15] Riehle, Kevin P. "Information Power and Russia's National Security Objectives." *The Journal of Intelligence, Conflict, and Warfare* 4, no. 3 (2022): 62.
[16] Soldatov, Andrei and Irina Borogan. "Russia's very Secret Services." World Policy Journal 28, no. 1 (2011): 83-91.

intelligence roles, but with the advent of computers and computer networks, have adapted to have roles in the domestic and foreign cyber spheres.

With the collapse of the Soviet Union, some speculated that their intelligence agencies and their capabilities would diminish[17], and it may have been so during the early tumultuous transition period. With the eventual rise of President Putin and his affixation with Russian intelligence services, the vacuum of control and resources was filled and allowed them to thrive, "enjoying expanded responsibilities and immunity from public oversight or parliamentary control."[18] GRU, having survived the transition from Soviet Union to the Russian Federation control, kept its name, structure, and mandate.[19] Unlike the GRU, the Komitet Gosudarstvennoy Bezopasnosti (KGB) did not survive the transition but the Federal Security Service (FSB) has taken on many of the roles, especially within the former territories of the USSR and is seen as the most direct successor.[20] The Foreign Intelligence Service (SVR), as its namesake suggests, is predominately occupied with targeting Europe, NATO, and especially the United States and their interests.

An important overview of Russian capability and tactics as it relates to cyber-attacks can be learned by examining how it was used during the recent Russian-Ukrainian conflict, as it represents how Russian and Russia-affiliated organizations can work together to support and further their national strategic goals.

The main organizations involved in the cyber-attacks for the Russians during the were GRU, SVR, FSB, and private cyber companies aligned with the political aims of the government.[21] The main aims of the cyber activities for Russia were along the lines of cyber-attacks, cyber espionage, and influence activities to lower the morale of Ukrainians while promoting the global support of their war.

Russian Cyber Attacks.

A key enabler for the Russians in the war has been their frequent offensive cyber actions against Ukraine and its allies in the war effort. It has proved effective, especially in the early stage of the war, by combining cyber-attacks along multiple vectors. Sometimes, these attacks in the cyber domain were combined with kinetic actions, such as missile strike, to eliminate a Ukrainian capability on the cyber and physical domains. From a MDO perspective, it demonstrated Russian military's ability to wage a relatively effective operation in a contemporary environment dominated by the internet and connectivity.

---

[17] Soldatov, Andrei and Irina Borogan. "Russia's very Secret Services." *World Policy Journal* 28, no. 1 (2011): 83-91.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Add reference

At the start of the war, Russia relied on their inhouse development of cyber tools along with their stable of malware and phishing attacks. With the relative inexperience and vulnerabilities within Ukrainian government, military, and critical infrastructure, Russia was able to target a wide range of infrastructure, agencies, and military. One of the protections that Ukraine enjoyed in the early stages of the war from cyber perspective was the lack of widespread adoption of internet of things and connectivity.[22]

However, starting in 2016, the Shadow Brokers started releasing hacking tools, most likely developed by the NSA, on the internet. While Snowden's leaks on the NSA may have been embarrassing and strained relationships among the US and its allies, the Shadow Brokers had an arguably a greater effect on the cyber landscape.[23] In particular, the release of NSA's hacking tools greatly diminished the technological superiority that was enjoyed by the western intelligence community from an offensive point of view, while concurrently making them more vulnerable of these tools being used against them.[24] For example, the *NotPetya,* one of the most costly Russian malware to be released, was developed using elements of the *EternalBlue* exploit. *EternalBlue* was an exploit that was devised by the NSA which was subsequently leaked by the Shadow Brokers in April 2017.[25] By 2018, *NotPetya* was not only employed against Ukrainian, but across the world causing over $10 billion in damages.[26]

Russian Cyber Espionage.

In addition to attacks, Russia has leveraged the cyber domain to conduct frequent and effective cyber espionage. In addition to private companies, the GRU, SVB, and FSB have all conducted espionage and theft of digital materials in Ukraine over the course of the Ukrainian war; however, as Microsoft noted in their special report on Russia's activity in Ukraine, these actions may have started as early as 2021 in order to shape the environment for the subsequent 2022 invasion.[27] It should be noted that "Ukrainian military and cyber responders have been dealing with Russian aggression since at least the first Russian invasion in 2014, making it difficult to identify an exact time when long-term espionage may have shifted to support invasion preparation."[28] But the key takeaway is that cyber is becoming an important shaping activity for Russia prior to more kinetic military operation.

FSB, have been the most active agency involved in cyber espionage actions in Ukraine.

---

[22] Add reference Nicole peroth
[23] https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/?sh=44fb0464417f
[24] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[25] https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html
[26] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[27] An overview of Russia's cyberattack activity in Ukraine. Pg 5
[28] An overview of Russia's cyberattack activity in Ukraine. Pg 5

Russian Cyber Influence Activities.

In addition to attacks and espionage, Russia has been able to successfully leverage its cyber influence operations to promote Russian interests, including in its war with Ukraine. In many cases, these influence activities seem to be linked with other cyber actions as part of concerted efforts in pushing certain narratives.[29] This is in line with previous techniques and tactics developed by the KGB during the Soviet era, but enabled with modern ICT in order to act with "greater reach, higher volume, more precise targeting, and greater speed and agility."[30]

As per Microsoft's assessment on the Russian cyber influence surrounding the Ukraine war, their agencies are operating along four lines of operations: the Russian population to support the war, the Ukrainian public to demoralize them in an effort to damage their willingness to defend their country, Western populations to ignore or downplay Russian transgressions, and nonaligned countries to maintain or mitigate the damage to their reputation and interests abroad.[31]

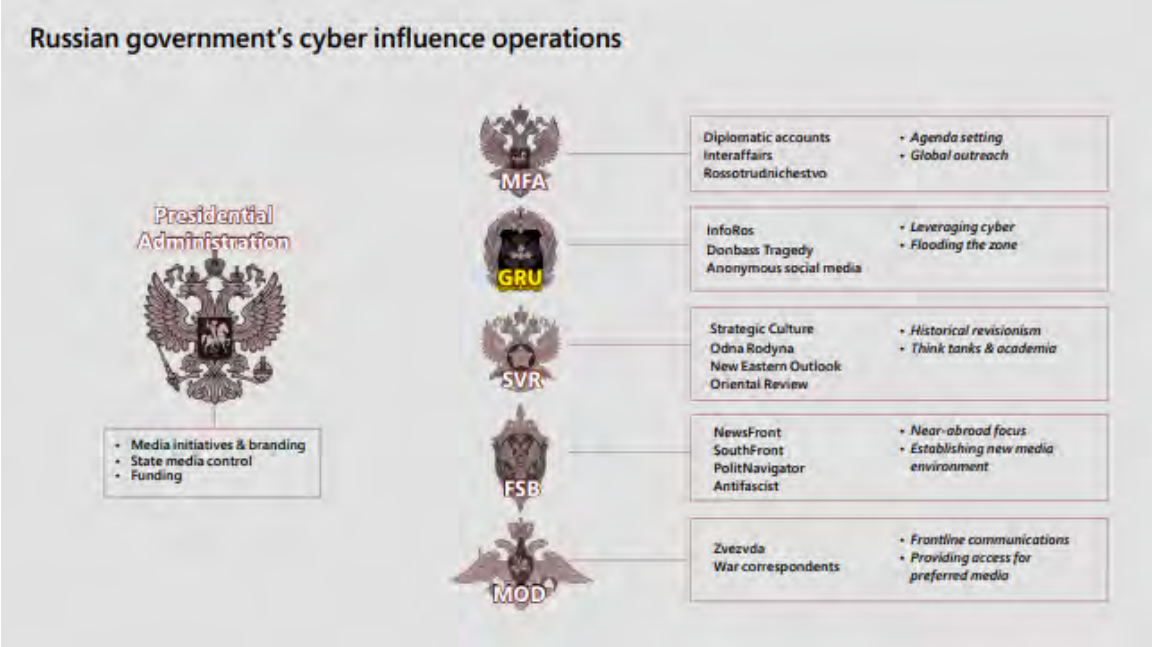

Figure 1- Russian government's cyber influence operations[32]

[29] Microsoft. Defending Ukraine: Early Lessons from the Cyber War. pg 3 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
[30] Ibid, 3.
[31] Ibid, 4.
[32] Ibid, 13.

China

> *"And although this was never formally articulated, in private conversations Chinese officials made clear that economic cyber espionage was seen as justifiable retribution for the indignities suffered by China at the hands of the West during the so-called Century of National Humiliation."* [33]

Although Russia has seen the brunt of the media scrutiny in recent years, China has quietly built up a competitive cyber force capable of conducting cyber activities at home and abroad. In fact, the Council on Foreign Relations in its Cyber Operations Tracker shows that China has sponsored 222 cyber operations since 2005, compared to 142 for Russia.[34] Chinese growth in their capacity and reach in the cyber domain is a growing concern, especially in light with their agreement in principle to cooperate with Russia.[35] An examination of their history and policies shows their desire to use the emerging ICT technology to control their domestic population, provide a counter to American hegemony in the cyber domain, and use of cyber activities to further their national interests in the real world.[36]

To carry out these cyber activities, the main state sponsored actors in China will be explored. The main Chinese intelligence agencies of the Ministry of State Security (MSS), the People's Liberation Army (PLA), the Ministry of Public Security (MPS), and the Ministry of Industry and Information Technology will be covered, along with examples of their involvement in cyber-attacks and espionage. In addition to these agencies, the Cyberspace Administration of China (CAC) will be examined as the government agency responsible for overseeing China's internet and cybersecurity policies, including their cooperation with the former organizations in carrying out cyber operations.

Chinese Cyber History and Policies.

Since China's adoption of the internet in 1994,[37] China has grown to become one of the most connected countries in the world with over a billion Chinese having internet and mobile internet connectivity.[38] The journey from nascent adoption to a major global player in the cyber domain was marked predominately by periods of cooperation,

---

[33] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. 202

[34] https://www.cfr.org/cyber-operations/, last accessed 11 April 2023

[35] Soldatov, Andrei and Irina Borogan. "Russia's very Secret Services." World Policy Journal 28, no. 1 (2011): 83-91.

[36] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020.

