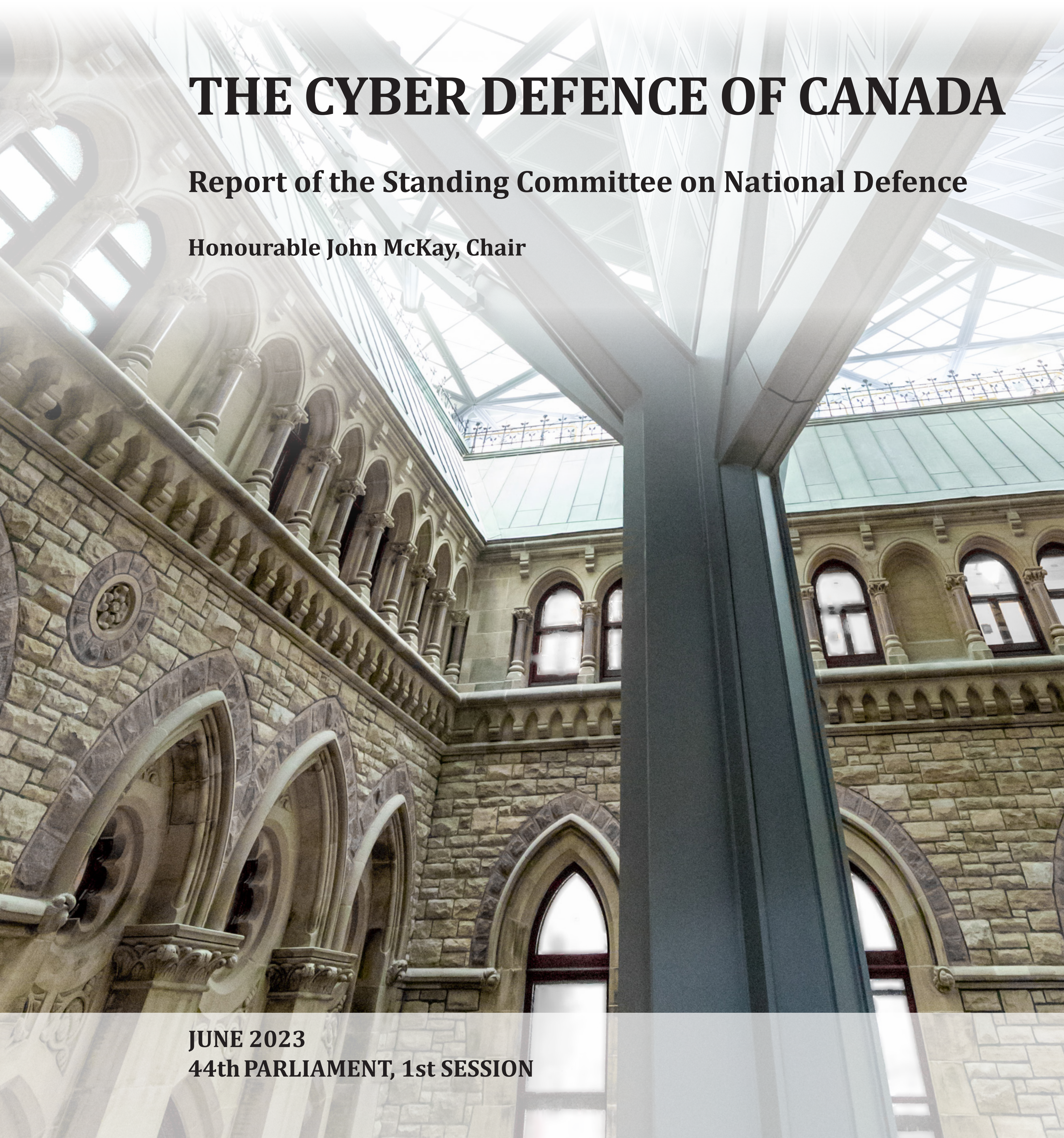
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA



THE CYBER DEFENCE OF CANADA

Report of the Standing Committee on National Defence

Honourable John McKay, Chair

JUNE 2023
44th PARLIAMENT, 1st SESSION

Published under the authority of the Speaker of the House of Commons

Also available on the House of Commons website
at the following address: www.ourcommons.ca

THE CYBER DEFENCE OF CANADA

Report of the Standing Committee on National Defence

Hon. John McKay
Chair

JUNE 2023

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON NATIONAL DEFENCE

CHAIR

Hon. John McKay

VICE-CHAIRS

James Bezan

Christine Normandin

MEMBERS

Darren Fisher

Cheryl Gallant

Pat Kelly

Shelby Kramp-Neuman

Emmanuella Lambropoulos

Lindsay Mathyssen

Bryan May

Jennifer O'Connell

Charles Sousa

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Jenica Atwin

Taylor Bachrach

Alexandre Boulerice

Blaine Calkins

Luc Desilets

Andy Fillmore

Jean-Denis Garon

Mark Gerretsen

Yves Perron

Karen Vecchio

CLERK OF THE COMMITTEE

Andrew Wilson

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Martin Auger

Katherine Simonds

THE STANDING COMMITTEE ON NATIONAL DEFENCE

has the honour to present its

FIFTH REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied Cybersecurity and Cyberwarfare and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

That the Government of Canada establish an ongoing multistakeholder platform for collaboration and engagement on cybersecurity issues. The objectives of this platform could be modelled after the Industry 100, in the United Kingdom. It should be established to create a collaborative space where industry and cyber officials meet to exchange information, best practices and establish forms of reporting private sector cyberattacks to lead to better information sharing and prevention of future attacks. 53

Recommendation 2

That the Government of Canada invest in its own network infrastructure cybersecurity and undertake a comprehensive assessment of additional requirements necessary to harden government systems and third-party network infrastructure on which its data is stored, with the goal of ensuring that its sensitive data is protected and secure. 53

Recommendation 3

That the Government of Canada work with our Five Eyes partners to adopt a Cybersecurity Maturity Model Certification (CMMC) that would be consistent and recognized by our partners to ensure that Canadian defence companies are not disadvantaged by having different security standards in Canada compared to our Five Eyes partners. 53

Recommendation 4

That the Government of Canada take steps to incentivize companies, which could include tax credits, to adopt cybersecurity measures, such as the “CyberSecure” standard established by ISED and CSE for small and medium organizations. 53

Recommendation 22

That the Government of Canada immediately undertake a comprehensive review and expeditious reform of the procurement process for military equipment, including cyberwarfare equipment—this would include Treasury Board guidelines on competition and sole sourcing—with the intent to bring project times down from years to months or weeks. 56

Recommendation 23

That the Government of Canada adapt and develop a comprehensive plan for the recruitment and retention of cyber operators which is competitive with the private sector to ensure positions are filled and the cyber skills gap is closed in the Canadian Armed Forces and the Communications Security Establishment........... 57

Recommendation 24

That the Government of Canada develop and deploy "persistent engagement" capacity in collaboration with the Canadian Armed Forces....................................... 57

Recommendation 25

That the government of Canada implement a system for allowing veterans to maintain security clearances equivalent to the clearances they had with the Canadian Armed Forces when transferring out of service thus enabling a seamless continuity in clearance in order to facilitate their employment in the Department of National Defence. The government should also examine a system of fast-tracking security clearance for veterans seeking employment in other federal departments. 57

Recommendation 26

That the Government of Canada take steps to clearly define the duties and responsibilities of the Canadian Armed Forces and the Communications Security Establishment as they relate to cyber security in Canada and abroad........... 57

Recommendation 27

That the Government of Canada take immediate steps to address logistical support issues in the Canadian Armed Forces, including the Cyber Forces. 57

Recommendation 28

That the Government of Canada ensure the future viability of the CAF Cyber Forces by creating a retention program for its Cyber Operators and supplying them with the necessary cyber infrastructure. 57

Recommendation 29

That the Government of Canada continuously update the legal framework for dealing with cyberattacks, which includes guidelines for attribution, response and liability. 57

Recommendation 30

That the Government of Canada work with our allies to update international laws, such as the Rome Statute and the Geneva Convention, to include state-sponsored cyberwarfare as a war crime. 58

Recommendation 31

That the Government of Canada immediately adopt all outstanding recommendations of the Auditor General's Report 7—Cybersecurity of Personal Information in the Cloud, tabled to Parliament on November 15, 2022. 58

Recommendation 32

That the Government of Canada use existing sanctions regimes to target individuals and entities targeting Canadians with misinformation, disinformation and/or malinformation. 58

Recommendation 33

That the Government of Canada impose effective sanctions on countries which condone or deploy cybercriminals for purposes such as theft of funds, theft of intellectual property, information warfare, and other malicious intents................... 58

Recommendation 34

That the Government of Canada open a review of existing cyber-defence policy and hold bilateral conversations with allies, such as the US, to ensure cohesive and consistent policies are being used. 58

Recommendation 35

That the Government of Canada share Finland and Sweden’s cognitive warfare education for civilians with the provinces. 58

Recommendation 36

That the Government of Canada establish clear boundaries in the operations of the Communications Security Establishment between their signals intelligence and cybersecurity mandates, including ministerial authorization processes and reporting mechanisms. 58

Recommendation 37

That the Government of Canada appoint a cybersecurity ambassador. 59

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

THE CYBER DEFENCE OF CANADA

INTRODUCTION

Reliance on the Internet, computers, smartphones and other digital devices, and networks has become a reality of daily life. The critical infrastructure and systems on which Canadians and the populations in other countries depend every day are becoming increasingly interconnected. People routinely use the Internet for a wide range of activities, including financial transactions, shopping, research, entertainment, connecting with family and friends, dating, interacting on social media, attending medical appointments, engaging in education and training, and working. For many, this use became common at the beginning of the COVID-19 pandemic, and it has remained an enduring feature of their lives since in-person activities of various sorts have resumed. It is now relatively common to find people undertaking activities using a combination of in-person and virtual options in various aspects of their lives. The digital age has completely revolutionized how our societies function, and it has transformed how we work, do business and interact with each other.

However, alongside increases in the amount of time people spend on the Internet, the number of Internet-enabled activities in which they engage, and the volume of personal, business and financial data available online, cyber threats have been rising in both number and sophistication. Worldwide, numerous state and non-state actors are taking advantage of the growing dependence and vulnerabilities of modern societies on complex and interconnected digital systems and technologies to conduct cybercrimes, espionage, sabotage and other malicious activities. In addition, China, Russia and other aggressive authoritarian states are exploiting digital networks and technologies to conduct disinformation campaigns, foreign influence operations and other cognitive warfare activities designed both to divide and manipulate public opinion and to undermine trust and cohesion in democratic countries.

Cybersecurity brings together elements of national security, foreign policy, technology, governance and finance, and involves both the public and private sectors. Cyber threats—including ransomware, attacks on critical infrastructure and network disruptions—involve a range of state and non-state actors, motives and tools. Cyberattacks can be not only difficult to detect and attribute, but also relatively easy to deny, thereby creating uncertainties about appropriate responses.

Moreover, in recent years, cyberspace has emerged as a new domain of warfare, competition and confrontation between and among countries. To an ever-greater extent, state-sponsored actors are leveraging the technical, policy and legal ambiguities associated with operating in the cyber realm to achieve their military and political objectives. Militaries worldwide have been increasing their presence in cyberspace and investing in sophisticated cyber capabilities both to protect their own systems and networks against cyberattacks and to conduct offensive cyber operations against potential adversaries. Russia's use of offensive cyber weapons in its ongoing war against Ukraine has demonstrated the extent to which cyberwarfare and the weaponization of cyberspace have become realities of modern war. Also of note in recent years are the increasingly sophisticated disinformation and foreign influence campaigns conducted by China, Russia and other aggressive authoritarian states against democratic countries, including Canada. These types of activities underscore the critical importance of ensuring the existence of cybersecurity and of combatting cyberwarfare.

Like other countries, Canada has developed national strategies, launched and funded cybersecurity initiatives, adopted legislation and fostered closer international cooperation in cyberspace. That said, more could be done to strengthen Canada's cybersecurity and cyberwarfare efforts, and to improve the extent to which the country, its residents and businesses, and its infrastructure are resilient to domestic and foreign cyber threats.

In this context, on 6 October 2022, the House of Commons Standing Committee on National Defence (the Committee) adopted a motion to undertake a study on cybersecurity and cyberwarfare. In particular, the motion specifically required the Committee to study "the evolving sophistication of threats associated with cybersecurity and foreign actors' capabilities to hack, disrupt, and dismantle means of communication, power grids, databases, and other critical infrastructure." Moreover, it mandated the Committee to examine "the full capabilities of advanced countries to conduct cyberwarfare," as well as "the threat of non-state actors to our cybersecurity," actions that are being taken to "defend Canada against" foreign cyber threats and "the role of individuals and the private sector in cybersecurity."

During five meetings on this study, which were held between 7 February and 31 March 2023, the Committee heard from 17 witnesses comprising Canadian federal government and military officials, academics and other stakeholders. The Committee also received written briefs submitted by individuals who did not appear as witnesses.