[37] Belli, Luca. "Cybersecurity Policies in China." In Cyberbrics, 183-226. Switzerland: Springer International Publishing AG, 2021. p184

[38] https://www.statista.com/statistics/273973/number-of-mobile-internet-users-in-china/#:~:text=This%20statistic%20shows%20the%20number,in%20the%20end%20of%202021.

followed by periods of disagreements, with the United States.[39] A year considered to be a major turning point is in 2010 when "political disagreement regarding online information emerged"[40] involving the US' push for internet freedom, along with "harsh criticism of China's cyber censorship and its restrictions on the free flow of information."[41]

Since the early days of the internet, the Chinese regime saw the emerging ICT as a means to accelerate "the development of the national economy."[42] Trying to comprehend China's cyber strategies and policies is difficult as it involves navigating through the iterations of Chinese white papers and specific policies.[43] China's first pertinent white paper was published in 2010,[44] which established the internet as intrinsically linked to their national economy. A new plan was developed and promulgated in 2015 as "Internet Plus" to 'integrate mobile internet, big data, cloud computing and the Internet of Things to modernise traditional industries."[45] That year, the concept of a "Digital Silk Road" was also developed to be incorporated into the overall "Belt and Road Initiative" in order to seek new markets for Chinese technological products and services.[46] This push to leverage the cyber domain in furthering China's economic interests further entrenched the two together. In essence, the goal of increasing broadband penetration to the population and transforming China into a major player in ICT was not only to become a global internet hegemon,[47] but rather to promote a policy of Informatization in order to 'tackle economic developmental problems' through finding efficiencies in technology.[48]

The widespread distribution of internet access and the information that comes along with it also posed a threat to the authoritarian control of the Chinese government and the Chinese Communist Party. This is why China is very much focused inwards when considering cyber policies. This is most famously exemplified by the Golden Shield project, including the Great Firewall of China which is part of it.[49] The firewall works by blocking access to domains, websites, and URLs[50] which include information

---

[39] Jinghua, Lyu and Gaurav Kalwani. "Navigating the US-China Competition in Cyberspace." Turkish Policy Quarterly 19, no. 2 (2020): 135-144. P 136
[40] Ibid, 136.
[41] Ibid, 136.
[42] Parasol, Max. "China's Cyber Policies: Conflict between Innovation and Restriction." In AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, 62-79, 2021. p62
[43] Raud, M. (2016, August). China and Cyber: Attitudes, Strategies, Organisation . Tallinn, Estonia: NATO CCDCOE. https://haldus.taltech.ee/sites/default/files/2021-03/ICR2015_proceedings.pdf#page=14
[44] Parasol, Max. "China's Cyber Policies: Conflict between Innovation and Restriction." In AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, 62-79, 2021. p62
[45] Ibid, 63.
[46] Belli, Luca. "Cybersecurity Policies in China." In Cyberbrics, 183-226. Switzerland: Springer International Publishing AG, 2021. p184-185
[47] Parasol, Max. "China's Cyber Policies: Conflict between Innovation and Restriction." In AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, 62-79, 2021. p63
[48] Ibid, 63.
[49] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020. p288
[50] In simple terms, the domain is the name, the URL is the address, and the website is the page that visitors see and click on.

that the government wants to limit its population from having access to. For China, this includes information such as the Tiananmen Square, Taiwan, Tibet, Falun gong, and other events and groups which runs counter to the government narratives.[51] This explicit form of censorship and control is not limited to just certain words, but it also includes entire platforms and services, such as "Google, YouTube, and other media interfaces that exude free though and free flow of information."[52]

To exercise the level of control within the cyber domain required to regulate its economic growth and domestic censorship, China has placed strict regulations on its corporations in its application of ICT[53] and developed a framework of cyber sovereignty.[54]

Chinese Cyber Organizations

The Ministry of State Security (MSS) is the main civilian intelligence agency[55] in China who is responsible to conduct a wide range of intelligence activities, including counterintelligence, foreign intelligence, and political security. It was created in 1983 through a merger of the Investigation Department of the CCP with the counter espionage elements of the MPS.[56] Although not mentioned explicitly in its mandate, the MSS has been involved many of the detected foreign intelligence collection efforts[57], including cyber espionage targeting the US, with the resulting information being passed on to other governmental agencies or state-affiliated corporations for their material benefit.[58] These attacks are often carried out through subordinate organizations, labelled as advanced persistent threat (APT) by the FBI. MSS affiliated entities such as APT40, also known as BRONZE MOHAWK, FEVERDREAM, G0065, GreenCash, Hellsing, Krptonite, Panda, and other alias, have targeted various levels of Western society. This includes attacking governments, corporations, and research facilities in the "United States, Canada, Europe,

---

[51] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020. p288
[52] Ibid, 288.
[53] Ibid, 288.
[54] Belli, Luca. "Cybersecurity Policies in China." In Cyberbrics, 183-226. Switzerland: Springer International Publishing AG, 2021. p184
[55] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. P205
[56] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. P205
[57] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. 199
[58] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. 200

the Middle East… South China Sea area, as well as industries included in China's Belt and Road Initiative."[59]

The Ministry of Public Security (MPS) is another civilian agency who's responsible for public order, as its name suggests; however, it is also tasked to run counter intelligence and counter espionage as part of its mandate.[60]

In addition to the civilian agencies, the People's Liberation Army (PLA) runs China's military intelligence, with the PLA Strategic Support Force (SSF) carrying out cyber activities since its creation. The SSF was formed in 2015 as part of China's efforts to project its military power in the emerging domains of space and cyber space.[61] The PLA had the capability to operate in these domains, but they were scattered across different PLA organizations and entities. [62] The SSF arose to consolidate PLA's space, cyber, info ops, and psyops functionalities into one responsible organization. The broad mandate to "obtain information dominance"[63] provides the SSF with the latitude to conduct its activities with relative freedom. The SSF in turn provided the PLA with the ability to conduct hybrid warfare "in the form of digital public opinion warfare,"[64] mirroring the capacity of their Russian counterpart's influence activities in the cyber domain. A contextual differentiator is that China looks at cyber activities as part of the informational warfare and not a sperate domain in of itself.[65] Regardless of the difference, the SSF is considered to have sophisticated tools, resources, and cyber operators/hackers capable of conducting large scale attacks on targeted networks and conduct influence activities in line with their strategic narratives.[66]

This modern and capable cyber force did not emerge by happen stance. In the early days of the internet, the PLA faced issues with qualified and suitable personnel, lack of technology, and people to lead the cyber warfare integration.[67] "Beijing has

---

[59] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a
[60] Inkster, Nigel. "The Chinese Intelligence Service." In The Routledge International Handbook of Universities, Security and Intelligence Studies, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020. P199
[61] https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/
[62] Ibid.
[63] THE PLA BEYOND BORDERS Chinese Military Operations in Regional and Global Context, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf
[64] THE PLA BEYOND BORDERS Chinese Military Operations in Regional and Global Context, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf. p 295
[65] THE PLA BEYOND BORDERS Chinese Military Operations in Regional and Global Context, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf . p296
[66] https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/
[67] THE PLA BEYOND BORDERS Chinese Military Operations in Regional and Global Context, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf . p 298

demonstrated its willingness to enlist the aid of China-based commercial enterprises to help surveil and censor PRC critics abroad, and China's technology industry is a key global supplier of advanced surveillance technologies to foreign governments."[68]

China's Cyber Activities.

Chinese MSS-affiliated actors, much like other state and non-state sponsored cyber attackers, continue to leverage open-source tools and resources to use "relatively low-complexity capabilities to identify and exploit target networks."[69] Most commonly, the TTP involves targeting networks by attacking the gaps in configuration management and outdated or poor patching of security updates.[70]

Although the focus on China's cyber activities is on its espionage of intellectual property and exfiltration of military data, they represent a serious threat to the West's cyber security. "China is the leading threat actor for cyber espionage operations. Examples of such operations include spying on the networks and services of telecommunication companies and conducting malign influence activities to undermine the United States' geopolitical standing."[71]

Non-state Actors

Although state-sponsored actors in the cyber space provide for an easily identifiable adversary and threat that Canada and the West need to compete against, the non-state actors are a major player who must be considered. As described earlier, the cyber domain has intrinsic benefits for the 'underdogs' who may have less resources. The low barrier to entry, combined with the global reach, allows small groups or even individuals to be able to potentially have a significant impact on targets. This is not to say that they can compete on equal footing with state-sponsored cyber organizations who have access to both resources and a large talent pool. Although there is still the caricature of a basement dwelling hacker who can exploit vulnerabilities in state and corporate networks to steal money and secrets, most cyber security policies and systems in place guarding those networks represent too great of a challenge for individuals. In fact, when looking at the major cyber-attacks in recent times, they have been directly or indirectly attributed, or at least strongly linked, with powerful government organizations, such as the NSA. This can be attributed to the rapidly growing awareness and development in states and corporations' cyber security capabilities for each comparable resource would naturally be required to overcome them. But no walls are impenetrable, and non-state

---

[68] Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community. 6 Feb 2023. p 28

[69] Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-258a

[70] Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-258a

[71] https://www.csis.org/analysis/emerging-cyber-threats-no-state-island-cyberspace#:~:text=China%20is%20the%20leading%20threat,the%20United%20States%27%20geopolitical%20standing.

actors can carve out an existence within the cyber domain and, although no longer the norm, have major impacts.

Some of these groups are backed by states directly and act as proxies in going after targets that are assigned.[72] These organizations, although can be broadly categorized as non-state actors, will not be discussed in this section as their involvement is directly linked to state backing; however, these groups can be indirectly backed as proxies. Chris Whyte and Brian Mazanec, in their book "Understanding Cyber-Warfare: Politics, Policy and Strategy" categorizes non-state actors into most common groupings of: cyberterrorists, proxies, hacktivists, subversives, criminals, and vicious employees.[73] Although these categories provide a generalized groups to assist in examine the various role or roles a non-state actor can have, the characteristics that define them are often not clear cut and at times can straddle two or more categories simultaneously. To add further complexity, these groups can be hired for a period or to conduct specific tasks in order for states or other organizations to assist in avoiding attribution.[74]

ALLIES' CYBER CAPABILITIES

In the previous section, the adversarial threats from Russia, China, and non-state actors were examined, along with the key considerations. As much as it is important to look at the adversarial threats, it's also valuable to study the policies and organizations in place who are in a similar position as Canada. When looking at the adversarial threats, Canada is probably not the main target of those organizations. Although Canadian networks are targeted and challenged with constant reminders from the media, Canadian allies such as the US and UK present a more alluring choice as the recipients of attention. By looking at how our allies who have these challenges have structured themselves, it may provide Canada with a useful azimuth check on the current progress. Furthermore, the allies' more developed cyber capabilities may provide a useful point at which to aim.