This report summarizes comments made in appearances before the Committee or in a brief, as well as other relevant publicly available information. The first section analyzes the cyber threat environment. The second section outlines the members of the Government of Canada's "cybersecurity community," and examines the roles and responsibilities of three cybersecurity community members: the Canadian Security Establishment (CSE); the Department of National Defence (DND); and the Canadian Armed Forces (CAF). The third section describes some challenges that Canada's federal organizations currently face concerning cybersecurity, and identifies possible areas of improvement. The fourth section addresses whole-of-society cybersecurity efforts and considers ways to improve Canada's cyber resilience, with a particular focus on critical infrastructure, cooperation between the public and private sectors, research and development, education, outreach and training provided to the public, and individual privacy and civil liberties. The report concludes with the Committee's thoughts and recommendations.

THE CYBER THREAT ENVIRONMENT

Canada and other countries throughout the world are becoming increasingly interconnected, both within themselves and with each other, partly because of the digital systems on which a rising number of essential services depend. This interconnectedness is not without risks. With ease of access to the Internet and growing technological dependence, there are myriad opportunities for cyber threat activities—including those perpetrated by cybercriminals, hackers, terrorists and state-sponsored actors—to affect daily lives. Moreover, the expanding use of cyberspace by certain aggressive authoritarian states to conduct disinformation campaigns, foreign influence operations and other cognitive warfare threats against Canada and its allies has become an ongoing national security concern. Cyber threats have become a reality of life and they continue to evolve at a rapid pace, giving rise to a need to protect against those threats through a sufficient and sustained focus on cybersecurity.

In this context, witnesses spoke to the Committee about cyber threats to Canada and its allies, cyberwarfare, cognitive warfare and emerging technologies relating to cybersecurity.

Cyber Threats

Cyber threats are growing in number, and they are becoming increasingly complex and sophisticated. The Canadian Centre for Cyber Security defines the term "cyber threat" as "an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains, or to disrupt digital life in general.”[1]

In characterizing cyber threats as an immediate and pressing security concern for Canada, witnesses highlighted the nature of the threat domain and commented on the frequency with which such threats occur in Canada. According to Alexander Rudolph, a Ph.D. candidate in Carleton University’s Department of Political Science, the “cyber-threat domain” can best be described as existing in a “perpetual state of conflict and tension.” In March 2022, as part of the Committee’s study on the defence of Canada in a rapidly changing threat environment,[2] Cherie Henderson, the Canadian Security Intelligence Service’s Assistant Director of Requirements, underscored that “Canada regularly suffers thousands of cyber threat attacks on a daily basis all across the country, and numerous organizations are under that attack.”

State and non-state actors have used offensive cyber programs to target Canada, including its financial sector, critical infrastructure and democratic institutions. Sami Khoury, Head of the CSE’s Canadian Centre for Cyber Security, stated that “cybercrime remains the largest cyber-threat to Canadians,” although the “state-sponsored cyber-programs of China, Russia, Iran and North Korea … pose the greatest strategic cyber-threat to Canada.” As well, he observed that cybercriminals and state-sponsored cyber threat actors mainly target critical infrastructure, adding that ransomware is a prominent and persistent threat to Canadian organizations. Alia Tayyeb, the CSE’s Deputy Chief of Signals Intelligence, agreed, and argued that “the severity of cybercrime and cyber-incidents targeting Canadians and Canadian critical infrastructure, both public and private, is growing exponentially.”

Witnesses drew attention to the rising frequency of ransomware and other types of malware attacks.[3] Alexander Rudolph asserted that ransomware has “completely revolutionized how adversarial states and non-state actors” conduct cyberattacks. In particular, he emphasized that Russia, North Korea and other state actors regularly use ransomware as part of their cyber operations, and indicated that North Korea has been

[1] See Canadian Centre for Cyber Security, Communications Security Establishment (CSE), *An Introduction to the Cyber Threat Environment 2023–2024*, 2022, p. 2.

[2] House of Commons Standing Committee on National Defence (NDDN), *An Interim Report on the Defence of Canada in a Rapidly Changing Threat Environment*, 44th Parliament, 1st Session, June 2022.

[3] According to the Canadian Centre for Cyber Security, the term “malware” is short for “malicious software” and “refers to any software or code designed to infiltrate or damage computer systems.” The term “ransomware” refers to “malicious software that restricts access to or operation of a computer or device, restoring it following payment” of a ransom. The Centre asserts that threat actors often use encryption, although they may also “employ any number of methods of extortion.” See Canadian Centre for Cyber Security, CSE, *An Introduction to the Cyber Threat Environment 2023–2024*, 2022, pp. 10–11.

"very prolific" in using ransomware to steal personal, financial, governmental and corporate information worldwide. Dr. John de Boer, BlackBerry's Senior Director of Government Affairs and Public Policy, noted that—in the previous 90 days—BlackBerry, which protects more than 500 million systems worldwide, had "stopped more than 1.5 million malware-based cyber-attacks, including more than 200,000 new malware samples, before they had a chance to execute." He also pointed out that "there are more than 400,000 new malware samples a day."

Moreover, Dr. de Boer stated that the health care, financial and manufacturing sectors were the most targeted during the previous year, elaborating that cyberattacks on the manufacturing sector are "rising the quickest," probably because of "supply chain vulnerabilities" and the "intrinsic link between economic security and national security." In his estimation, in the last year, the number of cyberattacks on the manufacturing sector rose by 2,000%. In the view of Tadej Nared, Chairman of the Board of the Slovenian Certified Ethical Hackers Foundation, cybercrime has become "the third largest economy in the world." He claimed that, "by 2025, the damage resulting from cybercrime is going to amount to $15 trillion," adding that the damage "grows by an amount of $1,500 billion a year" and is "a huge problem."

Brigadier General (Retired) John Turnbull commented that "cyber crime, whether perpetrated by individuals, organized crime or state sponsored or state enabled entities can become a significant threat to national security." In his opinion, cybercriminals challenge "the effectiveness of all levels of government, tax the economy, and ultimately erode [public] trust in [the capabilities of] national institutions to protect citizens."[4] Alia Tayyeb mentioned that "state and state-sponsored cyber-actors also pose a continuing threat to Canada." Sami Khoury underlined that China, Russia, North Korea and Iran "have a variety of motivations to go against Canada." He noted, for instance, that China is using its cyber tools to target "research, technical data, business intellectual property and military capabilities," and that North Korea is "very much interested in enhancing its economic value by stealing credentials and then stealing funds."

Aaron Shull, the Centre for International Governance Innovation's Managing Director and General Counsel, said that cyberattacks are often carried out by state actors "who aim to steal sensitive information or disrupt critical infrastructure over a long period of time." In providing an example, he contended that Chinese, Russian and other authoritarian state actors have been using ransomware for extortion and conducting cyberattacks on supply chains and critical infrastructure worldwide, adding that they also use cyber tools to interfere in democratic elections, spread disinformation and

[4] Document submitted to NDDN by Brigadier General (Retired) John Turnbull, 13 February 2023.

manipulate social media, all with a view to influencing and dividing public opinion in foreign countries.

According to Alex Rapin, Research Fellow, Raoul-Dandurand Chair in Strategic and Diplomatic Studies of the Université du Québec à Montréal, there have been 93 publicly recorded geopolitical cyber incidents targeting Canada since 2010, of which 14 took place in 2022. He highlighted that these 93 incidents included economic espionage directed against Canadian businesses and universities, covert electronic surveillance of Canadian-based activists and non-governmental organizations, and intelligence gathering that targeted Canadian government organizations. In his view, "the overwhelming majority of these incidents originate from just four countries: China, Russia, Iran and North Korea." Regarding current cyber threat trends, he drew attention to "the growing threat of ransomware cyber-attacks against Canadian entities" for clandestine intelligence collection or to disrupt critical infrastructure, the "increasingly aggressive targeting of Canadian-based activists, exiles and dissenters … for purposes of espionage, intimidation and harassment," and the "rise of the cyber-mercenaries industry, which is starting to target Canadian entities, most probably at the request of foreign powers."

Cyberwarfare

Witnesses spoke about cyberwarfare and the increasing use of cyber tools in military operations. Jonathan Quinn, the Department of National Defence's Director General of Continental Defence Policy, indicated that "cyberspace has become another domain of military and national security operations, characterized by constant low-level, below threshold competition that draws in allies and adversaries alike." In Alexander Rudolph's opinion, "cyber-defence and cyberwarfare are very targeted on the threats" to national defence and—for the most part—are focused on "state and not non-state actors."

Witnesses referred to the ongoing war in Ukraine as an example of cyberwarfare. According to Jonathan Quinn, "the conflict in Ukraine demonstrates that cyber capabilities play a critical role in modern-day warfare." Alexander Rudolph emphasized Russia's use of "cyber-operations with near-simultaneous joint kinetic military operations" in Ukraine over the past year. Expressing similar views, Sami Khoury suggested that Russia's cyberwarfare activities in Ukraine demonstrate that Russia is "a formidable cyber-actor." In particular, he noted that the Russians have been using cyber tools as weapons and, alongside kinetic military attacks, have launched numerous cyber strikes against targets in Ukraine.

Dr. Wesley Wark, Senior Fellow at the Centre for International Governance Innovation, observed that the war in Ukraine has been a cyberwarfare testing ground and "has provided important real-world insights into the ways in which cyber-weapons can and will be used in wartime in conjunction with more conventional military attacks." Moreover, he argued that Canada and its allies need to "pay attention" to how the Russians and Ukrainians have been conducting cyber operations militarily and to how that conflict has become "a laboratory for cyberwarfare" because it is the first real war where cyberwarfare methods are being used to a significant extent. In his view, "[e]verything that's been used by Russia against Ukraine, and the way in which Ukraine has responded, is very important for us as a matter of study." He highlighted three conclusions that can be reached about Russia's cyberwar against Ukraine: "First, civilians are prime targets. Second, cyber weapons are not precision munitions, and third, cyber-aggression knows no rules or bounds."

As well, Dr. Wark pointed out that the "scope and severity" of Russian cyber operations directed against Ukraine have become "more sophisticated and widespread" since February 2022, underscoring that Russian cyberattacks have been targeting energy and other critical infrastructure in an "effort to destroy Ukrainian sources of civil power supply and undermine morale." Furthermore, he commented that Russia carried out—on average—"more than 10 cyberattacks on Ukrainian critical energy infrastructure per day in November of 2022." He also asserted that Ukraine has been "ramping up [its cyberwarfare] capabilities" with the assistance of "key allies in the west and from all the Five Eyes partners," and has been effective in conducting cyber counterattacks against the Russians. Moreover, in his opinion, "beyond the Ukraine theatre," Russian cyber threat actors "were engaged in widespread cyber-espionage campaigns against NATO countries and looking to develop further cyber-capabilities against such targets, including Canada."

Cognitive Warfare

Witnesses focused on cognitive warfare threats,[5] which include foreign influence, espionage and disinformation, misinformation and malinformation campaigns.[6] Marcus Kolga, Senior Fellow at the Macdonald-Laurier Institute, drew attention to the "information operations aspect of foreign cyberwarfare and the threat it poses to our information environment and our national security." Describing cognitive warfare as "an extremely important tool in [the] tool kit" of Russia, China and other adversarial state actors, he stated that "we need to make sure that we have the capabilities to address those threats and to go on the offensive against our adversaries when they engage in that sort of warfare." More specifically, he indicated that disinformation is a form of cybersecurity threat, and contended that foreign adversaries often spread disinformation in "digital communication" form using various social media platforms, emails and websites.

As well, witnesses mentioned that China and Russia have been using their cognitive warfare capabilities against Canada. Marcus Kolga underlined that, over the past decade, "information warfare has become a primary tool in Russia's hybrid and cyber tool kit," and argued that the country "has directly targeted Canada." According to him,

> [t]he broad goal of Russian information warfare is to undermine public trust in our democracies and the cohesion of our societies. They do this by weaponizing issues and narratives that have the greatest potential to polarize us. They inject and amplify narratives that exploit both Conservative and Liberal biases and any issues that have the potential to drive wedges between Canadians.

In providing an example, he referred to Russia's disinformation operations targeting Canadians during the COVID-19 pandemic, as well as Canadian Armed Forces personnel

[5] A recent study defines the term "cognitive warfare" as "the weaponization of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions." The study also indicates that cognitive warfare "goes a step further than just fighting to control the flow of information. Rather, it is the fight to control or alter the way people react to information. Cognitive warfare seeks to make enemies destroy themselves from the inside out." See Alonso Bernal et al., *Cognitive Warfare: An Attack on Truth and Thought*, North Atlantic Treaty Organization and Johns Hopkins University, 2020, p. 3.

[6] The Canadian Centre for Cyber Security defines "disinformation" as "intentionally false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction," "misinformation" as "unintentionally false information that is not intended to cause harm" and "malinformation" as "information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm." See Canadian Centre for Cyber Security, CSE, *An Introduction to the Cyber Threat Environment 2023–2024*, 2022, p. 12.

deployed in Latvia, Ukraine and elsewhere in Europe under Operations REASSURANCE and UNIFIER since 2015.