To examine our allies' capabilities, the US, UK, and Australia were chosen for this paper. The choice to include the US is more obvious as they are the global hegemon for military power, including in the cyber domain. Many of their tools have been the foundation for many of the global cyber-attacks, as demonstrated in the above section when discussing adversarial actions. Furthermore, the leaks from within, such as the Snowden documents, as well as through opposing organizations, such as the Shadow Brokers, have shined some light on the activities of its intelligence agencies. As Canada's closest military and intelligence ally, understanding their policy development and organizational capabilities surrounding cyber will be important when considering Canada's own policies.

---

[72] Whyte, Christopher and Brian M. Mazanec. Understanding Cyber-Warfare: Politics, Policy and Strategy. Milton: Taylor & Francis Group, 2023. 242
[73] Whyte, Christopher and Brian M. Mazanec. Understanding Cyber-Warfare: Politics, Policy and Strategy. Milton: Taylor & Francis Group, 2023. 242
[74] Whyte, Christopher and Brian M. Mazanec. Understanding Cyber-Warfare: Politics, Policy and Strategy. Milton: Taylor & Francis Group, 2023. 242

The UK was also selected as an allied nation to consider. As the sole five eyes intelligence partner in Europe, the UK provides a unique vantage point from which to observe cyber activities. Russia is still the main threat in the consciousness, especially considering the ongoing war on the continent following Russia's full-on invasion of Ukraine in 2022. Although oceans away, China's cyber activities in the UK and within UK's sphere is a growing concern.[75] UK's policies and organizational experience, sharpened and made famous during their exploits in the Second World War and the ensuing Cold War in Europe, provides a foil with which to compare Canada's policies and organizational structure.

Australia also provides a unique five eyes perspective, particularly in the Indo-Pacific. As stated in *Canada's Indo-Pacific Strategy*, Australia is an important partner for Canada's interests in the region.[76] As Canada seeks to "deploy additional military assets and increase its investments in border and cyber security"[77] in the region, an understanding of Australia's policies and organizations related to the cyber domain will provide valuable takeaways for Canada from their experience. This will assist Canada in being able to respond quickly and effectively for cyber security issues and threats that originate from the Indo-Pacific.[78]

The examination of the allied countries of US, UK, and Australia will provide important insight when looking at their cyber policies and organizations. Their diversity in geography, populations, and resources will allow for different perspectives and knowledge to be learned from. Among the three allied countries, cyber activities in the Americas, Europe, and the Indo-Pacific will be covered. This is in addition to a diverse range of population and resources for their respective programs.

United States

Overview. The US, as the birthplace of the internet,[79] has developed into a cyber hegemon to rival their lead in other military domains of land, air, sea, and space. As the internet was being developed, the US government showed openness with working with universities and corporations alike by providing funding and resources required in such ambitious endeavours. As the technology for the internet migrated from the original use case of creating an interconnected system to link the US's ballistic missile program in 1966 to other civilian and academic applications throughout the world, the US government slowly reduced their control over the oversight of the global network.[80]

---

[75] NCSC Annual Review 2022. https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[76] Canada. Canada's Indo-Pacific Strategy. Global Affairs Canada. (Ottawa, ON: 2022). 5
[77] Canada. Canada's Indo-Pacific Strategy. Global Affairs Canada. (Ottawa, ON: 2022). 14
[78] Canada. Canada's Indo-Pacific Strategy. Global Affairs Canada. (Ottawa, ON: 2022). 16
[79] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020. 463
[80] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020. 463

As the first adopter and birthplace of the internet, the US has been able to enjoy various advantages within the cyber space.[81] With significant presence of US government, researchers, and corporations within the domain and development of ICTs, they often provide the standardization and protocols for other nations and participants must follow, lest they be left out of the global clique.

This advantage and lead role in the new interconnected global economy made the US a larger target.[82] In 2003, the US released one of the first national cyber strategies, titled, "The National Strategy to Secure Cyberspace."[83] Although the strategy was published more than twenty years ago, many of the threats and objectives outlined in the document still permeates today. Concerned with the "speed and anonymity of cyber-attacks" and the difficulties in being able to attribute the responsible actors, the strategy was focused on preventing cyber-attacks against critical infrastructures, reduce areas within the US that may be susceptible from cyber-attacks, and to minimize the impact of the attacks when they are successful.[84] To achieve the aim, the strategy outlined several priorities in establishing the American approach to cyber security.

One of the key aspects of the 2003 strategy was to reinforce the importance of the public-private system built on cooperation in responding to cyber incidents of national concern.[85] This priority drove the requirement to ensure a coordinated response system would be in place to mitigate the impact of any cyber-attacks from adversarial and enemy actors. Another key aspect of the strategy was the National Cyberspace Security Threat and Vulnerability reduction program designed to strengthen the resiliency against cyber activities.[86] In particular, critical infrastructure and government departments were highlighted as particular vulnerable vectors for which to protect. The third priority was to increase the awareness through training programs.[87] Even today, the threat to networks through individual users are of significant concern which need to be addressed through continuous awareness and training to prevent unwitting employees opening the doors for malicious actors to enter.[88] The fourth priority was in ensuring that the US government can "lead by example"[89] in securing their ICT through assurance technologies. The final

---

[81] Romaniuk, Scott N. and Mary Manjikian. Routledge Companion to Global Cyber-Security Strategy. Milton: Taylor & Francis Group, 2020. 463
[82] https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf
[83] Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003.
[84] Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003. p viii
[85] Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003. p 3
[86] Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003. p 3
[87] Ibid, 4.
[88] Microsoft Digital Defense Report 2022. p 21
[89] Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003. p 4

priority was in protecting the links within the cyber domain between the US and the global networks.[90]

After the 2003 national strategy on cyber security, the US released policies and laws aimed at further strengthen their defences against threat actors. This included laws such as the "Undertaking Spam, Spyware, and Fraud with Enforces Beyond Borders Act of 2006"[91]; however, the next major iteration was not promulgated until 2018. That year, the National Cyber Strategy (September 2018)[92] and the Department of Homeland's Cybersecurity Strategy (May 2018)[93] were released describing their respective vision and priorities.

National Cyber Strategy (2018)

The National Cyber Strategy signed by President Trump recognized and reinforced previous cyber strategy of the US while providing a way forward on dealing with the "new threats and a new era of strategic competition."[94] To do so, four pillars were outlined to action in order to ensure that the "US cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data" as well as increasing the resiliency of these area by minimizing the harm and speeding up the recovery from attacks.[95]

The first pillar was aimed at defensive efforts to protect US networks.[96] It acknowledges the role of the federal government in assuming responsibility to secure information and security systems that US relies on.[97] In order to effect this change, the US aimed to centralize the management and oversight of the civilian cybersecurity through the Department of Homeland Security. Furthermore, it emphasizes the need to ensure that federal contractors secure government information and access to system in line with appropriate precautions. To mitigate a patch work of ICT equipment and patches, the government's plan was to adopt a consolidated acquisition strategy, thereby reducing overhead and establishing a consistent contract terms and provisions.[98] Other priority actions within the pillar included refining roles and responsibilities, leveraging ICT provides as cybersecurity enablers, incentivize investments into cybers security,

---

[90] Ibid, 4.
[91] UNDERTAKING SPAM, SPYWARE, AND FRAUD WITH ENFORCERS BEYOND BORDERS ACT OF 2006. https://www.congress.gov/109/plaws/publ455/PLAW-109publ455.pdf
[92] Whitehouse. National Cyber Strategy of the United States of America. September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[93] Department of Homeland Security. Cybersecurity Strategy. 15 May 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
[94] Whitehouse. National Cyber Strategy of the United States of America. September 2018. p2
[95] Whitehouse. National Cyber Strategy of the United States of America. September 2018. P3
[96] Ibid, 6.
[97] Ibid, 6.
[98] Ibid, 8.

prioritize national research and development, better support transportation and maritime cyber security, and improve space cybersecurity.[99]

The second pillar was aimed at "promoting American prosperity"[100] through growing its digital economy in both domestic and international markets, protecting American intellectual property, and increasing education and training of its workforce to compete in this digital economy.[101] Within these broader categories, there were specific mentions of priority actions, such as continuing to advocate for international standards and regulations for ICT and cyber domain.

The third pillar was intended to "preserve peace through strength"[102] through defensive cyber activities in responding to attacks, offensive cyber activities to disrupt and deter adversarial actors from taking action, and imposing consequences once actions have been taken against American networks or national interests within the cyber domain.[103] This included a whole-of-government approach where consequences was not necessarily in kind through the cyber domain but could encompass various law enforcement, diplomatic, economic, or military response.[104]

The fourth pillar was to "advance American influence"[105] through promoting an open and interoperable internet by leading efforts to establish cyber norms in the global network while promoting cyber security capacity among partner nations.[106] This aims to expand markets to which US can have more seamless electronic interactions, continue to reinforce America's lead in establishment of international norms, and heighten their diplomatic and trading partners ability to defend against cyber-attacks and espionage.[107]

US DHS Cybersecurity Strategy

The Department of Homeland Security was created in response to the September 11 terrorist attacks against the US.[108] From its inception, the mandate for the DHS has evolved, but today they have "six overarching missions that make up [their] strategic plan,"[109] including: counter terrorism and homeland security threats, US borders and approaches, cyber space and critical infrastructure, economic security, preparedness and

---

[99] Ibid, 8-11.
[100] Ibid, 14
[101] Ibid, 14-17
[102] Ibid, 20
[103] Ibid, 20-21.
[104] Ibid, 21.
[105] Ibid, 24.
[106] Ibid, 24-27.
[107] Ibid, 24-27.
[108] "Mission." U.S. Department of Homeland Security. Last modified February 26, 2023. https://www.dhs.gov/mission.
[109] "Mission." U.S. Department of Homeland Security. Last modified February 26, 2023. https://www.dhs.gov/mission.

resilience, and the DHS workforce.[110] In line with their mandate, the Department of Homeland Security released their "Cybersecurity Strategy" on 15 May 2018.[111]

The strategy outlines the department's aim to improve the cyber security and resiliency for government networks and critical infrastructures and better manage the national cyber security risks. It outlined five pillars of risk identification, vulnerability reduction, threat reduction, consequence mitigation, and enabling cybersecurity outcomes.[112]

US Threat Assessment 2023

On 6 February 2023, the Office of the Director of National Intelligence released their Annual Threat Assessment of the US Intelligence Community,[113] which strives to inform the reader on the current and anticipated security challenges facing the US from its geopolitical environment and transnational challenges. In particular, the report focuses on the "great powers, rising regional powers, as well as an evolving array of non-state actors" competing for ascendency in the world order. Secondly, it projects strategic challenges arising from the intermingling of "shared global challenges"[114] consisting of climate change, human security, health security, economic issues, energy uncertainty, and food insecurity.[115]

These challenges are also confronting the US while the backdrop of competition and threat from China persists. The assessment points out China as the top threat to "US technological competitiveness"[116] with China increasing their efforts to grow their domestic research and development while targeting key American sectors.[117] To effect this ambition, China is utilizing espionage and cyber theft in conjunction with their diplomatic and economic efforts.[118] In fact, "China probably currently represents the broadest, most active, and persistent cyber espionage threat to US government and private sector networks."[119]

In the event of a major conflict between China and the US, the assessment theorizes that China would undertake significant cyber operations against American networks on a global scale, attacking both military and critical infrastructure.[120] These

---

[110] "Mission." U.S. Department of Homeland Security. Last modified February 26, 2023. https://www.dhs.gov/mission.
[111] Department of Homeland Security. U.S. Department of Homeland Security. Cybersecurity Strategy. May 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
[112] Department of Homeland Security. U.S. Department of Homeland Security. Cybersecurity Strategy. May 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf. p 3
[113] Office of the DNI, Annual Threat Assessment of the US Intelligence Community, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
[114] Ibid, 4.
[115] Ibid, 4.
[116] Ibid, 8.
[117] Ibid, 8.
[118] Ibid, 9.
[119] Ibid, 10.
[120] Ibid, 10.

cyber attacks will be reinforced through their cyber influence activities to sow doubts against American government while concurrently boosting the support towards China's strategic goals within their political, economic, and security aims.[121] To affect this, China is moving closer to the Russian model of conducting influence activities within the cyber domain by using online personas to target US public to exploit divisive American domestic issues while softening the image of the CCP.[122] This is not limited to the general public. Worryingly, the assessment states that China is bolstering their influence activities towards state and local levels as they believe that "local officials are more pliable than their federal counterparts."[123]

In addition to China, Russia was highlighted as a threat to US security.[124] Similar to China, Russia is able to leverage their diplomatic, economic, and military machinations in order to promote their national interests while resisting the perceived American goal to weaken them by using Ukraine as a proxy.[125] Although Russia may look to leverage a whole of government approach, their military invasion and the subsequent price being paid in soldiers' lives, military equipment, and limited diplomatic options could see Russia relying more and more on their "nuclear, cyber, and space capabilities" to cover those gaps.[126] These capabilities would also assist Russia in continuing their effective foreign influence operations against the US by levering their large array of proxies, troll farms, sympathetic individuals and organizations.[127] Through these vectors, Russia is able to continue spreading false contents and amplify conspiracy theories in order to prevent US to reach consensus thereby delaying their response while furthering Russian strategic interests.

Along with China and Russia, developments in technology are accelerating potential threats from state and state-sponsored actors.[128] In conjunction with AI and large-scale data analysis, cyber-attacks are becoming more effective at exploiting American networks.[129] Further amplified by cutting edge technology which is commercially available, development of threats against US military and their societal cyber networks represents a threat risk which must be carefully mitigated and managed.[130]

In addition to threats emanating from state actors, non-state actors are also identified as a danger to US security. Transnational criminal organizations (TCOs)[131] were specifically highlighted as antagonists to keep aware of. Their ability within the cyber domain create chaos should not be underestimated. On top of the more traditional

---

[121] Ibid, 10.
[122] Ibid, 10.
[123] Ibid, 10.
[124] Ibid, 12.
[125] Ibid, 12.
[126] Ibid, 14.
[127] Ibid, 15.
[128] Ibid, 26.
[129] Ibid, 26.
[130] Ibid, 26-27.
[131] Ibid, 30.

illicit actions of human trafficking, drug distribution, and financial crimes, cyber activities have both enhanced their existing operations while creating new opportunities.[132] Cybercrime organizations and entities have used various cyber tools to expand their business ventures to ransomware, malware, coercive actions through hacked materials, and release of sensitive information.[133]

The Annual Threat Assessment of the US Intelligence Community for 2023 provided a comprehensive overview of the threats facing the US in the contemporary geopolitical environment. The assessment highlighted key challenges represented by Russia, China, and non-state actors, such as TCOs. Understanding these threats and what it represents within the cyber domain is crucial for both US and Canadian decision makers to ensure our organizations are equipped with the appropriate policies and have the necessary tools to safeguard our networks.

National Cybersecurity Strategy 2023

In March of 2023, President Biden's Whitehouse released the updated National Cyber Strategy.[134] Prior to the release of the strategy, the Biden administration invested $65 billion to increase the broadband penetration of high-speed internet in the US.[135] As mentioned before, high-speed internet penetration is a double-edged sword. It brings more connectivity and access to information and services to more people, while increasing the vulnerabilities to cyber threats. As such, the updated cyber strategy was designed to shift "the advantage to its defenders and perpetually"[136] frustrate the bad actors who attempt to attack it. In line with the threat assessment of the same year, it highlights specifically the malicious state actors of China, Russia, Iran, and North Korea as threats to the networks of the US and its allies. To emerge from the contemporary environment in a better state, the strategy outlines steps to "rebalance the responsibility to defend cyberspace"[137] and "realign incentives to [favour] long-term investments."[138] Thematically, it builds upon the 2018 National Cyber Strategy of the Trump administration, including the collaborative nature of cyber security within digital ecosystem.[139] The strategy outlines its comprehensive approach to ensure American cyber security through five pillars.

The first pillar revolves around defending the critical infrastructure of the US.[140] It focuses on ensuring the systems and networks surrounding key American services are safeguarded in a way that they are resilient and the public has faith in its ability to defend

---

[132] Ibid, 30-31.
[133] Ibid, 31.
[134] Whitehouse. National Cyber Strategy. March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[135] Ibid.
[136] Ibid, 1.
[137] Ibid, 4.
[138] Ibid, 5.
[139] Ibid, 6.
[140] Ibid, 7.

itself against threats.[141] It acknowledges the importance of the private sector in the overall cyber security of the US and looks to integrate efforts of corporations with the "State, local, Tribal, and territorial (SLTT) partners."[142] For the government's part, it looks to the longer term work to implement a zero trust architecture strategy while updating its ICT infrastructure to enable it.[143]

The second pillar looks to "disrupt and dismantle threat actors"[144] by leveraging a whole of government approach, including diplomatic, information, military, cyber, financial, and other powers available to the federal government.[145] This pillar also outlines ways for the federal government to work together with non-federal entities to respond against malicious state and non-state cyber actors.[146] It recognizes the greater need to cooperate between the private and public actors through information sharing, coordinated execution of cyber response, and improving the cyber security capabilities.[147]

The third pillar outlines steps to "shape market forces to drive security and resilience."[148] It aims to shift the responsibility and consequences of poor cyber security aware from the vulnerable individuals and smaller organizations towards a more equitable structure where the federal government will work with industry to "shape the long-term security and resilience of the digital ecosystem."[149] This way, the strategy is attempting to move the liability for software and services away from those who do not have the resources to properly defend themselves.[150]

The fourth pillar looks to "invest in a resilient future"[151] with the goal of remaining as the forefront nation in development of technology related to cyber and cyber security. This would allow the US to have more influence and ways to reduce the vulnerabilities at the foundational level of the internet architecture.[152] The idea behind this pillar seems to originate from the constant threats and attacks against American

---

[141] Ibid, 7.
[142] Ibid, 7.
[143] Ibid, 7.
[144] Ibid, 14.
[145] Ibid, 14.
[146] Ibid, 14.
[147] Ibid, 14.
[148] Ibid, 19.
[149] Ibid, 19.
[150] White House. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House. Last modified March 02, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/?utm_source=link.
[151] Whitehouse. National Cyber Strategy. March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, p 23
[152] White House. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House. Last modified March 02, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/?utm_source=link.

networks and incidents of cyber theft over the past decades.[153] This pillar doesn't just look at investments to improve the research and development of technology. It also aims to grow and expand the available workforce who are trained to take up the "hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide"[154] in the US.

The final and fifth pillar summarizes the need for the US to "forge international partnerships to pursue shared goals"[155] The goal for this effort seems to be not only expand the coalition of willing allies to tackle transnational cyber security issues, but to also establish and reinforce international norms on what is and what is not tolerated within the cyber space as part of the MDO. In order to effect this change, the US seeks to strengthen the cyber capacity of its partner nations in order to further reduce the vulnerabilities in the global network.[156]

In summary, the National Cybersecurity Strategy (2023) of the US draws out the key considerations and steps to synchronize the direction of cyber security in the short, medium, and long term. The document recognizes the importance of cyber security in light of the new digital society which the world faces itself in. While it builds upon many of the foundations of the previous National Cybersecurity Strategy of 2018, the updated 2023 version places a much heavier emphasis on the coordination and partnerships that will be required to counter the global threats posed by malicious state and non-state actors. Furthermore, it outlines logical actions that the US must take to respond to the 2023 threat assessment.

US Cyber Organizations and Structure

Cyber security is taking a more prominent role in the American national policy and strategy, as discussed in the previous section. In the US, there are numerous organizations, departments, and agencies who are responsible for different aspects of the national cyber security infrastructure. In particular, the Department of Homeland Security and the Department of Defense play a crucial role within the cyber domain for the US.

The Department of Homeland Security (DHS)

The DHS was created in the aftermaths of the September 11th terrorist attacks in 2001 through the "Homeland Security Act" in 2002.[157] The benefit touted in creating this new department was to amalgamate a "patchwork of government activities and agencies" involved in various aspect of securing the US into one department.[158] Although it is the newest department within the US government, it is now the third largest department with

---

[153] Whitehouse. National Cyber Strategy. March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, p 23
[154] Ibid, 27.
[155] Ibid, 29.
[156] Ibid, 31.
[157] Slyke, Jeffrey Van, Joseph Skinner, Barbara Russo, Greg Etter, Michael Corey, Robert Nations, Carl J. Jensen III, David H. McElreath, Daniel Adrian Doss, and Jr Michael Wigginton. Introduction to Homeland Security CRC Press, 2021. p96
[158] Ibid, 96.

over 229,000 employees covering a wide range of components, including customs and border, immigration, transportation security administration, US coast guard, and more. Under the DHS, the Cybersecurity and Infrastructure Security Agency (CISA) plays an important role within the US cyber security network.