Furthermore, Marcus Kolga pointed out that China's information operations are "a significant and persistent threat" to Canada's national security and defence, asserting that—in recent years—"China has very much targeted Canada" with disinformation, and has used "increasingly sophisticated" cognitive warfare methods. He elaborated that "China has targeted Canada with various different nefarious activities to try to undermine our democracy during the past three elections," and encouraged the Government of Canada to keep "a very close eye" on China. Moreover, he warned about a possible "close alignment" of Chinese and Russian disinformation campaigns in the future, suggesting that the two countries might "support each other" concerning cognitive warfare.

Similarly, Dr. Wark commented that China and Russia "are particularly good" at disinformation, misinformation and malinformation campaigns, and cautioned that the countries are developing new and more sophisticated ways of spreading false information and influencing public opinion in Canada and allied countries. In his view, Canada must remain vigilant and responsive to such activities.

Aaron Shull spoke about the need for "societal resilience" against cognitive warfare threats. In his opinion, "[w]hen we think about disinformation, misinformation or malinformation, the point is that people are persuadable. There are sophisticated influence campaigns that are taking place all the time to try to change our discourse, to sow societal division and to pull people in different directions, when we need to be uniting."

Emerging Technologies

Witnesses drew attention to the cyber threats posed by emerging technologies in cyberspace, particularly artificial intelligence (AI) and quantum computing. Marcus Kolga expressed "deep concern" about "any future technologies [in] the information realm," and particularly noted both that AI is "developing very quickly" and that "the speed with which our foreign adversaries can put out information and disinformation is going to be quite alarming" with such technologies. According to him, "deepfakes"—"fake videos, fake images and fake audios that are increasingly created by AI"—are another emerging technological threat that is "growing and will become problematic in the coming years." In providing an example, he observed that deepfakes can make an image of a person—such as the President of the United States—appear to be "saying something that he's not actually saying," with the technology used to create these videos becoming “terrifyingly accurate.” In his view, Canada is not prepared to “deal with the emergence,” and “to address that growing threat,” of AI and deepfakes.

Dr. Thomas Keenan, Professor at the University of Calgary’s School of Architecture Planning and Landscape, also warned about AI, speculating that it will “revolutionize everything, including cybersecurity and cyberwarfare, and a lot quicker than most people expected.” He highlighted that AI is already being used in civil society in a wide range of areas, “from detecting tiny tumours on MRIs to helping cities optimize traffic signals,” and cautioned that, “like so many industries, our defence folks will embrace AI without fully understanding how it can be used against us.” In underscoring particular concerns about training, ethical issues and the use of public domain information databases by armed forces that use AI technologies, he emphasized that “there definitely should be a policy” outlining the limits of the use of AI in the military, and argued that this policy should be developed in “consultation with industry and academia.”

Tim Callan, Chief Experience Officer and Chief Compliance Officer at Sectigo, focused on quantum computing, indicating that—at the moment—the “proper and comprehensive use of digital identity” is essential to providing “secure digital processes across businesses, government, infrastructure, finance, transportation, health care, education and nearly all other walks of life.” In his opinion, “securing digital identities occurs through public key infrastructure,” which is a “time-proven method of exchanging cryptographic keys to verify connected systems and encrypt data.” He suggested that “the stakes are rising with the advent of quantum computers,” which—in the coming years— “will be able to easily defeat more than 99% of the world’s encryption,” thereby “rendering encrypted data subject to exposure by any attacker with access to a quantum computer.” For that reason, he urged the Government of Canada and the private sector to begin preparing for this threat, asserting that “the time for this action is today.”

Kristen Csenkey, a Ph.D. candidate from Wilfrid Laurier University’s Balsillie School of International Affairs, referred to AI and quantum computers as “disruptive” emerging technologies, and advocated “more co-operation to address the threats we associate with the use of these particular technologies, while also keeping in mind that it is not just the technology that's the threat.” According to her, there is “the potential for certain malicious actors to use these certain technologies in a way that could cause harm.”

THE GOVERNMENT OF CANADA’S CYBERSECURITY COMMUNITY

In Canada, no single entity is responsible for cybersecurity. Rather, cybersecurity is seen as a whole-of-society effort involving multiple entities within the public and private sectors. The Government of Canada's cybersecurity community comprises at least one dozen federal departments and agencies, including CSE, DND and the CAF. These departments and agencies have distinct roles and responsibilities relating to cybersecurity, and they cooperate with each other to help keep Canada safe from cyber threats. As well, they collaborate and share information with provincial and territorial governments, the private sector and international partners, including Canada's Five Eyes partners—Australia, New Zealand, the United Kingdom and the United States—and the 31 member states of the North Atlantic Treaty Organization (NATO).

In speaking to the Committee, witnesses focused on the Government of Canada's cybersecurity efforts to help protect Canada against cyber and cognitive warfare threats. More specifically, witnesses examined Canada's whole-of-society effort concerning cybersecurity, the main federal departments and agencies that play a role in the Government of Canada's cybersecurity community, the particular roles and responsibilities of CSE, DND and the CAF, and cybersecurity-related cooperation within the national defence portfolio.

A Whole-Of-Society Effort

Witnesses contended that everyone has a role to play in ensuring cybersecurity. In Aaron Shull's view, cybersecurity "is a whole-of-society concern for Canada." He underlined that cybersecurity is about governance, and noted that it affects both the public and the private sectors. He argued that, in "light of current geopolitical trends, … it is our collective duty to better prepare the country" to deal with cyber and cognitive warfare threats.

Kristen Csenkey characterized cybersecurity as a "dynamic" whole-of-society effort, emphasized that it is "complex, constantly changing and involve[s] multiple actors, contexts and ideas," and described it as "an interconnected social, political and technical endeavour, wherein humans and technologies are intertwined." Consequently, in her view, "we can't really think of cybersecurity issues as a siloed issue" and there must be a recognition that "we live in a cyber-physical world, where many aspects of our lives occur in digital spaces with physical linkages."

In acknowledging the whole-of-society effort required to ensure cybersecurity, Kristen Csenkey stressed the need for coordination and cooperation between the private and public sectors, and with like-minded, high-tech foreign allies. According to her, coordination and cooperation between and among the diverse entities involved in the "interconnected political, social and technical aspects of cybersecurity" must be a priority if the goals are to protect Canada effectively and efficiently against cyber threats and to address the "evolving nature of threats associated with cybersecurity, including the technological capabilities and capacities of various actors."

The Government of Canada's Cybersecurity Community

In 2018, the Government of Canada released its *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* (the National Cyber Security Strategy), which led to the creation of the Canadian Centre for Cyber Security and the National Cybercrime Coordination Centre. The National Cyber Security Strategy identifies three pillars of action: securing government systems; partnering to secure vital cyber systems outside the government; and helping Canadians be secure online.

As noted earlier, at least 12 federal departments and agencies have roles and responsibilities relating to cybersecurity in Canada.[7] Jonathan Quinn contended that cybersecurity "is a complicated space" because "there are lots of players across government in this area." That said, he identified Public Safety Canada as the "Canadian federal lead for cybersecurity—ensuring the security of government networks, providing assistance to holders of networks in critical infrastructure and that sort of thing."

As the Government of Canada's policy lead for cybersecurity and the coordinator for most federal cybersecurity activities, Public Safety Canada works with the other federal departments and agencies on a range of policy and operational issues. CSE leads the development and deployment of cybersecurity capabilities. In addition to Public Safety Canada and CSE, the other federal department and agencies involved in cybersecurity in Canada are the following:[8]

- the Canadian Anti-Fraud Centre;
- the Canadian Radio-Television and Telecommunication Commission;
- the Canadian Security Intelligence Service;
- Defence Research and Development Canada;
- DND and the CAF;
- Innovation, Science and Economic Development Canada;

[7] Public Safety Canada, "Cyber Security in the Canadian Federal Government."

[8] Ibid.

- the Office of the Privacy Commissioner of Canada;
- the Royal Canadian Mounted Police;
- Shared Services Canada; and
- the Treasury Board of Canada Secretariat.

Among the federal departments and agencies with responsibilities relating to cybersecurity, witnesses discussed the cybersecurity activities of the main national defence portfolio organizations—CSE, DND and the CAF—and cooperation among them.

The Communications Security Establishment

As one of the three primary federal departments and agencies with roles and responsibilities concerning cybersecurity, witnesses made comments about CSE. Sami Khoury and Alia Tayyeb characterized CSE as Canada's lead organization for foreign signals intelligence and cyber operations, and as the technical authority for cybersecurity. The 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* indicates that CSE "collects intelligence on threats to government systems and networks, operates a sophisticated, layered defensive network of sensors that identifies and blocks those threats, and provides direction and advice to government organizations (and increasingly, to Canadians and private sector organizations) to strengthen their own information technology security."

CSE also operates the Canadian Centre for Cyber Security, which is the "single unified source of expert advice, guidance, services and support on cybersecurity" for federal departments and agencies, the provinces and territories, municipalities, critical infrastructure owners, the private sector, academia and the Canadian public. Jonathan Quinn explained that the Canadian Centre for Cyber Security is a "CSE body, but it also works under policy set by Public Safety [Canada]," and noted that "it has an important role to play … in sharing best practices, providing assistance to Canadian companies, and identifying and mitigating threats."

Sami Khoury said that, although CSE has the task of defending Government of Canada networks and the Canadian Centre for Cyber Security leads the Government's response to cyber-incidents, "cybersecurity is not solely a federal government responsibility or concern, as cyber-threats continue to target and impact Canadian individuals and organizations." According to him, CSE works with various partners within and outside of government, including the private sector, in “sharing information about threats and best practices in cybersecurity.” In particular, he outlined that the Canadian Centre for Cyber Security regularly publishes guidance and expert advice for Canadians, and drew attention to the *National Cyber Threat Assessment 2023–2024*, which describes current cybersecurity trends affecting Canadians.

Alia Tayyeb commented that, in August 2019, the *Communications Security Establishment Act* was amended to add the conduct of “active cyber operations” (i.e., offensive cyber operations) to CSE’s existing authorities regarding signals intelligence and cybersecurity. In her opinion, these amendments “allowed CSE to expand its tool suite to conduct active and defensive cyber-operations, together referred to as foreign cyber-operations.” The statute defines “active cyber operation” as “activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.” Such operations cannot be carried out against Canadians or people in Canada, and they must be authorized by the appropriate federal minister.

Moreover, Alia Tayyeb asserted that, “since being granted these new [offensive cyber operations] powers, CSE has leveraged its cyber operations capability to hinder the efforts of foreign-based extremists seeking to recruit Canadians, to carry out online campaigns and to disseminate violent extremist content,” and has “disrupt[ed] the activities of cybercriminals planning ransomware attacks.” That said, she mentioned that “CSE is not permitted in any way, shape or form to target Canadians or any individuals in Canada,” adding that this “basic prohibition” applies to CSE’s foreign intelligence and cyber operations mandates.

In describing CSE as forward-looking and determined “to continue to adapt to the evolving threat environment, bolster defences and help better protect Canada,” Sami Khoury expressed hope that Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, “will continue to progress in Parliament.”[9] He stated that the bill is intended to promote cybersecurity across four federally regulated critical infrastructure sectors—telecommunications, energy, finance and transport—and suggested that it would not only establish a regulatory framework to strengthen cybersecurity for services and

[9] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, was introduced in the House of Commons on 14 June 2022 and completed its first and second readings on 14 June 2022 and 27 March 2023, respectively. As of 19 June 2023, it had been referred to the House of Commons Standing Committee on Public Safety and National Security for study.

systems that are vital to national security and public safety, but also would give the Government of Canada a new tool for responding to emerging cyber threats.

Furthermore, Sami Khoury highlighted the work underway at Public Safety Canada designed to renew the 2018 National Cyber Security Strategy, explaining that the renewed strategy will “articulate Canada's long-term strategy to protect our national security and economy, deter cyber-threat actors and promote norms-based behaviour in cyberspace.” He underscored that, for CSE, renewal of the strategy provides an opportunity “to review the situation and build on what the Canadian Centre for Cyber Security has achieved over the past five years,” emphasizing that the Centre’s creation was among the main initiatives set out in the 2018 strategy.

Finally, Sami Khoury noted that CSE will “work to build relationships with Canadian industry and other levels of government,” as well as collaborate “with our international partners, in the Five Eyes and beyond.”

The Department of National Defence and the Canadian Armed Forces

In acknowledging that—like CSE—DND and the CAF are important members of the Government of Canada’s cybersecurity community, witnesses discussed the particular roles, responsibilities and capabilities of DND and the CAF. Jonathan Quinn and Rear-Admiral Lou Carosielli, Commander of the Canadian Armed Force’s Cyber Force, pointed out that cyberwarfare has been a growing concern for DND and the CAF for several years, with Canada’s military making efforts to strengthen and expand its cyber capabilities in cooperation with other federal departments and agencies, as well as foreign allies and partners.

In explaining specific cyber-related roles, responsibilities and capabilities, Jonathan Quinn and Rear-Admiral Carosielli highlighted that DND and the CAF are mainly responsible for protecting their own information systems and networks against cyber threats, and not for protecting those of other federal departments and agencies or the private sector. Jonathan Quinn added that *Strong, Secure, Engaged: Canada’s Defence Policy*, which was released in 2017, directed DND and the CAF “to assume a more assertive posture in the cyber domain to develop offensive cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.” He stressed that DND and the CAF are doing so “in close partnership with … colleagues at the Communications Security Establishment.”