CISA. In 2018, CISA replaced the previous National Protection and Programs Directorate (NPPD), a directorate which no longer exists but was mandated to improve the security and resiliency of the American critical infrastructure.[159] Since then, CISA has been afforded much more responsibility within the cyber defence system of the US. They work with all levels of US government and the private sector in order to assist them in improving their own cyber security networks and practices.[160] To fulfill its mission to "lead the national effort to understand, manage, and reduce risk to [US] cyber and physical infrastructure,"[161] CISA acts as the operational lead for matters of cyber security which affects the US critical infrastructure. Within its short history, CISA has been granted more resources and responsibilities, including in the 2020 National Defense Authorization Act (NDAA).[162] The NDAA provided authority for CISA to "issue subpoenas to internet service providers compelling them to release information on cyber vulnerabilities detected on the networks of critical infrastructure organization."[163] This provided the government agency with the legal tools to ensure that they are able to investigate potential vulnerabilities affecting the critical infrastructure, thus able to disseminate the proper security measures to the rest of the community.

Subsequent NDAAs in 2021,[164] 2022,[165] and 2023[166] continued to further reinforce the cyber capabilities within the DHS, including the CISA, through more funding. There is more focus on interdepartmental cooperation at the federal level, coordination with SLTT, and shared knowledge with the private sector. The NDAA for 2023 specifically stated that "the need for government and private sector stakeholders to be able to share and consume cybersecurity-related information on a single platform, or at least achieve interoperability… remains as urgent as ever."[167] It further highlights the

---

[159] Ropek, Lucas. "Will CISA Be the Savior of State and Local Cybersecurity?" Government Technology, July 24, 2020. https://www.govtech.com/security/will-cisa-be-the-savior-of-state-and-local-cybersecurity.html

[160] Ibid.

[161] "About CISA." Cybersecurity & Infrastructure Security Agency. Accessed April 22, 2023. https://www.cisa.gov/about-cisa.

[162] Ropek, Lucas. "Will CISA Be the Savior of State and Local Cybersecurity?" Government Technology, July 24, 2020. https://www.govtech.com/security/will-cisa-be-the-savior-of-state-and-local-cybersecurity.html

[163] Ibid.

[164] "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R.6395, 116th Congress (2019-2020)."

[165] "National Defense Authorization Act for Fiscal Year 2022, S.1605, 117th Congress (2021-2022)."

[166] "National Defense Authorization Act for Fiscal Year 2023, H.R.7900, 117th Congress (2021-2022)." Congress.gov. https://www.congress.gov/bill/117th-congress/house-bill/7900

[167] Krishan, Nihal. "NDAA requires intelligence agencies to study creation of cyber collaboration program." FedScoop, December 8, 2022. https://www.fedscoop.com/ndaa-requires-intelligence-agencies-study-creation-cyber-collaboration-program/

importance that the US government is placing on ensuring that the private sector is aware of the cyber threats that exists[168] as they represent a critical vector for malicious actors attempting to attack the US. As mentioned in the section on adversarial threat, state and non-state actors targeting US interests are not solely focused on the American defence and military networks, but rather see the entire digital society as the target to degrade US strategy interests and influence.

JCDC. To assist in realizing the goal of a collaborative environment for the public and private sector to strengthen the mutual cyber defence, the Joint Cyber Defense Collaborative (JCDC) was created. The establishment of the JCDC was resultant from the 2021 NDAA to create a "public-private cybersecurity collaborative… in the collective defense of cyberspace." JCDC's core functions involve developing plans for cyber defense and assisting with their execution, promoting cyber security cooperation and the integration of information between the public and private sectors, and creating guidelines for cyber security for all stakeholders involved.[169] This collaborative nature towards cyber security has enabled the JCDC to find success not only from an economical point of view, but it has helped the US in being able to extent their influence abroad. For example, the JCDC was able to coordinate the response when an intrusion was detected within Albania's Computer Emergency Response Team's network.[170] By working with the private sector companies, JCDC was able to analyze the intrusion, share the data with Albania and private industry, and conduct remediation measures to remove sensitive contents posted by the intruders on social media.[171] Examples such as this not only help strengthen American government and corporate cyber defenses by learning from others, but it also builds credibility among international partners as a reliable source of assistance within the cyber domain. Furthermore, if these actions can be attributed to adversarial nations or to entities who may be linked to them, it can provide geopolitical advantages in being able to influence the countries that are affected by these attacks and intrusions.

Department of Defense (DoD)

With the overwhelming reliance on computer and information technology for military operations and communications, the DoD has invested heavily into their cyber security capability.[172] As such, the DoD, along with the DHS and the Department of Justice (DoJ) is considered one of three major departments who play critical roles within the overall cyber security operations of the US.[173] Although cyber security is layered throughout the department, DoD has three subordinate organizations that play a crucial role in US cyber policy. Reporting to the Under Secretary of Defense for Intelligence, the

---

[168] Ibid.
[169] "Cybersecurity & Infrastructure Security Agency. 'Joint Cyber Defense Collaborative.' Accessed April 22, 2023. https://www.cisa.gov/jcdc"
[170] Ibid.
[171] CISA. "JCDC Success Stories." Accessed April 22, 2023. https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories.
[172] Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017. p84
[173] Ibid, p84.

Defense Information Systems Agency (DISA) and the National Security Agency (NSA) are key agencies for cyber security and defence operations for the DoD. The NSA is also part of the US Intelligence Community (IC) and has a direct line to the Director of National Intelligence (DNI) as the DNI has the authority to establish goals and priorities for intelligence gathering and analysis for US IC member agencies.[174] Under the unified combatant commands within the DoD, US Cyber Command (USCYBERCOM) was formed in 2010 as a sub unified command under the US Strategic Command (USSTRATCOM) in order to defend DoD networks, defend US interests at home and abroad from cyber threats, and provide cyber support in execution of operations and in the planning process.[175] Since then, USCYBERCOM has been elevated to the status of a Unified Combatant Command, led by a four star general, General Paul Nakasone.[176] The commander of USCYBERCOM has a dual role as the director of the NSA; therefore, both the USCYBERCOM and NSA are headquartered at Fort George G. Meade in Maryland.

National Security Agency (NSA). The NSA is considered to be the "premier US intelligence agency operating in the cyber domain."[177] Like the DISA, the NSA is a combat support agency within the DoD and supports military operations through their signals intelligence (SIGINT) and cyber security skills.[178] NSA was originally founded in 1949 as the Armed Forces Security Agency (AFSA).[179] AFSA consolidated the code breakers and assets in the US under a single entity but in 1952, it was changed to the current name of National Security Agency.[180] As the agency responsible to leverage cryptology for the DoD, the NSA demonstrated forward thinking in its relationship with computers.[181] "While many government agencies adopted a wait-and-see approach to computers, the NSA set aside increasing portions of its budget for the purchase and improvement of computers."[182] Since NSA revealed its competence in computing and cryptology throughout its formative years, the NSA was naturally assumed to be the agency responsible for providing security within the new domain.[183] The growth of computer systems in every facet of government and public society significantly increased the complexity of the NSA's mission to provide "SIGNIT insights and cybersecurity

---

[174] Presidential Document. 'Further Amendments to Executive Order 12333, United States Intelligence Activities.' Federal Register, August 4, 2008. https://www.federalregister.gov/documents/2008/08/04/E8-17940/further-amendments-to-executive-order-12333-united-states-intelligence-activities
[175] Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017. p305
[176] U.S. Cyber Command. 'Our History.' Accessed April 22, 2023. https://www.cybercom.mil/About/Our-History/
[177] Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017. P195
[178] National Security Agency/Central Security Service. 'Mission & Combat Support.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/about/mission-combat-support/
[179] Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017. P195
[180] Ibid, 196.
[181] Ibid, 196.
[182] Ibid, 196.
[183] Ibid, 197.

products and services" and enable the "computer network operations to gain a decisive advantage for the [US] and [their] allies."[184]

The ways that the NSA carries out its activities to fulfill its mission has been controversial. In 2010, General Alexander, then the director of the NSA and commander of the newly created USCYBERCOM, recommended that the NSA conduct offensive cyber activities as a response when US was targeted by malicious actors.[185] Previously, the NSA was also caught in a public scandal when it was revealed that the agency was collecting and shifting through massive amounts of the public's data via US telecommunications networks in its 'War on Terror.'[186] In response to the outrage from the American public on the violations to their privacy, the US promised to stop the programs implicated in the leak;[187] however, a NSA contractor named Edward Snowden released considerable amount of NSA documents to journalists revealing that the NSA's activities and capabilities had only increased since then.[188] Although President Obama took steps to build in more safeguards against the NSA from conducting actions that the US public would not accept, the NSA "remains the foremost offensive cyber-operations organization."[189]

Cybersecurity Collaboration Center (CCC). The CCC was the created in 2020 in order to develop and foster partnerships between the NSA and the private sector.[190] It's mission includes protecting the National Security Systems, the DoD, and the Defense Industrial Base (DIB) from malicious cyber actors.[191] While still under the NSA and therefore the DoD, the CCC is designed to feel more open and transparent in order to better integrate with private industry partners.[192] It further emphasizes the vital nature of close cooperation between the government and industry. As noted by the NSA's Cybersecurity Director, "It doesn't do anybody any good if we know a thing and don't do something."[193]

---

[184] National Security Agency/Central Security Service. 'Mission & Combat Support.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/about/mission-combat-support/

[185] Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017. P198

[186] Ibid, 198.

[187] Ibid, 198.

[188] Ibid 198.

[189] Ibid, 199.

[190] National Security Agency/Central Security Service. 'NSA Cybersecurity Collaboration Center.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/what-we-do/cybersecurity/cybersecurity-collaboration-center/

[191] National Security Agency/Central Security Service. 'NSA Cybersecurity Collaboration Center.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/what-we-do/cybersecurity/cybersecurity-collaboration-center/

[192] Smalley, Suzanne. "'No guns, no guards, no gates.' NSA opens up to outsiders in fight for cybersecurity." CyberScoop, November 16, 2022. https://www.cyberscoop.com/nsa-cybersecurity-collaboration-center-morgan-adamski/

[193] Ibid.