Rear-Admiral Carosielli argued that “cyberspace is critical when conducting modern military operations and is recognized by Canada and its allies as a domain of military operations, a true war-fighting domain.” As well, he commented that the CAF relies on the “force multiplier effect of technology-enabled communications, intelligence and weapons systems, which must be adequately secured and defended from cyber threats.” He drew attention to the CAF Cyber Forces, which were established in 2017 to defend the information systems and networks of DND and the CAF against cyber threat actors and to support partners and allies, “as capacity permits.” In his view, the CAF Cyber Forces “contribute to international peace and security through cyber threat intelligence sharing with allies and partners and through the conduct of full spectrum cyber operations as authorized by the Government of Canada.”

Furthermore, Rear-Admiral Carosielli recognized that, even though the CAF Cyber Forces “are responsible for defending the networks and [information technology] systems” for DND and the CAF, they also work “very closely” with other federal partners, such as CSE and the Royal Canadian Mounted Police, “to ensure that we share all of the information that we receive among the partners from intelligence … so that all of us have a good wealth of information and understand what's going on in the other networks.”

According to Rear-Admiral Carosielli, the CAF considers its cybersecurity relationships with international allies to be “critical.” He underlined that the CAF Cyber Forces “are very closely aligned with U.S. Cyber Command, so much so that [it has] a liaison officer embedded within U.S. Cyber Command, as well as numerous personnel who range all the way from cyber-operators to cyber operations planners.” In his opinion, this relationship allows the CAF Cyber Forces and the U.S. Cyber Command to “have daily conversations,” adding that the CAF Cyber Forces also maintains strong cybersecurity relationships with “allies within the Five Eyes and NATO.”

In further illustrating the extent to which the CAF Cyber Forces collaborate with international allies, Rear-Admiral Carosielli mentioned that, in response to Russia’s invasion of Ukraine in February 2022, the “CAF immediately stood up a cyber task force to help Ukraine bolster its cyber defence capabilities.” He also said that Canada currently “provides Ukraine with cybersecurity expertise, cyber threat intelligence, software tools and technical solutions that allow them to better defend their networks against malicious cyber-activities.” As well, according to him, at the request of the Government of Latvia, the CAF has “deployed a persistent cyber task force to Latvia to conduct joint threat hunt operations to assist them in better defending themselves from [cyber] threats.”

Jonathan Quinn emphasized that DND and the CAF are "committed to seizing the opportunities of cyberspace in a responsible manner and will continue working toward advancing the ability of our military cyber forces to conduct cyber operations independently with allies and other government departments to make Canada safer from cyber threats."

Cooperation Within the National Defence Portfolio

In focusing on cooperation among CSE, DND and the CAF, witnesses examined the ways in which they interact with each other and share cybersecurity-related resources and information. Alia Tayyeb indicated that CSE has a strong relationship with DND and the CAF, and has "used its capabilities to support the Canadian Armed Forces in carrying out its mandate." In particular, she contended that they "essentially have a combined workforce," with "embedded officers" who "work effectively" together on cybersecurity issues.

Jonathan Quinn and Rear-Admiral Carosielli agreed, with the latter observing that CSE, DND and the CAF have "a long-standing relationship" that "is continuing through cyber" as they "work closely [together] day in and day out." Rear-Admiral Carosielli added that:

> CSE personnel are embedded within the CAF teams and CAF personnel are embedded within the CSE teams. We share information. We share tools. We share intelligence … and mutually support each other in operations for CSE, as well as in operations for the Canadian Armed Forces.

That said, Rear-Admiral Carosielli stressed that "the CAF and CSE cyber capabilities differ for the principal reason that we do not want to duplicate or have redundant capabilities." In his view, "CSE has more specialized technical expertise, while the Canadian Armed Forces are typically used for the last mile," clarifying that "CSE personnel do not typically go into war zones or conflict zones, so in Canadian missions the last mile is done by Canadian Armed Forces personnel."

Rear-Admiral Carosielli also commented that "the CAF and CSE operate together, depending on what support is required and under whose authorities certain operations are being done." He elaborated that,

> [i]f a specific military operation is being done under CAF authorities and we need some support in the form of intelligence or tools, we can get that via Section 20 of the CSE Act. Similarly, if CSE is working on something and they need some of our subject matter expertise, there are ways for them to ask for our support. We can provide that and support them under CSE authorities in order to meet the requirements of Canada.

Jonathan Quinn and Rear-Admiral Carosielli spoke about the ways in which CSE and the CAF work together on offensive cyber operations.[10] Rear-Admiral Carosielli explained that CSE and the CAF can conduct offensive cyber operations as long as they receive a mandate to do so. He pointed out that authorizations concerning the CAF are given by the Government of Canada or by Cabinet and that, for "operations done under a mandate given [to] the Communications Security Establishment," the "approval is given by the Department of National Defence and the Department of Foreign Affairs." Concerning mandates, Jonathan Quinn highlighted that:

> [t]he Canadian Armed Forces have the authority to conduct offensive cyber-operations in the context of approved military missions. In those, it's the Canadian Armed Forces leading and conducting offensive cyber-operations under their own authorities, often with assistance from colleagues at the Communications Security Establishment. There are other offensive cyber-operations that are conducted under CSE authorities, under the CSE Act. … When CSE is conducting offensive cyber-operations under the CSE Act, they are able to reach over to the Canadian Armed Forces for assistance as required under Section 20 of the Act.

Regarding CSE's role in offensive cyber operations, Alia Tayyeb emphasized that CSE does not "work independently," stating that:

> [w]e work very closely with the Canadian Armed Forces and the Department of Foreign Affairs. … The Minister of Foreign Affairs is required to provide her consent for [active cyber] operations. We work very closely in the planning and development of those operations and assessing the risks.

Dr. Christian Leuprecht, Professor at the Royal Military College of Canada, supported the powers that the Government of Canada has given to CSE, DND and the CAF in recent years to enable them to undertake offensive cyber operations against malign cyber threat actors, but asserted that Canada should be bolder and should not hesitate to conduct such operations to defend its interests in cyberspace. In his opinion, the Government has been reluctant to undertake offensive cyber operations and has been "extremely reticent" in using the powers that were given to CSE in August 2019. He suggested that, by not using those powers, Canada currently "lacks the political will to

[10] The Canadian Association of Defence and Security Industries defines "defensive cyber" capabilities as "activities and operations conducted on or through the global information infrastructure to protect an institution's electronic information and information infrastructures as a matter of mission assurance. Defensive cyber operations do not normally involve direct engagement with the adversary." It defines "offensive cyber" capabilities as "operations [that] manipulate and disrupt adversarial networks and systems to limit or eliminate their operational capability. Although offensive cyber capabilities and cyber weapons can be developed by the private sector independently or in partnership with government, operations that utilize these capabilities are often led by nation states, and require legislative or ministerial-equivalent approvals." See Canadian Association of Defence and Security Industries, *From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence*, 2019, pp. 8, 9.

demonstrate independent international leadership to reduce instability and uncertainty," and the country should "use them to defend the interests of Canada and its allies in cyberspace." According to him,

> [t]he reason we need to use them is that this is a very particular role for the state to play, because private sector actors and other public sector actors do not have active and offensive capabilities that they can employ. Only the state can deploy those capabilities, so only the state can be proactive in either interdicting or, if need be, in cyberspace, also perhaps sabotaging the capabilities of state-based or state-tolerated malicious actors.

Moreover, Dr. Leuprecht argued that Canada must move away from its traditional defensive approach to cybersecurity when dealing with cyber threats and malicious state and non-state actors in cyberspace. According to him, the Government of Canada should be "more robust and muscular" in demonstrating to adversaries that certain types of behaviour "will not be tolerated in cyberspace and will draw repercussions, whether those repercussions are in cyberspace or kinetic." To that end, he proposed that Canada should develop a cyber doctrine that would clearly define and communicate how the country could employ its cyber capabilities against malicious cyber actors.

IMPROVING FEDERAL CYBERSECURITY EFFORTS

Cybersecurity requires constant vigilance, as well as ongoing and significant investments in financial, human, material and technological resources. With new and more sophisticated cyber threats and cognitive warfare threats emerging daily, federal departments and agencies with cybersecurity roles and responsibilities must adapt rapidly in order to defeat those threats and protect Canada. Regarding cybersecurity, there is always room for improvement.

In identifying a number of cybersecurity challenges facing the Government of Canada's cybersecurity community, witnesses provided possible solutions. In particular, they spoke to the Committee about strengthening cyberwarfare capabilities and relationships, centralizing cybersecurity efforts, addressing cyber workforce challenges, responding to cognitive warfare threats, reforming defence procurement, enhancing global cooperation and developing international legal frameworks in cyberspace.

Strengthening Cyberwarfare Capabilities and Relationships

Witnesses generally acknowledged the important relationships between and among CSE, DND and the CAF in relation to cybersecurity, but some advocated actions that would strengthen their capabilities and cooperation. Alexander Rudolph contended that CSE's and the CAF's roles and responsibilities regarding cybersecurity should be better defined through a legal framework or "bill to address cyber-defence in the armed forces and CSE." In his view,

> [t]here particularly needs to be a formal force and command structure that organizes CSE and the military, as it currently doesn't exist. It's very ad hoc. … There needs to be an actual formal command structure in place to mediate what happens in the event of a conflict.

Witnesses were critical of DND's and the CAF's cybersecurity capabilities and level of preparedness. Alexander Rudolph asserted that Canada needs a "very targeted cyber-defence response" to cyber threats, adding that "the CAF is, in no way, prepared to face cyberwarfare in the event of a conflict." In his opinion, "Canadian cyber-defence policy can be described as incomplete, ad hoc and inconsistent in strategy and definition with Canada's allies, particularly the United States." Likewise, Tadej Nared claimed that the "CAF is not ready to meet even moderate cyber threats" and "won't be ready to meet modern cyber challenges for the foreseeable time." According to him, more must be done to strengthen the cyber capabilities of DND and the CAF.

Similarly, witnesses contended that more should be done to strengthen the cyber capabilities of CSE, including through increased funding and other resources for the Canadian Centre for Cyber Security. In Alexander Rudolph's view,

> [t]here needs to be a lot more funding to the Canadian Centre for Cyber Security and ways for the centre to interface with the rest of the government and for the government to look to what the provinces need and what the federal government needs, as there are very different, diverse needs for both to provide services … [and to] protect the government from threats.

Dr. Leuprecht proposed "a lot more intergovernmental collaboration" between CSE and Canada's provincial and territorial governments. In providing an example of such collaboration, he noted that "the Australian Signals Directorate, the equivalent of the Communications Security Establishment in Canada, or CSE, has offices in each of the Australian states."

Centralizing Cybersecurity Efforts

Witnesses drew attention to the lack of centralization regarding Government of Canada cybersecurity efforts, and expressed concerns about accountability. Dr. de Boer underscored that, "today, cyber-responsibilities in the federal government are distributed across at least 12 departments and agencies," adding that "multiple ministers have cyber-responsibilities, yet it is unclear who leads and who is responsible for ensuring coherence and a unity of effort." In his opinion, "when cybersecurity doesn't have a dedicated person pushing and fighting for the issue, it sits in the middle of everyone's priority list."

Dr. de Boer commented that, in several countries, cybersecurity efforts are centralized under a single authority, including in Australia and the United States, where the issue was "tackled … head-on by appointing a cyber minister," and—in the case of the United States—by selecting someone who is presidentially nominated and congressionally confirmed. According to him, "Canada should consider establishing a cabinet or other senior position responsible for ensuring government-wide coherence and action on cybersecurity" because, at present, the Government of Canada lacks "a unity of effort" and it is "unclear" who is responsible for protecting critical infrastructure in Canada against cyber threats.

Similarly, Tim McSorley, National Coordinator of the International Civil Liberties Monitoring Group, argued that cybersecurity efforts in Canada should be centralized, stating that:

> we need a centralized office to engage with cybersecurity. … Having an agency tasked with not only ensuring cybersecurity is handled properly but also that it's reviewed and accountable, and that there's transparency around it, would be important as well.

Dr. Leuprecht suggested that the Government of Canada should consider Quebec's centralized model, where cybersecurity efforts are led and coordinated through a Ministry of Cybersecurity and Digital Technology (Ministère de la Cybersécurité et du Numérique), which is supported by a group of advisers. In describing Quebec's efforts as "very interesting," he asserted that the Government of Canada "could learn a number of things from Quebec." Moreover, he indicated that "the problem with current political decision-making processes" is that "we dither too long in making key decisions where we need to provide political authority, authorization and direction." In his view, Canada needs to accelerate cybersecurity decision-making because "the longer we wait, the narrower our margin to manoeuver gets and the fewer options we have in our toolbox." According to him, "we need [cybersecurity-related] decision-making processes that are more agile, … [and] that are faster in order to maximize the options available politically to the government and the instruments in terms of operations to achieve the effect that the government intends."

Addressing Cyber Workforce Challenges

With a focus on the cyber workforce, witnesses stressed that shortage of cyber specialists is affecting Canada's private and public sectors, including CSE, DND and the CAF. Dr. de Boer mentioned that "there are not enough cyber professionals in the world," explaining that "there are more than three million vacant [cyber] jobs globally, and in Canada there are probably around 200,000." In his opinion, the cyber workforce shortage is a critical and pressing challenge for Canada.

Sami Khoury identified some of CSE's recruitment and retention challenges regarding cybersecurity experts, acknowledging that CSE and other federal departments and agencies have to compete with the private sector for personnel in a field in which there is a labour shortage. In his view, CSE is making investments in both retaining its current workforce and trying to hire new employees for a number of positions. He said that CSE is "very mindful of the challenges associated with the current employment landscape," is endeavouring "to attract talent from all over Canada," and is particularly interested in "Canadians who represent the rich and diverse society in which we live." According to him, CSE's recruitment efforts are not limited to the national capital region, but also focus on hiring people from across Canada who have expertise in various fields. Furthermore, he noted that CSE is hiring not only people "willing to move to Ottawa" to work at CSE's headquarters, but also individuals who are interested in residing in regions across Canada and who are ready to support cybersecurity activities locally.

In highlighting that CSE is also trying to hire students, including those who have co-op placements at CSE, Sami Khoury emphasized that CSE is both modernizing its "multidisciplinary recruitment effort to attract the top talent" and "investing in a student program and a co-op program to make sure that [its] talent pool is rich." Moreover, he observed that CSE is "very engaged" in various communities "to raise cybersecurity awareness in presentations to students to get them interested in the [science, technology, engineering and mathematics] field[s]."

Alia Tayyeb added that there is "a great deal of interest" in CSE's activities, including in relation to cybersecurity, and contended that its recruitment efforts are going well. In her opinion,

> [w]ith [the Canadian Centre for Cyber Security] taking a more public profile, we have certainly developed greater inroads into the public in terms of awareness and that has translated into a great deal of interest in working here. We hire a variety of people from different technical fields; it's not all one type of profession. We have engineers, mathematicians, cybersecurity experts, etc.

That said, she recognized that CSE must remain competitive in order to continue to attract cyber experts, including through continuously innovating and ensuring that CSE is "keeping up with [its] competitors." For example, she drew attention to initiatives designed both to make "CSE an excellent place to work" and to help it "become a top employer in Canada," such as providing "an environment for people to be innovative" and fostering an "inclusive environment, where you can continually bring in new people to the sector who might not have considered it before, particularly women or individuals from different ethnic origins."

As well, Alia Tayyeb underlined that CSE has partnered with the CAF to address "force generation" issues and to develop "a new workforce to be interested in the cyber domain." She also pointed out that CSE works very closely with the U.S. Cyber Command to share information and lessons learned and to discuss cyber workforce strategies in terms of "building the expertise we need in order to have successful tools to meet the challenges of the future."

Rear-Admiral Carosielli focused on DND's and the CAF's cyber workforce recruitment and retention efforts in noting that the recruitment of cyber experts has been progressing well since the CAF created the Cyber Operator occupation in 2017. He explained that,

> [w]ith respect to cyber forces specifically, … within the last three years, we are meeting all of our [recruitment] intake goals for cyber operators. We have not had to provide any directed cyber-operator recruitment strategies because we have no issues getting the people in the doors. The Canadian Armed Forces are generating cyber-operators.

As well, he asserted that the CAF is making investments "in the growth of the cybersecurity force, from both a technical and a personnel perspective," and argued that the Cyber Operator occupation provides an "ability to recruit people out of high school" or "directly from industry or from other levels of academia, such as universities."

Notwithstanding these activities, witnesses made proposals aimed at strengthening federal efforts to be competitive in the labour market for cyber experts. Christyn Cianfarani, President and Chief Executive Officer of the Canadian Association of Defence and Security Industries, urged Canada to "consider … talent exchanges between the public and private sectors," similar to the United Kingdom's National Cyber Security Centre Industry 100 program, "to address the cyber-talent shortages we're all facing, because cannibalizing each other isn't going to work." According to the National Cyber Security Centre, the Industry 100 program facilitates close cooperation between the Centre and the private sector, bringing people together to enable greater understanding of cybersecurity, identify systemic vulnerabilities, discuss lessons learned, develop new ideas and reduce the impact of cyberattacks. Under the program, private-sector cyber experts can be seconded for a wide range of part-time job placements at the Centre, ranging from one day per week to one day per month, with participating private-sector organizations paying the salary of their staff while they are on the secondment.[11]

Christyn Cianfarani speculated that CAF "reservists with cyber and computing skills who are employed by companies could be an attractive way to support reconstitution of the CAF, so long as the government does not claim the [intellectual property] and patents that reservists create while employed in the private sector." Furthermore, she suggested that Canada could also rely on its veterans, many of whom are leaving DND and federal "security agencies" and who have both a security clearance and cybersecurity expertise. As well, she stated that another possible source of cyber experts is Canada's Five Eyes partners.

Similarly, Brigadier General (Retired) Turnbull encouraged greater cooperation between Canada's public and private sectors to find possible solutions to cyber workforce shortages. In emphasizing that the United Kingdom, the United States and other Canadian allies are "not shy to go to industry and engage in long term partnerships with industry leaders and to directly invest in emerging technology," Brigadier-General (Retired) Turnbull contended that Canada's federal departments and agencies "seem to want to resolve all issues internally." In his view, the "true cyber security leaders in Canada are not found in the Government or even in the CSE. They work in the telecoms industry, the financial sector, the retail sector and the full-time, persistent cyber security sector."[12] He mentioned that there is an "instinctive aversion to contracting for cyber security services" to strengthen the federal cyber workforces, stressing that "most departments [and agencies], including CSE and DND, insist on building and trying to sustain their own workforce within their own human resource systems." In his opinion, "the efficiency and effectiveness of this approach needs to be challenged."[13]

Dr. de Boer also provided suggestions designed to strengthen Canada's cyber workforce, suggesting—for instance—that the lack of cyber personnel has to be "complement[ed] with machines, with AI." In proposing that the Government of Canada should compensate for cyber workforce shortfalls by "immediately" ensuring that DND and the CAF, as well as other federal cybersecurity partners, are equipped with the latest AI-driven technologies, he argued that such "is not the case right now."

[11] United Kingdom, National Cyber Security Centre, "Industry 100."

[12] Document submitted to NDDN by Brigadier General (Retired) John Turnbull, 13 February 2023.

[13] Ibid.

Responding to Cognitive Warfare Threats

Witnesses advocated greater Government of Canada efforts to address foreign interference, disinformation campaigns and other cognitive warfare threats. Dr. Wark underscored that Canada should "be worried most about adversaries who are deliberating conducting disinformation campaigns and interfering in democratic practices," noting that—since 2016—there has been a great deal of concern about foreign interference in democratic elections. As well, he pointed out that foreign disinformation, misinformation and malinformantion campaigns are dividing populations, as well as eroding trust in governments and other established institutions in Canada and many other countries around the world. Moreover, according to him, much attention has recently been paid "to the ways in which foreign state adversaries can use cyber-tools to try to impact diaspora communities in Canada and among our allies."

In encouraging the Government of Canada to address cognitive warfare threats by exposing the state actors engaging in such activities and by responding publicly with facts, Dr. Wark indicated that:

> [t]he most important thing is to monitor and call them out publicly. Call them out as a form of deterrence for foreign state actors trying to use those tools, but also call them out to make sure that the Canadian public understands what's going on. … Public education is a critical part of the piece.

Marcus Kolga asserted that Canada, especially its armed forces, "might have some challenges in defending itself" in cyberwarfare situations. In recognizing that the CAF previously developed capabilities to defend itself against psychological warfare and foreign disinformation operations, he claimed that efforts to maintain and enhance those capabilities were "terminated" in 2020 after media sources reported "that the Canadian Armed Forces were preparing to use psychological warfare and information operations against Canadians." In his view, "since then, it doesn't appear that the Canadian Armed Forces have continued … those efforts to defend our forces" against psychological warfare operations and disinformation campaigns, with the result that the CAF currently lacks "the capabilities to defend against those sorts of information attacks." According to him, more should be done to help the CAF to defend itself against cognitive warfare threats.

Furthermore, in highlighting the National Security and Intelligence Committee of Parliamentarians, Marcus Kolga urged the creation of two all-party joint parliamentary committees: one to focus on cyber threats and another to concentrate on foreign disinformation. In his opinion, these committees should be non-partisan and should meet regularly to discuss and analyze various cyber threats and cognitive warfare threats, including "disinformation narratives," with a report made to committee members' respective caucuses about such threats.

Reforming Defence Procurement

According to witnesses, Canada's defence procurement should be reformed because the current process is too bureaucratic and slow, thereby limiting the extent to which the country has the state-of-the-art cybersecurity technologies and tools required to address ever-evolving cyber threats. Christyn Cianfarani advocated timely procurement of such technologies, with contracts awarded to Canada's expanding cybersecurity sector. She noted that, as a fast-growing global sector that is expected to surpass traditional information technology in terms of spending, the sector grew by more than 30% in Canada in terms of employment, research and development (R & D) activities and revenue between 2018 and 2020. That said, she emphasized that only 8% of the sector's revenue is derived from Government of Canada contracts, with "the sector sell[ing] three times as much to our Five Eyes allies …." In her view, the implication is that Canada's allies "see more value in Canada's cybersecurity sector than [the Government of] Canada does." She contended that the Government of Canada "needs to acquire more from [its] own industrial base, using procurement as a policy lever to drive innovation and build scale in Canadian businesses," and it "needs to procure at the speed of cyber."

As well, Christyn Cianfarani cautioned that, with cybersecurity innovation cycles that are "measured in months, sometimes weeks," a slow defence procurement process is a "recipe for buying out-of-date or obsolete technology," adding that "time is the enemy" concerning cybersecurity. In her opinion, Canada's existing defence procurement practices and procedures are too slow to keep pace with the rapid evolution of cyber threats and constant developments in cybersecurity technologies. She pointed out that these practices and procedures should be more agile and proposed that there should be an increased opportunity for sole-source contracts with Canadian firms. She contended that:

> [t]here is a time and a place for competition. Typically, nations compete when there are two foreign vendors and there is no Canadian incumbent. … When there is a Canadian incumbent—and what we're talking about here on the cyber side is that you would want to have an already trusted, curated Canadian business that you are prepared to deal with—then in that particular case, sole-sourcing is not and should not be viewed as a shortcut to the process. It should be a solution.

According to Christyn Cianfarani, “most nations use the process of sole-sourcing or agile procurement to sustain, maintain and grow their businesses within their own country, meaning that national security is economic security.” She added that those nations “fundamentally understand that by investing in a [domestic] company, and by doing that in an agile way with trusted sources or trusted individuals,” they are “effectively … investing in [their] economy.”

To improve and expedite the defence procurement process, Christyn Cianfarani encouraged the Government of Canada to consider the following three proposals by the Canadian Association of Defence and Security Industries that are outlined in its 2021 report entitled *Procurement at Cyber Speed*:

> You start to create these umbrella projects that procure [cyber] capability. … So you have trusted partners and there is a capability development and sustainment that is resident within a country, and you allocate funding at an umbrella level. The other thing you could do is have more flexible funding. Right now, we have a whole approvals process. It goes through Treasury Board and there are about 200 steps. … You would get rid of [those steps] … and you would consider a vote of funding [for high-technology acquisition] that has the flexibility of Vote 1 and the ability to acquire new capability of Vote 5. Then, the last thing you could do is fast-track the approval and contracting process by … setting guidelines, which is where you have technology and services made by Canadian nationals with Canadian security clearances and trusted, curated Canadian businesses where taxes are paid in Canada and [intellectual property] rests in Canada.

Similarly, Glenn Gulak, Chief Executive Officer of Lorica Cybersecurity, argued that cybersecurity must be a priority, with procurement accelerated—whenever possible—to “move at the speed of cyber-threats.”[14] He referenced a recent Innovation, Science and Economic Development Canada study indicating that, on average, Canadian cybersecurity firms generate 69% of their revenue from domestic sales—including federal, provincial, territorial and municipal governments, as well as other public-sector clients, and the private sector—and 31% of revenue from export sales.[15] In his view, the Government of Canada should invest in Canada’s cybersecurity sector, and should develop a more streamlined procurement process to accelerate the acquisition of cybersecurity technology and tools.

Glenn Gulak drew attention to Shared Service Canada’s Cyber Security Procurement Vehicle program, which—in his opinion—seeks to enable the Government of Canada and the private sector to respond quickly to cyber threats, as well as to simplify and

[14] Document submitted to NDDN by Glenn Gulak, Chief Executive Officer (CEO) of Lorica Cybersecurity Inc., 24 March 2023.

[15] Ibid.

accelerate the procurement of technologies relating to cyber and information technologies. He explained that the program creates “a Secure Supplier Ecosystem that can quickly deliver enterprise-scale cybersecurity solutions to meet the specific needs of government departments and agencies.” According to him, the program is an example of agile procurement regarding the cybersecurity capabilities and technologies that are required to protect Government of Canada systems and networks against cyber threats.[16]

Enhancing Global Cooperation

Witnesses encouraged greater efforts to enhance cybersecurity cooperation between Canada and its allies. In mentioning her research, Kristen Csenkey said that the “specific cybersecurity threats are understood differently” among the Five Eyes countries, speculating that the “discrepancies in understanding [these threats] will have an impact on the roles and responsibilities of actors involved in addressing these threats.” In her view, those discrepancies provide Canada with an opportunity “to lead on this issue area within the Five Eyes,” which the country could do by “addressing and understanding certain cybersecurity issues, such as the quantum [computer] threat.” She noted that, according to her research, there are differences “in how this [quantum computer] threat and its intentions, associated technology, users and potential threat actors [are] understood in policies” among the Five Eyes countries. In her opinion, Canada could be leading a “Five Eyes quantum consortium.”