DISA. The DISA is a relatively small combat support agency of 7,000 military and civilian employees within DoD.[194] DISA is responsible to "provide, operate and assure command, control, information-sharing capabilities"[195] as well as directly support "joint warfighters, national-level leaders, and other mission and coalition partners" across the full spectrum of operations.[196]

"China initiated the De-IOE program the same year, which aimed to uninstall software made by American suppliers, including IBM, Oracle, and EMC, from its e-commerce companies and banks."[197]

United Kingdom

The United Kingdom of Great Britain and Northern Ireland (UK) provides a great blueprint for Canada regarding cyber security. It is routinely ranked second in the world after the US on global cyber security index due to its strong centralized government guidance and interface with the private sector. As the only member of the Five-Eyes intelligence partnership located in Europe, the UK provides a vital foothold for the alliance. Through its National Cybersecurity Strategy (NCSS) which is reviewed every five years, the government can play a central role and work together with industries to identify vulnerabilities and patch them to limit its vulnerabilities. But the UK also provides a case study on the balance between effective cyber security and the right to individual privacy. Although UK has strong cyber security policies actioned by capable government organizations, it has come under criticism from privacy advocates due to legislations such as the IPA, which critics have decried as gross violations of individual rights. This is a dynamic which must be carefully maintained as erosion of public trust in government leaves the country more susceptible to foreign influence activities, degrades support to legislative changes which may be required, and creates fractures in the whole-of-society approach to cyber security.

Cabinet Office responsible for developing cybersecurity policy and implementing National Cyber Security Program (NCSP) through Cyber and Government Security Directorate (CGSD). NCSC as primary public-private interface and advise on future proofing through advice outside of government.

[incidents of cyber-attacks, detection]

Australia

Like the UK, Australia provides as a valuable foil for Canada regarding their respective cyber security policies and organizations. As another Five-Eyes partner in the

---

[194] Defense Information Systems Agency. 'About Our Work.' Accessed April 22, 2023. https://www.disa.mil/About/Our-Work
[195] Ibid.
[196] Ibid.
[197] Jinghua, Lyu and Gaurav Kalwani. "Navigating the US-China Competition in Cyberspace." Turkish Policy Quarterly 19, no. 2 (2020): 135-144. 136

Indo-Pacific, Australia can act as a senor for adversarial states in the region, namely China. Although the cyber domain is not restrained by geography, its role in shaping and enabling other geopolitical objects is evident; therefore, Australia faces a tangible threat. This is highlighted by the release of Australia's Cyber Security Strategy in 2020 (2020 CSS). The strategy built on the 2009 Cyber Security Strategy (2009 CSS) and provided a more contemporary scan of the threat environment. It echoed many of the other cyber strategies of Canada's allies, including a focus on the relationships among the government, businesses, and the community.

After the release of the 2020 CSS, the Australian government recognized that the "patchwork of policies, laws and frameworks" are not able to maintain pace with the evolving digital landscape. In effect, reactive policies and legislations as novel threats emerge was not conducive to a holistic, centralized cyber strategy.

CANADA

Canada, much like the rest of the modern world, relies heavily on ICT to run many of its critical infrastructure and services. As such, Canada is not immune to cyber-attacks from state and state sponsored actors, malicious non-state actors, and cybercriminal organizations. The targets of these attacks are all levels of government, corporations, and private entities and individuals. Successful attacks on these networks can result in large amounts of money, proprietary data, and personal information being exploited or lost. This is why it is not a surprise that "75 per cent of Canadians expressed their concerns about cyberattacks."[198]

To address the cyber threats to government, military, and society at large, Canada has both external and internal cyber security mechanisms. As a member of the 5-Eyes intelligence group, Canada can give and receive intelligence, including in the cyber domain, from its allies. This greatly aids Canada as they can not only learn from the experiences of its allies, but also to cross pollinate in proactive areas for ideas, skills, and technologies. With respect to internal mechanisms, Canada can create strategies and develop policies for cyber activities, including in areas of cyber defence. In addition, there exists nine Government of Canada organizations[199] that are involved in Canada's cyber activity who can execute the national strategies.

Canadian Policies

Successive Canadian governments have taken the issue of cyber security seriously. Since the early inception of computerization of government information and services, strategies and policies have been formulated and published to provide direction to the government organizations. The three strategic directions for cyber security for

---

[198] Routledge Companion to Global Cyber-Security Strategy, edited by Scott N. Romaniuk, and Mary Manjikian, Taylor & Francis Group, 2020. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=6415984.
Created from cfvlibrary-ebooks on 2023-05-04 00:15:56. p454
[199] Ibid, 454.

Canada came through "the 2004 National Security Policy, the 2010 Cyber Security Strategy and the 2019 National Cyber Security Strategy."[200] Through these strategies, how the government and Canadian industries functioned with respect to cyber security evolved, mainly with the establishment of Shared Services of Canada (SSC) in 2011 and the Canadian Centre for Cyber Security (CCCS) in 2018.[201] On top of organizational changes, investments into cyber security topped over $6 billion,[202] demonstrating the importance placed on protecting Canadian networks and institutions from attacks.

2004 National Security Policy. The Liberal government under Prime Minister Paul Martin released the National Security Policy in 2004 (2004 NSP) to address the important security issues facing Canada at that time.[203] In a "first ever policy of its kind in Canada,"[204] the 2004 NSP focused on protecting Canada and its citizen, preventing the Canada from becoming a home base for threats to its allies such as the US, and contributing to the establishment and maintenance of world order.[205] The strategic framework of 2004 NSP was very much a creation in the security environment of the post 9/11 terrorist attacks in North America. It is in this cultural milieu that the 2004 NSP focused chapters on areas of intelligence, transportation security, border security, and increasing security cooperation with the US;[206] however, the document also highlighted the need to expand the capability of Canada to protect its networks against cyber-attacks.[207] Using an example of the threat climate of its time, the 2004 NSP provided the case study of the August 2003 electrical blackout in Ontario and Eastern US to show the vulnerabilities of the critical infrastructure in Canada. [208]

To address the threat posed by malicious actors in the cyber domain, the 2004 NSP clarified the requirement for increasing cyber security in all federal government systems and networks. Recognizing that cyber security is "at the forefront of the transborder challenge to Canada's critical infrastructure,"[209] Canada pledged to develop a national cyber security strategy to decrease the number of successful attacks against its networks and lower their severity and impact.[210]

2010 Canada's Cyber Security Strategy. Highlighting the penetration of the internet in Canadian households in conjunction with the ever-expanding use of online services, the government released the Canada's Cyber Security Strategy in 2010 (2010

---

[200] National Security and Intelligence Committee of Parliamentarians. "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack." https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf. p4
[201] Ibid, 4.
[202] Ibid, 4.
[203] Canada. Securing an Open Society: Canada's National Security Policy. Privy Council Office. Her Majesty the Queen in Right of Canada, 2004. vii
[204] Ibid.
[205] Ibid.
[206] Ibid.
[207] Ibid, 21.
[208] Ibid, 7.
[209] Ibid, 26.
[210] Ibid, 26.

CCSS).[211] Acknowledging that the strategy, along with the creation of the Canadian Cyber Incident Response Centre under the portfolio of Public Safety Canada, was "but one element in a series of initiatives designed to protect Canadians,"[212] The document describes the threat environment within the cyber domain originating from state-sponsored actors and non-state entities, such as terrorists and cyber criminals.[213] To counter these emerging threats and lay the groundwork for cyber security strategy in Canada, the 2010 CCSS delves into three pillars.

The first pillar looks to secure Government of Canada's systems in order to ensure that the backbone of the national cyber security and infrastructure can be protected from threats and vulnerabilities. The second pillar aims to create partnerships with other cyber stakeholders, including provincial government and the private sector.[214] The final pillar outlines ways to help Canadians to be secure in the cyber space through proactive actions in order to prevent harm and providing more tools to law enforcement in order to pursue justice in the aftermath.[215] Overall, the strategy recognizes that cyber security "is a shared responsibility, one in which Canadians, their governments, the private sector and … international partners all have a role to play."[216] Akin to a whole-of-government approach to tackling concerns of national importance, the strategy alludes to a whole-of-society approach that may be needed in addressing the cyber threats to Canadian networks.

2018 National Cyber Security Strategy. The 2018 National Cyber Security Strategy (2018 NCSS) represented another leap forward in the development of Canada's cyber security.[217] Although longer does not necessarily mean better, the 2018 NCSS as published was 40 pages, compared to 17 pages in the 2010 CCSS. It perhaps illustrates the growing awareness of the threats that exists within the cyber domain. The 2018 NCSS focuses the context for the strategy on predominately blockchain technology and protecting Canadian networks from malicious actors that are intent on cybercrime activities. Somewhat perplexingly, the document does not spend much time discussing state and state-sponsored actors as threats to Canadian cyber space. Even the stated goal of the cyber security strategy is to "work with its international partners to advance Canadian interest… [including] advocating for an open, free, and secure internet and enhancing our international cooperation to combat cybercrime."[218] The focus on cybercrime instead of state actors in the 2018 NCSS seems to be a deliberate decision. During the review process for the strategy, the number one cyber security related issue that came up during the public consultations was the "increasing number of incidents that

---

[211] Canada. Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada. Her Majesty the Queen in Right of Canada, 2010. 2
[212] Ibid, 3
[213] Ibid, 5.
[214] Ibid, 7.
[215] Ibid, 7.
[216] Ibid, 14.
[217] Canada. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. Her Majesty the Queen in Right of Canada, 2018.
[218] Ibid, 32.

are causing harm to the economy and society, ranging from breaches, crimes, disruption of essential services, and destruction of corporate and country assets."[219]

To achieve the stated goal, the 2018 NCSS uses the 2010 CCSS as the "basis for future action,"[220] by expanding upon the three pillars; however, the 2018 NCSS looks at three themes to realize its intent. The first theme involves the security and resilience among all Canadian systems: the government networks, private industry's systems, and individual Canadians. Secondly, the 2018 NCSS outlines theme of fostering domestic innovation within the cyber space.[221] In addition to the obvious benefit to the cyber security infrastructure with improvements in research and technology, it also provides an advantage of expanding Canada's share of the global cyber security market.[222] Lastly, the third theme revolves around the leadership demanded of the federal government in coordinating cyber actions as well as the collaboration required to protect across the wide spectrum of Canadian systems and networks.[223] This need to streamline cyber advice and provide a robust cyber incident response[224] let to the creation of the Canadian Centre for Cyber Security (CCCS) under the Canadian Security Establishment (CSE) in 2018. The mandate for CCCS includes defending Government of Canada's networks, providing guidance and assistance to other Canadian stakeholders and entities, and educating the Canadian public on way to keep their information and computers safe.[225] In addition to educating the public, the CCCS produces the National Cyber Threat Assessment which outlines the "current cyber security trends, and how they are likely to evolve."[226]

2023-2024 National Cyber Threat Assessment.

In 2022, the CCCS released their National Cyber Threat Assessment for 2023 to 2024 (NCTA).[227] The 2023/2024 NCTA reiterated many of the threats from its previous versions, released in 2018 and 2020, respectively.[228] The comments from the Minister of National Defence and the head of the CCCS both painted an inauspicious security landscape where Canadians are faced with cyber threats from state-sponsored entities and cyber criminals.[229] As part of the NCTA, the CCCS focused on five key threat vectors for Canada in the near future: ransomware, vulnerabilities in critical infrastructure, malicious state-sponsored activities, cyber influence activities, and disruptive technologies.

---

[219] Ibid, 16.
[220] Ibid, 2.
[221] Ibid, 19.
[222] Ibid, 19.
[223] Ibid, 26.
[224] Ibid, 31.
[225] CSE. "Cyber Security." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/mission/cyber-security
[226] Canadian Centre for Cyber Security. National Cyber Threat Assessment: 2023-2024. Communications Security Establishment. Ottawa, ON. P ii
[227] Canadian Centre for Cyber Security. National Cyber Threat Assessment: 2023-2024. Communications Security Establishment. Ottawa, ON, 2022.
[228] Ibid, p iii.
[229] Ibid, p ii-iii.

CSE's Legislative History

Akin to the British experience during the Second World War, Canada found success and great value in having developed its signals intelligence (SIGINT) and communications security (COMSEC). Recognizing these hard-earned skills and capability should be retained, Canada created the Communications Branch of the National Research Council (CBNRC) in 1946 as its national cryptologic agency.[230] Since its inception, the CBNRC carried out key intelligence activities in support of national interests and provide an "autonomous SIGINT capabilities"[231] for Canada. Maria Robson argues that this national SIGNIT capability that CBNRC provided had three key benefits for Canada: "directly bolstering Canadian national security" through its organic capability, indirectly through receiving partner nations' intelligence products, and finally demonstrating enough value to be included in the post-war intelligence alliances, which became the Five-Eyes partnership.[232]

Among the important work being done by CBNRC was the intelligence sharing within the Five-Eyes partnerships;[233] however, the existence of the CBNRC and its role within the Canadian security establishment was not known to the general public. In 1974, the Canadian Broadcasting Corporation aired a program on the American foreign surveillance program in which CBNRC was mentioned for the first time to the Canadian public. The scope and magnitude of Canada's SIGINT program and the CBNRC's role within the Five-Eyes community caused a stir in the media, leading to the "first ever acknowledgement of the existence of the CBNRC in Canada's Parliament" that year.[234] In 1975, the CBNRC was renamed to the Communications Security Establishment (CSE) and placed under the Department of National Defence (DND).[235] It was not until 2011 when the CSE became its own standalone agency as the National Defence Act (NDA) was too restrictive for the evolving mandate of the CSE.[236] Although CSE gained more latitude in executing its tasks, it still fell under the portfolio of the Minister of National Defence.[237] In addition, CSE was placed under the oversight of the intelligence commissioner, the National Security and Intelligence Review Agency (NSIRA),[238] and

---

[230] CSE. "Our Story." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story

[231] Robson, Maria A. "The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing." Intelligence and National Security 35, no. 7 (2020): 954-969.

[232] Maria Robson. "The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing." Intelligence and National Security 35, no. 7 (2020): 954-969.

[233] CSE. "Our Story." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story.

[234] Ibid.

[235] Ibid.

[236] Ibid.

[237] Ibid.

[238] Prior to the creation of the NSIRA in 2011, the Office of the CSE Commissioner provided the oversight of CSE's activities.

the National Security and Intelligence Committee of Parliamentarians (NSICOP) in order to ensure that CSE's activities complied with its legal mandate and responsibilities.[239]

In addition to the becoming a standalone agency in 2011, the CSE received two major legislative changes since its inception in 1975. In 2001, shortly after the September 11 terrorist attacks, Canada passed the Anti-Terrorism Act (ATA) which received Royal Assent on 18 December 2001.[240] The ATA made changes to Canadian laws regarding national security, including the NDA, the CSIS Act, Criminal Code, and Official Secrets Act.[241] Crucially for the CSE, these changes equipped the agency with a broader scope to pursue its mandates.[242]

The CSE Act. The second major legislative change for CSE was in 2019 with the passing of the CSE Act.[243] The Act articulated the CSE's role as the national SIGINT agency for foreign intelligence as well as the "technical authority for cybersecurity and information assurance."[244] The Act also listed the five aspects of the CSE's mandate: "foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance."[245] Although the recording keeping requirements seem onerous, the potential latitude that the Act affords the CSE is extensive, especially on the aspects of cyber operations authorizations.[246]

ANALYSIS OF CANADIAN CYBER DEFENCE

To analyze the current state of Canada's cyber security, a sample of adversarial entities, both state and non-state sponsored, were analyzed. Through this examination, key deductions regarding how they could affect Canada was recorded. Russia's example pointed to potential pitfalls of having multiple agencies overlapping their mandate within the cyber domain. This not only creates room for friction within the government but can lead to unhealthy dynamic where political favouritism and internal politics can play a factor in allocation of resources. This is in contrast to where resources should be apportioned based on capability. Russia's tactic in its invasion of Ukraine also

---

[239] CSE. "Oversight and review." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/accountability/oversight#OAM

[240] CSE. "Our Story." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story.

[241] Ibid.

[242] Ibid.

[243] Canada. Communications Security Establishment Act, S.C. 2019, c. 13, s. 76. Current to April 20, 2023. Last amended on August 1, 2019. http://laws-lois.justice.gc.ca.

[244] Ibid, 7.

[245] Ibid, 7.

[246] Ibid, 13.

demonstrated the importance of the cyber domain within the MDO, especially in the areas of shaping, enabling and influence operations.

Examination of China's cyber policies showed a slightly different focus from Russia. China's concept of Digital Belt and Road Initiative provides a real threat to Canada and its allies as it has the potential to entrench Chinese technology and hardware throughout the world. In addition, the centralized control of the Chinese Communist Party in all aspects of security benefits their cyber operations, in both defensive and offensive terms, as they have a innate private-public interface.

In addition, study of the US, UK, and Australia provided examples of alternative approaches for Canada in its cyber security strategy. As world leaders, US and UK lays a foundational blueprint for how Canada can develop its strategies and organizations.

CONCLUSION

Cyber is not strictly a military or a civilian problem, but rather it is an issue of importance for the whole of society. A comprehensive and coordinated plan is required to establish the foundation of the national cyber security policy. This must start from the top with the federal government strengthening the existing intelligence sharing partnerships, such as the Five-Eyes, while looking to build a coalition of like-minded democratic states. As examined, information on new trends, vulnerabilities, and threats are a valuable resource within the cyber security sphere and information sharing can provide the vital warning or buffer to better protect Canadian networks. Furthermore, Canadian governments at all levels must closely cooperate with the private sector. Cyber threats are not isolated to distinctively military or civilian targets. For example, cyber-attacks on civilian critical infrastructures can potentially cause more damage to Canada's national security than attacks on military networks. The level of cooperation demands that the federal government take a stronger and more centralized role in the national cyber security. Decentralized sensors and solutions from international and domestic partners is important, but clear and concrete directions must be centralized.

There also needs to be a higher baseline of competency for cyber security for individuals, governmental organizations, and companies of all sizes. Although sophisticated cyber-attacks using zero-day exploits are still a grave threat, most successful cyber intrusions and attacks are still through individual vulnerabilities. Whether it is through social engineering, lack of cyber hygiene, or shortage of access to cyber tools, individuals within an organization remain a key vector for malicious entities to target. Strengthening the individual's cyber resiliency will create a better foundation for which organization can operate; however, governments must also improve its own safety procedures. Providing more access to authentication applications, better education and training for all personnel involved in the entirety of the supply chain, and more centralized procurement of ICT would all increase the cyber security and resilience within the Government of Canada.

Canada must also look towards expanding its digital economy through innovation of Canadian entrepreneurs, promoting the export of Canadian ICT, and expanding the

domestic work force to fuel the growth. Though some may argue that Canada has an unassuming technological sector, recent history has demonstrated that Canadian companies can grow to compete on the international stage. Companies such as Blackberry and Shopify grew to astronomical market capitalizations and recognition. Government must support the "made in Canada" branding of Canadian innovations in technology, including within the cyber security industry. The threat posed by China's Digital BRI can degrade the West's influence in the world's cyber security domain and open more vectors for malicious actors to conduct cyber-attacks and influence activities. Furthermore, in order to sustain the growth within this sector, Canada must expand the available pool of cyber operators and analysts. These roles demand a unique skillset and represent a special example of where one extremely talented individual can have more strategic impact than a team of average operators. DND can be leveraged to provide a constant churn of cyber operators and specialists by offering prospective recruits with comprehensive training, guaranteed starting employment, and a unique access that only government cyber operators can legally enjoy. These military cyber operators can then move on to work in other governmental departments or in the private sector where they can be compensated beyond what the DND can offer. Akin to the American model, the CAF can provide a starting point for cyber operators instead of the traditional career path which may not be as attractive to the talent pool.

Furthermore, the cyber roles and responsibilities within the Government of Canada should be re-examined to potentially provide a greater role for DND and CAF members. Although the details of the ministerial authorizations for the CSE and DND are not available through open source, the legislative acts that govern their mandates do not seem to be developed with the holistic cyber security in mind. Instead of a patchwork approach where additional roles are added to existing organizations and capabilities, a holistic review should be conducted.