As well, witnesses urged Canada to emulate other countries’ actions concerning cybersecurity. Dr. Leuprecht highlighted that several countries have cybersecurity ambassadors to promote cybersecurity issues domestically and globally, with Denmark being the first country to create such a position and the United States having done so as well. According to him, the lack of a Canadian cybersecurity ambassador “shows that the way we think about the field of cybersecurity could be updated.” He asserted that a Canadian cybersecurity ambassador should be appointed “to build links with the private sector and different stakeholders around the world, who may not be in a country per se.” In elaborating about this role, he stated that:

> [t]he field of cybersecurity is very widely distributed geographically, and establishing direct contacts requires effort. The purpose of embassies and ambassadors is to provide the government with open information. … The Canadian government currently does not have enough open information about the different stakeholders and private actors in this field. A cybersecurity ambassador would allow us to build relationships with these

[16] Ibid.

> important players who, in several cases, are more powerful than many of our mid-power partners.

Likewise, Dr. de Boer advocated the appointment of a Canadian cybersecurity ambassador to enhance domestic cybersecurity efforts and to ensure greater collaboration between the public and private sectors. He outlined various roles for such an ambassador, suggesting that:

> [t]he primary role of such an individual … would, first of all, be to signal to all Canadians that cybersecurity is important. Second, it would be one individual empowered with ensuring policy coherence and program coherence across Canada. Currently, that does not exist. … The role would be to look across the Government of Canada to ensure coherence and unity of effort and to unify our approach to defending the country.

Developing International Legal Frameworks in Cyberspace

Witnesses underscored the lack of international legal frameworks governing cyberspace and cybersecurity. Alexander Rudolph argued that "no norms or international laws currently exist to address cyber-conflict and cyberwarfare." In agreeing, Dr. Leuprecht contended that, for two decades, "cyber-diplomacy has largely failed to generate broad agreement on international norms to constrain malicious behaviour by state-based and state-tolerated actors in cyberspace." In his view,

> [w]e've tried for 20 years to build norms and consensus around this, and we've made very little progress within the [United Nations] and within other bodies. What you need to understand is that there are people who believe in the liberal rules-based international order—that's about 57 countries—there are countries that are agnostic, and then there's a subset of countries that simply do not believe in that order, so we will never get an international cyber-governance regime, at least not in the foreseeable future.

Dr. Leuprecht emphasized that, because of the lack of international norms and consensus in cyberspace, the best way for Canada and its allies "to deter and constrain bad behaviour" is to "engage" against malicious state and non-state cyber threat actors using "offensive cyber-measures."

Witnesses stressed that Canada should encourage the development of international norms and frameworks for addressing threats in cyberspace. Dr. Wark observed that there is a need to codify cyberattacks as a war crime in international law, commenting that—at present—"it's not clear in the international law" if a cyberattack on a foreign nation constitutes an act of war. In his opinion, Canada should "take a lead … in terms of international law developments" in this area. He indicated that Ukraine is promoting "a clear designation of cyber-attacks on civilian critical infrastructure as a war crime" and "accountability for such crimes." He encouraged the Government of Canada to "support the Ukrainian position" and to "take a lead role" in advocating globally "to designate cyber-attacks on critical infrastructure as a war crime in international law and assist Ukraine to pursue accountability."

As well, witnesses urged the development of domestic legislation concerning foreign cyberattacks. Aaron Shull said that the Government of Canada should "establish a clear and concise legal framework for dealing with cyber-attacks that includes guidelines for attribution, response and liability." According to him, "the governance structure should be nimble and responsive to the fast-changing environment," and the "regulations should be expert-driven, focusing on sound policy and not good politics." Furthermore, he mentioned that the Governor in Council "should be able to approve standards, codes of practice and certification programs to act as an integrated compliance mechanism."

Moreover, witnesses asserted that Canada and its allies should apply sanctions as a response to foreign cyberattacks. Dr. Wark noted that Ukraine is currently asking the international community to use "sanctions to undermine the cyber-capabilities of an aggressor." He proposed that Canada, along with its allies, should apply "targeted sanctions to undermine Russian state and proxy cyber-capabilities," and should also "continue to document and publicly call out Russian cyber-aggression against Ukraine and NATO." In agreeing, Marcus Kolga added that sanctions should not be limited to cyber threats, but should also be applied in relation to disinformation campaigns and other cognitive warfare threats. He asserted that the Government of Canada "could be using [its] sanctions regime to greater effect to target Russian propagandists, the ones who … target Ukraine and that target Canadian interests as well" with their disinformation campaigns.

STRENGTHENING CANADA'S CYBER RESILIENCE

Cybersecurity in Canada remains complex and challenging, and it requires ongoing vigilance. The cyber threat environment is constantly evolving, with new and more sophisticated cyber threats emerging daily, and state and non-state actors increasing their use of emerging technologies—like artificial intelligence and quantum computing—for malign purposes. It is critically important that countries, their governments and their residents understand cyber threats, and have the right knowledge and other capabilities to deter and defeat them.

Witnesses identified a number of challenges and ways in which to strengthen cybersecurity in Canada, keep the country protected in cyberspace, and build resilience against cyber threats and cyberattacks. In underscoring that preparing Canada for the cyber threat environment of tomorrow must begin today, they focused on protecting critical infrastructure, enhancing Government of Canada–private sector collaboration, reporting cyber incidents, establishing cybersecurity standards for the private sector, creating incentives for private-sector investments in cybersecurity, investing in cyber-related R & D, increasing public outreach, education and training, and safeguarding individual privacy and civil liberties.

Protecting Critical Infrastructure

Critical infrastructure underpins many everyday services, and compromising it could have a debilitating effect on safety and security in Canada. It includes physical assets, information technology and electricity distribution networks, and banking, manufacturing, transportation and government systems. Released in 2010, Canada's *National Strategy for Critical Infrastructure* identifies 10 critical infrastructure sectors,[17] with defence and security included in the "government" sector. Responsibility for protecting critical infrastructure is shared among the federal, provincial and territorial governments, as well as the private sector, which owns and operates most of this infrastructure.

Canada's critical infrastructure faces risks because of the digitization of systems and processes. The *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure* states that "Canada's critical infrastructure remains a high value target for foreign interference, including for the purposes of intentional service disruptions and intellectual property theft." It also notes that the high level of interconnectedness across sectors means that disruptions in one sector could have cascading effects in others, which could significantly interrupt essential services.

In the view of witnesses, there is a need to protect Canada's critical infrastructure. Tadej Nared said that—worldwide—attacks on critical infrastructure "are growing daily," and provided the example of Russia's attacks on critical infrastructure in Ukraine, elsewhere in Europe and around the globe in recent years. In elaborating, he observed that the Russians are "compromising systems, power plants, hydroelectric power plants, electricity grids and civilian infrastructure from hospitals to everything else." He expressed concern that "western countries, NATO countries, are not protecting their

[17] Canada's 10 critical infrastructure sectors are: energy and utilities; finance; food; transportation; government; information and communication technology; health; water; safety; and manufacturing. See Public Safety Canada, *National Strategy for Critical Infrastructure*, 2010.

infrastructure in the manner that they should be," which is a "huge problem" that "should be addressed promptly."

Brigadier General (Retired) Turnbull speculated that, "in a true cyber war, it is the critical infrastructure and economy of Canada that [will be] the target." Adding that the CAF is not responsible for protecting critical infrastructure, he commented that DND and the CAF have "little capability in [the cyber] battlespace other than to protect" themselves, their systems and their network. In his opinion, it is Public Safety Canada, the country's other national security agencies and the private sector that "need to prepare for and fight this battle."[18]

Witnesses drew particular attention to the cyber threat that Russia poses for critical infrastructure. Sami Khoury characterized Russia as "a formidable cyber-player," emphasizing that "we've seen the extent of its capabilities in Europe, or at least in Ukraine, with the deployment of cyber-capabilities that are destructive in nature" and noting that Russia has shut down Ukraine's power grid twice. In contending that CSE is "very concerned" about the security of critical infrastructure in Canada, he stated:

> That's why we work with critical infrastructure providers in Canada to make sure they are taking every precaution or every measure to protect themselves and their networks from those kinds of cyber-threats. Everything we learn, everything we see in Ukraine and everything we learn from what Russia is doing around the world we try to promulgate through cyber-flashes and other information bulletins to Canadian businesses.

Marcus Kolga highlighted similar concerns, arguing that—at the moment—"the greatest threat from Russian cyber-operations are obviously those areas of critical infrastructure." Pointing out the vulnerability of Canada's critical infrastructure to cyberattacks, he mentioned that, several months ago, Canada's health sector was "prey to ransomware," and underlined that "a lot of the … organizations that engage in criminal activity such as ransomware are in Russia" and operate "with the blessing of the Kremlin." According to the Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023–2024*, more than 400 healthcare organizations in Canada and the United States have experienced a ransomware attack since March 2020. For example, in October 2021, Newfoundland and Labrador's healthcare system was affected by a cyberattack that disrupted medical services, and compromised networks and sensitive information. Marcus Kolga suggested that there is "a threat to health and other critical infrastructure from Russian operators," who have "demonstrated very clearly" in Ukraine that "they will not hesitate to attack critical infrastructure."

[18] Document submitted to NDDN by Brigadier General (Retired) John Turnbull, 13 February 2023.

Witnesses encouraged Canada to do more to protect its critical infrastructure. In comparing Canada's current investments in critical infrastructure to those in the United States, Dr. Wark stressed that "we have a long way to go in deciding what we want to do about critical infrastructure." In his view, Canada is still "waiting for a critical infrastructure strategy." He outlined the following actions concerning the development such a strategy:

> The starting point is going to have to be to decide what we mean by "critical infrastructure." Once we've done that … then we can think about regulating the terms under which critical infrastructure functions … in terms of, particularly, cybersecurity strategies.

As well, witnesses drew attention to the need to improve the extent to which Canada's defence industrial base is protected against cyber threats. Christyn Cianfarani said that, although the Canadian Centre for Cyber Security is currently focused on critical infrastructure, it is "starting to look at the defence industrial base, which includes the manufacturing component." Regarding cybersecurity and risks to Canada's defence and security industry, Tim Callan underscored that "defence manufacturing is critical to the defence infrastructure," and commented that state-sponsored actors can harm Canada and its defence industrial base through cyberattacks designed to disrupt systems, as well as steal vital information and secrets, through cyber espionage. In observing that more should be done to mitigate those risks, he proposed that Canada should "build a security fortress" to protect its defence industrial base, which is strategically important to the country's national security and defence.

However, witnesses mentioned that too much attention is being given to the vulnerability of Canada's critical infrastructure. According to Alexis Rapin, "[c]yberattacks on critical infrastructure are a high-risk but unlikely threat." He explained that, because such attacks are a high-risk threat, "you have to think about them, prepare for them and have plans in place in case they happen." However, he contended that cyberattacks on critical infrastructure "remain fairly unlikely," asserting that "very few … have actually materialized in Canada." In his opinion, there should be a greater focus on the "more subtle, less serious" cyber threats that "are repeated and occur on a daily basis" and that affect systems and networks—but not necessarily critical infrastructure—across Canada.

Enhancing Government of Canada–Private Sector Collaboration

Witnesses highlighted the need to enhance collaboration between the Government of Canada and the private sector concerning cybersecurity. Christyn Cianfarani argued that "Canada requires a much greater degree of collaboration, co-operation, knowledge sharing, and co-development between government and the private sector." In acknowledging that "some positive steps have been taken towards this," she indicated that "we're nowhere near where we need to be." She described federal agencies like CSE as "very capable" concerning cybersecurity, but emphasized that the Canadian Association of Defence and Security Industries' "research has shown that our government is falling behind our allies when it comes to working with the private sector in an institutionalized way." According to her, the private sector—which owns and operates 85% of Canada's critical infrastructure—is a key cybersecurity player and has the "very important role" of securing its own infrastructure from cyber threats.

More specifically, Christyn Cianfarani encouraged the Government of Canada to increase its collaboration with Canada's defence and security industry, noting that "about 60% of the industry has capability in securing networks and data infrastructure," which "can be for networks in threat environments, and … can also be for sensors and assets like planes, ships and tanks that operate in networked environments, as in the Canadian Armed Forces, as well as the infrastructure." She added that the Canadian defence and security industry is also "very strong in niche areas like encryption, penetration testing and threat monitoring," as well as in maintaining, operating and deploying satellites and other space-based assets that are "used for intelligence collection and targeting."