BIBLIOGRAPHY

ACSC Annual Cyber Threat Report, July 2021 to June 2022. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

ADM(RS). "Evaluation of the Cyber Forces." Last accessed 4 May 2023. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/eval-cyber-forces.html

Belli, Luca. "Cybersecurity Policies in China." *In Cyberbrics*, 183-226. Switzerland: Springer International Publishing AG, 2021.

Blackberry Cybersecurity. Global Threat Intelligence Report 2022. https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf

Canada. *Securing an Open Society: Canada's National Security Policy*. Privy Council Office. Her Majesty the Queen in Right of Canada, 2004. https://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

Canada. *Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada*. Her Majesty the Queen in Right of Canada, 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf

Canada. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. Her Majesty the Queen in Right of Canada, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Canada. *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76. Current to April 20, 2023. Last amended on August 1, 2019. http://laws-lois.justice.gc.ca.

Canada's Active Cyber Defence is Anything But Active. https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4768/attachments/original/1627507481/Canadas_Active_Cyber_Defence_is_Anything_But_Active.pdf?1627507481

Canada. *Canada's Indo-Pacific Strategy*. Global Affairs Canada. (Ottawa, ON: 2022).

Canada. Public Safety Canada. (2017). Horizontal Evaluation of Canada's Cyber Security Strategy: Final Report. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/vltn-cnd-scrt-strtg-en.pdf

Canadian Centre for Cyber Security. National Cyber Threat Assessment: 2023-2024. Communications Security Establishment. Ottawa, ON, 2022. https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

CBC. Global Affairs needs to get a grip on its most sensitive intelligence activities, committee says. https://www.cbc.ca/news/politics/global-affairs-intelligence-cyber-1.6641496

China Cyber Threat Overview and Advisories https://www.cisa.gov/uscert/china

China's cybersecurity regime https://www.tradecommissioner.gc.ca/china-chine/cyber-security_cyber-securite_china-chine.aspx?lang=eng

Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-258a

CISA. "JCDC Success Stories." Accessed April 22, 2023. https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories

CSE. "Cyber Security." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/mission/cyber-security

CSE. "Our Story." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/culture-and-community/history/our-story

CSE. "Oversight and review." Last accessed 4 May 2023. https://www.cse-cst.gc.ca/en/accountability/oversight#OAM

Cyber Centre Learning Hub, Discovering Cyber Security, Module 1.

Cyber Operations Tracker https://www.cfr.org/cyber-operations/

"Cybersecurity & Infrastructure Security Agency. 'Joint Cyber Defense Collaborative.' Accessed April 22, 2023. https://www.cisa.gov/jcdc"

Department of Homeland Security. *U.S. Department of Homeland Security. Cybersecurity Strategy*. May 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Department of Defense. Summary: Department of Defense Cyber Strategy 2018: U.S. Department of Defense, 2018.

https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Defense. DoD Cyber Workforce Strategy 2023-2027. https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

Department of Homeland Security. THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003. https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Defense Information Systems Agency. 'About Our Work.' Accessed April 22, 2023. https://www.disa.mil/About/Our-Work

Defense Information Systems Agency. 'Strategic Plan FY2022-2024.' Accessed April 23, 2023. https://www.disa.mil/About/Strategic-Plan

Gearon, Liam Francis. *The Routledge International Handbook of Universities, Security and Intelligence Studies*, edited by Gearon, Liam Francis. 1st ed. Milton: Routledge, 2020;2019;. doi:10.4324/9780203702086.

Greenberg, Andy, Inc OverDrive, and OverDrive ebook. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's most Dangerous Hackers*. 1st ed. New York: Doubleday, 2019.

Inkster, Nigel. "The Chinese Intelligence Service." In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, edited by Gearon, Liam Francis. 1st ed., 196-207: Routledge, 2020.

Jinghua, Lyu and Gaurav Kalwani. "Navigating the US-China Competition in Cyberspace." Turkish Policy Quarterly 19, no. 2 (2020): 135-144.

Krishan, Nihal. "NDAA requires intelligence agencies to study creation of cyber collaboration program." *FedScoop*, December 8, 2022. https://www.fedscoop.com/ndaa-requires-intelligence-agencies-study-creation-cyber-collaboration-program/

Lieutenant-Colonel Frances Allen. CN(EH?): SHOULD THE CF ADOPT COMPUTER NETWORK EXPLOITATION AND ATTACK CAPABILITIES?. https://www.cfc.forces.gc.ca/259/181/74_allen.pdf

Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Microsoft. Defending Ukraine: Early Lessons from the Cyber War. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

"Mission." U.S. Department of Homeland Security. Last modified February 26, 2023. https://www.dhs.gov/mission.

"Mission | Homeland Security." Department of Homeland Security. Last modified February 26, 2023. https://www.dhs.gov/mission.

National Security and Intelligence Committee of Parliamentarians. "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack." https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf

National Security and Intelligence Review Agency. "Review of the Communications Security Establishment's (CSE) Ministerial Authorizations and Ministerial Orders Under the *CSE Act*." NSIRA Review 08-501-5. Ottawa, Canada: 2023. https://nsira-ossnr.gc.ca/wp-content/uploads/NSIRA-Redacted-MA-MO-Review_EN.pdf

National Security Agency/Central Security Service. 'NSA Cybersecurity Collaboration Center.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/what-we-do/cybersecurity/cybersecurity-collaboration-center/

"National Defense Authorization Act for Fiscal Year 2022, S.1605, 117th Congress (2021-2022)."

"National Defense Authorization Act for Fiscal Year 2023, H.R.7900, 117th Congress (2021-2022)." Congress.gov. https://www.congress.gov/bill/117th-congress/house-bill/7900

National Security Agency/Central Security Service. 'Mission & Combat Support.' National Security Agency/Central Security Service. Accessed April 23, 2023. https://www.nsa.gov/about/mission-combat-support/

NCSC Annual Review 2022. https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

Netherlands Institute of International Relations. *How states could respond to Policy Brief non-state cyber-attackers*. June 2020. https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf

Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community. 9 April 2021 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community. 6 February 2023. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230313_ODNI_Annual_Threat_Assessment.pdf?VersionId=KRJSJ9e10PtvPVG1zgb6LJiToxxX7wRS

Parasol, Max. "China's Cyber Policies: Conflict between Innovation and Restriction." In AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws, 62-79, 2021.

Presidential Document. 'Further Amendments to Executive Order 12333, United States Intelligence Activities.' Federal Register, August 4, 2008. https://www.federalregister.gov/documents/2008/08/04/E8-17940/further-amendments-to-executive-order-12333-united-states-intelligence-activities

Rashid, Fahmida Y. "8 Types of Phishing Attacks and how to Identify them." CSO (Online) (2020).

Raud, M. (2016, August). China and Cyber: Attitudes, Strategies, Organisation . Tallinn, Estonia: NATO CCDCOE. https://haldus.taltech.ee/sites/default/files/2021-03/ICR2015_proceedings.pdf#page=14

Romaniuk, Scott N. and Mary Manjikian. *Routledge Companion to Global Cyber-Security Strategy*. Milton: Taylor & Francis Group, 2020.

Reuters. EXCLUSIVE Russian software disguised as American finds its way into U.S. Army, CDC apps. https://www.reuters.com/technology/exclusive-russian-software-disguised-american-finds-its-way-into-us-army-cdc-2022-11-14/

Riehle, Kevin P. "Information Power and Russia's National Security Objectives." *The Journal of Intelligence, Conflict, and Warfare* 4, no. 3 (2022): 62-83.

Robson, Maria A. "The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing." *Intelligence and National Security* 35, no. 7 (2020): 954-969.

Ropek, Lucas. "Will CISA Be the Savior of State and Local Cybersecurity?" Government Technology, July 24, 2020. https://www.govtech.com/security/will-cisa-be-the-savior-of-state-and-local-cybersecurity.html

Russia. "National Security Concept of the Russian Federation." Medzinárodné Otázky 9, no. 3 (2000): 99-118.

Russia. FEDERAL LAW NO. 149-FZ OF JULY 27, 2006 ON INFORMATION, INFORMATIONAL TECHNOLOGIES AND THE PROTECTION OF

INFORMATION.
https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf

Russian Cyberwarfare: Unpacking the Kremlin's Capabilities
https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/

Sanger, David E., Inc OverDrive, and OverDrive ebook. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. 1st ed. New York: Crown Publishers, 2018.

Slyke, Jeffrey Van, Joseph Skinner, Barbara Russo, Greg Etter, Michael Corey, Robert Nations, Carl J. Jensen III, David H. McElreath, Daniel Adrian Doss, and Jr Michael Wigginton. Introduction to Homeland Security CRC Press, 2021.

Smalley, Suzanne. "'No guns, no guards, no gates.' NSA opens up to outsiders in fight for cybersecurity." CyberScoop, November 16, 2022.
https://www.cyberscoop.com/nsa-cybersecurity-collaboration-center-morgan-adamski/

Soldatov, Andrei and Irina Borogan. "Russia's very Secret Services." *World Policy Journal* 28, no. 1 (2011): 83-91. https://read-dukeupress-edu.cfc.idm.oclc.org/world-policy-journal/article/28/1/83/76796/Russia-s-Very-Secret-Services

Springer, Paul J., EBSCOhost (Online service), and EBSCO ebook. Encyclopedia of Cyber Warfare. Santa Barbara, Calif: ABC-CLIO, 2017.

State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned 2022.

The Hill Times. Canada's cybersecurity in dire need of an upgrade.
https://www.hilltimes.com/story/2022/10/26/canadas-cybersecurity-in-dire-need-of-an-upgrade/353123/

THE PLA BEYOND BORDERS Chinese Military Operations in Regional and Global Context, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf

'Up your game,' Global Affairs told as report blasts weak governance in areas of national security, intelligence | National Post. https://nationalpost.com/news/up-your-game-global-affairs-told-as-report-blasts-weak-governance-in-areas-of-national-security-intelligence

U.S. Cyber Command. 'Our History.' Accessed April 22, 2023.
https://www.cybercom.mil/About/Our-History/

Whitehouse. National Cyber Strategy of the United States of America. September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Whitehouse. National Cyber Strategy. March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

White House. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." *The White House*. Last modified March 02, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/?utm_source=link.

Whyte, Christopher and Brian M. Mazanec. Understanding Cyber-Warfare: Politics, Policy and Strategy. Milton: Taylor & Francis Group, 2023. doi:10.4324/9781003246398.

"William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R.6395, 116th Congress (2019-2020)."