Moreover, Christyn Cianfarani underlined that Canada's defence and security industry has cybersecurity "talent and expertise within [its] organizations," and is "continuously developing and innovating" in that field, with the result that it "can bring that competency to the [federal departments and] agencies in order to keep them on the bleeding edge of what is available to protect Canada and Canadian society as well." In her view, the Government of Canada should leverage those private-sector cybersecurity resources and would benefit from "collaborative exchange" with Canada's defence and security industry.

According to Dr. de Boer, "improving public-private collaboration on cybersecurity should be a priority." In particular, he suggested that "foster[ing] proactive collaboration between government and the private sector at the operational level" would "help close gaps in our situational awareness, foster incident response playbooks that are aligned and help create a culture of proactive collaboration." Furthermore, he advocated "a joint collaborative environment or a joint cyber-defence collaborative" that would be a cybersecurity communication and information exchange channel between the public and private sectors.

Similarly, Christyn Cianfarani commented that "Canada needs improved systems for threat sharing that combine open sources [of information] with government and industry sources of information about breaches, indicators and potential responses," arguing that this approach would involve "rationalizing what is unclassified and what remains classified and who has access to what." In her view, there should be greater sharing of information about cyber threats and breaches "in a proactive disclosure manner" and "in an institutionalized way" in order that "we can leverage the technologies and agencies in order to get the best protections."

Moreover, Christyn Cianfarani contended that the Government of Canada should "establish a recurring forum for dialogue and discussion on cyber issues with all the key players … at the table," specifically mentioning the private sector, CSE, the Canadian Centre for Cyber Security, DND, the CAF, Global Affairs Canada and Public Safety Canada. In agreeing, Aaron Shull proposed that the Government should "establish an annual multistakeholder platform for collaboration and engagement on cybersecurity issues," with this platform including "participants from all levels of government, [the] private sector, Indigenous communities, academia, not-for-profits, law enforcement [entities] and industry leaders."

Witnesses criticized the current "rigidity" of security clearances and urged a reduction in the extent to which information is classified in Canada in order to ensure greater collaboration and information sharing between the Government of Canada and the private sector. Christyn Cianfarani highlighted the existence of a tendency to overclassify information in Canada, adding that—within federal departments and agencies—there appears to be a "fear of what people will do with that information and whether it will come back to harm us." According to her, "Canadians by nature, along with our government institutions, are a bit more risk-averse than our allies are," and the current rigidity of security clearances hinders the sharing of vital information between the Government and the private sector about cyber threats. She explained that:

> [w]e take a view in this country that we want the fewest security clearances possible. We think that clearing fewer people will make us safer, meaning that fewer people having access to that kind of information and knowledge will make us a safer country, because there will be perhaps fewer leaks or things like that.

In providing an international comparison, she noted that the United Kingdom, the United States and other countries have "taken a very different approach," pointing out that they are now "declassifying information in real time" in order to "make the public more aware." In her opinion, the "lens" through which security clearances are granted in Canada "needs to change," and "the idea that we need to keep people out instead of bringing people in and making them more aware needs to change."

Similarly, Dr. Leuprecht claimed that Canada is overclassifying information, and indicated that a lot of information should be declassified and shared publicly. In his view,

> [o]ne of the things we do in Canada is constantly and vastly overclassify material: 90% of the material we classify we probably don’t need to classify. The 10% of material that remains we absolutely need to protect at all costs. What we’re currently doing is classifying way too broadly instead of targeting our protection, our resources, to make sure that those elements that must never reach the outside are actually protected. Recent discussions over leaks show that, indeed, we have a lot of work to do.

Sami Khoury stressed that “each [federal] department has a departmental security officer,” with a “community” of them meeting regularly to discuss security classification issues. He characterized the Treasury Board of Canada Secretariat as the “policy arm” of this community, and mentioned that CSE does not audit other federal departments and agencies to assess their handling of classified information. According to him,

> [w]e come up with the various information security standards that are out there: protected A, protected B, protected C. We communicate those standards. They are sort of promulgated through Treasury Board. With each of these levels of classification, departments are aware of what information is classified as protected B or protected C, or what is secret and what is top secret. The departments themselves have to live by those standards.

With the goal of enhancing the sharing of information with the private sector, witnesses encouraged the Government of Canada to stop working in silos and to adopt a more uniform approach concerning cybersecurity. In particular, Christyn Cianfarani said that working in silos “greatly hinders our co-operative effort,” and contended that “government agencies provincially and municipally, and actually across the federal government, [are] not harmonized on approaches or information and threat sharing.” As well, she drew attention to the existence of silos in the private sector, which are “a hindrance to this country,” especially regarding cybersecurity. In proposing that breaking down silos would help the private sector “to be more cyber-aware” and to be better protected in cyberspace, she underscored that,

> [o]ur siloed approach means we look after ourselves. The agencies look after the government. The CAF looks after the CAF, and industry looks after itself. What we’re learning is that the approach we use is not working.

Reporting of Cyber Incidents

Witnesses suggested that it should be mandatory for the private sector to report cyber incidents to the Government of Canada, and more specifically to the Canadian Centre for Cyber Security. In Sami Khoury’s opinion, ransomwares are a “serious threat” to the private sector and many organizations fall prey to such cyberattacks, although they often do not report them. In mentioning that CSE is working with the private sector to mitigate and to address the threat of ransomware, he emphasized that the Canadian Centre for Cybersecurity "constantly publish[es] alerts and cyber-flashes to draw attention to what may be new vectors of ransomware or new techniques that cybercriminals are using in ransomware." As well, he stated that "every time" CSE has an "opportunity to speak to a business community, [it] speak[s] about the threat of ransomware," adding that, when CSE receives tips from cybersecurity partners about possible incoming cyberattacks directed against private-sector organizations, CSE alerts "the [targeted] organization" so that it can protect itself in advance of the attack.

However, Sami Khoury highlighted that "there is no requirement for the private sector to report to [CSE or its Canadian Centre for Cyber Security concerning] ransomware incidents, and many [private-sector organizations] don't report [them]." He noted that, in 2021, the Canadian Centre for Cyber Security received only 300 reports of ransomware incidents, "which is probably under-reporting." In focusing on CSE's offer of assistance to private-sector organizations that have experienced a cyberattack, he commented that the offer is "sometimes … accepted, but more often it's declined," which is an outcome that needs to change.

Christyn Cianfarani supported the Government of Canada using both "sticks and carrots" to ensure that the private sector reports cyberattacks and cybersecurity breaches, with the goal of "mak[ing] us better and more secure in the overall ecosystem." In her view, many private-sector organizations do not report cyber incidents voluntarily or proactively because they fear "that their brand or their business [will be] damaged in the process," so the "sticks" could compel them to "disclose their breaches." With a focus on "carrots," she advocated outreach and education that would increase awareness and security in cyberspace through identifying the benefits of reporting, such as access to information about cyber threats and about other organizations' vulnerabilities and lessons learned from cyberattacks against them. According to her, if the Government wants to compel private-sector organizations to report cyber incidents, it should invite them to do so in "an effective way" that does not damage their brand or their business, and that provides them with information designed to help them become more secure in cyberspace.

In agreeing, Kristen Csenkey argued that reporting cyber incidents should be mandatory for the private sector, and outlined such advantages as the following:

> Especially for [small and medium-sized firms], or companies in that category, to have a mandatory reporting for cyber-attacks would help us understand the breadth of the situation. It would also provide us with more information so that we can come up with a

> better threat assessment, risk assessment and framework to better protect certain industries and private sector companies.

Alex Rapin concurred, and asserted that mandatory private-sector reporting of cyber incidents should occur as “a best practice.” Marcus Kolga also indicated that cyber incidents should be reported, mentioning that “we should [not] be sweeping [incidents] under the rug. That way we’ll have a better understanding of where the threat is.”

Establishing Cybersecurity Standards for the Private Sector

Witnesses contended that the Government of Canada should promote the development of cybersecurity standards for the private sector. In particular, Aaron Shull proposed that the Government should “incentivize companies to adopt the latest security measures” and standards, and drew attention to the CyberSecure certification program for small and medium-sized firms established by CSE and Innovation, Science and Economic Development Canada. In describing the program as a positive measure, he also encouraged additional actions because the program—which “provides a high level of protection”—has had limited adoption.

Christyn Cianfarani suggested that, because of their degree of integration, the Canadian and U.S. industrial bases should have more collaboration and standardization regarding cybersecurity standards. In her view,

> [t]he Americans are, not surprisingly, ahead of us. Very soon, a demanding and mandatory cybersecurity standard will start appearing in Pentagon defence contracts. This is known as the Cybersecurity Maturity Model Certification, or CMMC. … Canada should adopt this standard by reference. CMMC will likely become a de facto Five Eyes, if not global, standard for defence firms.

Furthermore, she said that “fifty per cent of the [Canadian] defence industrial base exports … go to the United States. If we want to be a trusted partner in an American supply chain, we will need to be moving in lockstep with them to ensure that we can be trusted partners and that they will be able to procure from us.”

According to Christyn Cianfarani, Canada—particularly the Canadian Embassy in the United States, Public Safety Canada, DND and Public Services and Procurement Canada—are examining the CMMC “right now.” However, in her opinion, “they’re trying to understand whether the standard needs specific ‘Canadianization’,” which should not occur because doing so would lead to “Canadianized portions” of the standard and to higher costs for Canadian firms, which would “have to have two standards.” Moreover, she speculated that, “if we don’t get it right, the Americans could be moving forward and Canadian companies could be waiting for the Canadian standard and therefore be left behind" because they would be unable to bid for U.S. defence procurement contracts. She commented that "taking time to contemplate a separate standard in Canada could become a competitive disadvantage for us and a non-tariff trade barrier."

Creating Incentives for Private-Sector Investments in Cybersecurity

Witnesses urged the Government of Canada to provide incentives to private-sector organizations, especially to those that are small or medium in size, to encourage them to invest in cybersecurity. Dr. de Boer noted that, according to a 2021 Insurance Bureau of Canada survey,[19] 47% of respondents that were a small or medium-sized firm said that they "had invested zero dollars in cybersecurity." He underlined that those firms are very vulnerable to cyberattacks, and are prone to being the target of cyber espionage and intellectual property theft. In his view, because high costs are limiting cybersecurity investments by Canada's small and medium-sized firms, the Government of Canada should "incentivize these [firms] to protect their [intellectual property]," as well as their systems and networks.

Similarly, Aaron Shull advocated the creation of a federal tax credit that would provide the private sector with an incentive to invest in cybersecurity, which—in turn—would "help increase the overall level of cybersecurity in the country and reduce the risk of cyber-attacks on businesses." He highlighted that cyberattacks on the private sector result in significant financial losses, damage to reputation and disruption of operations.

Investing in Cyber-Related Research and Development

Witnesses focused on the need for Canada to invest in cyber-related R & D to ensure that the country can respond to new and emerging cyber threats. Dr. de Boer asserted that "we have to continually invest in [this area] … to ensure that we outpace our rivals." That said, he added that "we are laggers when it comes to R and D investment," explaining that—at the moment—Canadian firms, especially those that are multinational, benefit much more from undertaking R & D outside of Canada because other countries have "much more collaborative support systems in place." According to him, a "concerted partnership" between the Government of Canada and the private sector concerning cyber-related R & D is needed in "niche areas where Canada has a comparative advantage."

[19] See Insurance Bureau of Canada (IBC), "Many Small Businesses Vulnerable to Cyber Attacks," 2021; and Leger, *IBC Small Business Cyber Security Survey Report*, 17 August 2021.

In Dr. de Boer's opinion, the Government of Canada could foster cyber-related R & D through assisting the private sector with the "commercialization" of relevant domestically developed technologies. He elaborated by indicating that:

> [t]here's a lot of what we call lower TRL—Technology Readiness Level—or very initial-stage R and D that takes place in Canada, but then, after it passes this initial stage, it goes through something called the valley of death, which means that it's very difficult to productize this R and D here in Canada. There are very few programs, for instance, that support Canadian companies to help launch initial products to test them and get them to market.

In contrasting the situation in Canada with that in the United States, Dr. de Boer noted that the United States has "systems in place to help companies through that valley of death to help commercialize their products." He proposed that the Government of Canada should "establish a Canadian commercialization fund that would help Canadian companies move towards that productization."

In Glenn Gulak's opinion, the Government of Canada must find ways to enhance its engagement with Canadian private-sector leaders and to encourage innovative cybersecurity solutions. He suggested that those engagement efforts could take the form of "more regular showcases that generally highlight government areas of interest, more innovation challenges and paid pilot programs, and more streamlined procurement … to get cutting-edge, Made-in-Canada solutions integrated quickly in Government of Canada operational systems." He described these efforts as "an economic and security imperative that will protect Canadian prosperity, values and well-being in an increasingly uncertain future."[20]

Increasing Public Outreach, Education and Training

In the view of witnesses, Canadians should be provided with greater public outreach, education and training about cyber threats and cognitive warfare threats. In contending that "the human being is always the weak link in every digital system," Tim Callan argued that "it's very easy to build mathematically pure cryptographic solutions that can't be defeated" but underscored that it is "much harder to teach people not to fall for tricks." He advocated "social engineering" training, which would focus on cyber hygiene, as well as increased awareness of cyber threats and cognitive warfare threats.

Dr. Wark said that the Government of Canada should provide more cybersecurity outreach, education and training. He commented that CSE's "training systems" could be

[20] Document submitted to NDDN by Glenn Gulak, CEO of Lorica Cybersecurity Inc., 24 March 2023.

“migrate[d]” to other federal departments and agencies, as well as to the private sector” in the future.

Marcus Kolga agreed that there is a need to educate Canadians about cyber threats and to ensure that those working in government, other areas of the public sector and the private sector “have strong cyber hygiene skills, including using strong passwords.” In his view, “that's where we need to start in order to protect the critical infrastructure and other organizations in Canada.”

As well, Marcus Kolga drew attention to public outreach, education and training—“non-partisan” and with a “whole-of-society” approach—as an important element of any national effort to combat foreign interference and disinformation campaigns. He identified several countries that combat foreign interference and disinformation campaigns using these public measures, noting such “frontline countries” as Estonia, Latvia and Lithuania, all of which both share a border with Russia and have been the target of Russian interference and disinformation. He also stated that Taiwan “is doing an exceptional job in combatting Chinese disinformation,” and stressed that Finland and Sweden “have adopted early childhood education programs … to make sure that all future generations of Swedes and Finns have the cognitive resources necessary to critically assess the information they're consuming.”

Furthermore, Marcus Kolga urged Canada to emulate the best practices of other countries in providing the entire population with cyber-related public outreach, education and training, including in relation to cognitive warfare threats. According to him, “there needs to be broader awareness in general for all Canadians so that they can recognize information operations and defend themselves against them.” He also highlighted a need “to develop [a] capability to directly address” the “narratives” of disinformation campaigns and to “challenge them and push back on them” publicly.

Safeguarding Individual Privacy and Civil Liberties

A witness raised concerns about issues relating to individual privacy and civil liberties in the cybersecurity context. In Tim McSorley’s opinion, it is “vital that Canada take steps to modernize cybersecurity laws to protect the private information of Canadians and the information infrastructure on which we rely.” In recognizing that, “as cyber-attacks increase in activity and sophistication, Canada must take steps to defend itself,” he cautioned that “these actions must not come at the cost of accountability and transparency of government activities, including those of the CSE.”

Tim McSorley asserted that the “overly broad powers” given to CSE and other federal national security organizations, as well as the “extensive secrecy” under which they tend to operate, could lead the individual rights of Canadians to be violated. In his view, such violations could have “real-world impacts,” particularly when the information about individual Canadians is shared with foreign governments. He acknowledged that the *Communications Security Establishment Act* requires that CSE not target Canadians, but observed that CSE collects signals intelligence and various types of information—including some that “may relate to [individual] Canadians”—in carrying out its work relating to cybersecurity. He mentioned that, in those situations, CSE is not “targeting [individual] Canadians.” However, according to him, CSE is “incidentally collecting that information and retain[ing] it, and it is still used in other ways.” He argued that, when Five Eyes countries and other jurisdictions have access to information about individual Canadians, “Canada loses control over how the information may be used, including in ways that can result in rights violations, abuse and even torture.”

As well, Tim McSorley expressed concerns about CSE’s dual mandate—signal intelligence and cybersecurity—and warned that these two distinct areas “do not exist in a silo.” He advocated amendments to the *Communications Security Establishment Act* and Bill C-26 that would establish “strict separations” between CSE’s activities in these two areas, including restrictions on information sharing. Furthermore, he suggested “that greater restrictions [should] be placed on [CSE’s] collection, retention and use of both metadata and so-called publicly available information,” and supported stricter requirements concerning “foreign intelligence and cybersecurity authorizations, as well as approvals of active and defensive cyber operations, to ensure the CSE’s compliance with its obligations towards oversight and review bodies.” In proposing that CSE should “immediately implement a system to allow [the National Security and Intelligence Review Agency] to access its records,” he also urged “a full review” of CSE’s active and defensive cyber activities, “with a particular view to compliance with international law and Canada’s role in escalating the promulgation of cyberwarfare activities.,” and a review of CSE’s “international mass surveillance activities,” with a view to “restrict[ing]” such activities.[21]

Regarding oversight, Tim McSorley encouraged more oversight of CSE and other federal departments and agencies engaged in cybersecurity with the goal of ensuring greater public trust in their activities. He underlined that “oversight and review are simply not only about putting organizations on the defensive and calling them out but also seeing where we can learn from our errors and improve the operations.” In his opinion, “there needs to be openness and transparency to the degree that we understand what

[21] Document submitted to NDDN by the International Civil Liberties Monitoring Group, 6 April 2023.

Canadian agencies, including the CSE, are engaging in when they are engaging in protecting Canada's cybersecurity, engaging in active and defensive cyber-operations and engaging in signals intelligence." According to him, openness and transparency could be achieved through "greater mandatory reporting around the activities that they're carrying out."

Alexander Rudolph shared similar views and contended that there is a need for greater transparency in the field of cybersecurity in Canada. As he indicated:

> I will completely agree that there is a need for more transparency, I'd say, across the board on Canadian cyber-defence policy. Most of my research is from looking at audits and looking at departmental results. … As much as I know broad themes, there are still a lot of gaps in my knowledge. That's simply because the Canadian Armed Forces doesn't want to tell you and because they are prevented from doing so.

Moreover, Tim McSorley drew attention to the lack of a federal oversight body with the responsibility to examine cybersecurity in Canada. In noting the oversight activities of both the Intelligence Commissioner of Canada and the National Security and Intelligence Review Agency, he commented that "it's not clear that they have a role in reviewing Canada's cybersecurity operations, because they touch on national security but not necessarily in the way that those bodies always review it." In his view, either amendments should be made to their mandates to "clarify that they do have [a] mandate" to investigate cybersecurity operations or a new position should be created with a specific mandate to oversee cyber activities.

THE COMMITTEE'S THOUGHTS AND RECOMMENDATIONS

The cyber threat environment is constantly evolving. Every day, new and more sophisticated cyber threats are developed and used by malign state and non-state actors to achieve a variety of objectives. Canadians live in one of the most interconnected countries in the world, and they increasingly depend on digital technologies, systems and networks. They are using the Internet for work, education, health care, banking, shopping, entertainment and social interactions, among other activities. In addition to underscoring the importance of affordable and reliable Internet connectivity, the COVID-19 pandemic accelerated the adoption of digital technologies that facilitate telework, remote education and contact tracing in relation to exposure to the COVID-19 virus. Today, Canadians are much more vulnerable to cyber threats than they were even half a decade ago.

Rapid changes in the global security environment in recent years have led many countries to make unprecedented investments in security and defence, including in their armed forces. The return of global power competition and the increasingly aggressive actions of certain authoritarian, revisionist and expansionist states—such as China and Russia—have resulted in growing tensions between and among countries, and they have caused instability and conflict in several regions of the world. As part of their investments in security and defence, Canada and its allies have partly focused on protecting their digital systems and networks against foreign cyber threats, and on preparing their security forces and militaries to operate and prevail in today's cyberspace.

The Committee agrees that cybercrime is the primary cyber threat affecting Canadians, but the state-sponsored cyber programs of Russia, China, Iran and North Korea continue to pose the greatest strategic cyber threat to Canada. Russia's use of cyberattacks alongside its kinetic military operations directed against Ukraine over the last year demonstrates the extent to which cyberspace has become a new domain of warfare and cyberwarfare a new reality of war in the 21st century. As well, the emergence of cognitive warfare threats is a growing problem.

Like others, the Committee believes that protecting Canada against cyber threats and cognitive warfare threats is a whole-of-society effort. All levels of government, other public sector entities, the private sector and every Canadian must contribute to cybersecurity. The Government of Canada plays an important role, with a dozen federal departments and agencies—including CSE, DND and the CAF—engaged in cybersecurity efforts under the leadership of Public Safety Canada. In addition to domestic efforts, international collaboration and cooperation are key to protecting against cyber threats and cognitive warfare threats.

The Committee concurs that ongoing federal efforts are needed to ensure that Canada is both at the forefront of emerging digital technologies and focused on cybersecurity. These efforts are required in order that the country will be able to operate successfully in the cyberwarfare environments of not only today, but also—importantly—tomorrow. Among the areas where sustained attention should be paid are cyberwarfare, coordinated cyber efforts, the cyber workforce, cognitive warfare threats, cyber-related defence procurement, global cooperation concerning cyber issues, and international frameworks for cyberspace.

As well, the Committee joins others in noting that strengthened cyber resilience nationwide will require activities in a variety of areas. These include protecting critical infrastructure, enhancing public–private collaboration regarding cyber issues, reporting cyber incidents as they arise, establishing relevant standards, creating incentives for investments, investing in cyber-related R & D, increasing public education and training, and ensuring respect for individual privacy and civil liberties.

It is clear to the Committee that Canada—governments, the private sector and individuals—must take the actions required both to enable the country to defend itself against cyber threats, and to ensure that its digital systems and networks are protected against the rapidly evolving cyber threats and cognitive

warfare threats. Cybersecurity—a necessary focus for every part of our society—is a critical component of Canada's future safety, security and prosperity.

In light of the foregoing, the Committee recommends:

Recommendation 1

That the Government of Canada establish an ongoing multistakeholder platform for collaboration and engagement on cybersecurity issues. The objectives of this platform could be modelled after the Industry 100, in the United Kingdom. It should be established to create a collaborative space where industry and cyber officials meet to exchange information, best practices and establish forms of reporting private sector cyberattacks to lead to better information sharing and prevention of future attacks.

Recommendation 2

That the Government of Canada invest in its own network infrastructure cybersecurity and undertake a comprehensive assessment of additional requirements necessary to harden government systems and third-party network infrastructure on which its data is stored, with the goal of ensuring that its sensitive data is protected and secure.

Recommendation 3

That the Government of Canada work with our Five Eyes partners to adopt a Cybersecurity Maturity Model Certification (CMMC) that would be consistent and recognized by our partners to ensure that Canadian defence companies are not disadvantaged by having different security standards in Canada compared to our Five Eyes partners.

Recommendation 4

That the Government of Canada take steps to incentivize companies, which could include tax credits, to adopt cybersecurity measures, such as the "CyberSecure" standard established by ISED and CSE for small and medium organizations.

Recommendation 5

That the Government of Canada expedite the renewal of Canada's national cybersecurity strategy and establish an ongoing review that can better keep pace with the changing nature of cyber threats.

Recommendation 6

That the Government of Canada continue its ongoing dialogue with critical infrastructure owners/operators such as municipalities, Provincial, Territorial, Indigenous governments, and private sector operators such as utility companies; and, that this ongoing work be formalized to have consistent and ongoing dialogue to discuss potential threats as well as best practices.

Recommendation 7

That the Government of Canada examine the CSIS Act to ensure that CSIS has the legislative tools it needs to keep pace with technological advancements, modern digital realities, and the ever-evolving cybersecurity threats facing Canada.

Recommendation 8

That the Government of Canada work with provinces and industry to create requirements for private sector critical infrastructure operators to report ransomware and cybersecurity incidents to the Canadian Centre for Cyber Security within a designated time-period; create appropriate safeguards for victims of cyberattacks to mitigate or eliminate disincentives to reporting; and that the government incentivize owners and operators of critical infrastructure to cooperate with relevant authorities in identifying, reporting, and eliminating vulnerabilities.

Recommendation 9

That the Government of Canada work with industry partners to improve cyber-security at the development stage of hardware and software, in order to help shift the cyber-security burden away from individual users.

Recommendation 10

That the Government of Canada take steps to retain Canadian-developed information technology intellectual property in Canada, including commercialization measures that maintain Canadian ownership of cyber-technologies.

Recommendation 11

That the Government of Canada, in collaboration with civil society, industry and allies, further develop resources to deal with foreign cognitive warfare activities—such as misinformation, disinformation and malinformation—to better protect Canadians and ensure the public can access accurate information.

Recommendation 12

That the Government of Canada ensure federal departments and contracts are audited to confirm the information security standards are being met by government and contractors.

Recommendation 13

That the Government of Canada work with provinces to establish minimum standards for cyber security for small and medium organizations and incentivize companies to adopt the latest security measures to protect from both high-risk low probability and low-risk frequent attacks.

Recommendation 14

That the Government of Canada expand its collaboration with Canadian security and defence industries to bolster Canada's offensive and defensive cyber infrastructure amidst the growing assertiveness of malign foreign states.

Recommendation 15

That the Government of Canada undertake a comprehensive cyber security analysis to identify existent cyber vulnerabilities in Canada, including but not limited to critical infrastructure, and prioritize eliminating current vulnerabilities and intrusions by hostile actors.

Recommendation 16

That the Government of Canada include space-based platforms as critical infrastructure and, ensure they are protected and secure.

Recommendation 17

That the Government of Canada clearly define the roles and responsibilities of each government department currently responsible for monitoring, responding, and employing cyber capabilities in Canada.

Recommendation 18

That the Government of Canada reviews all cyber-related infrastructure, used for the operational functions of the Department of National Defence and the Canadian Armed Forces, to ensure it is free from sensitive technology designed, assembled and operated, either directly or indirectly, by malign foreign states, which could pose a cybersecurity risk or otherwise compromise protected information.

Recommendation 19

That the Government of Canada mandate all federal government departments and request provincial, territorial, municipal, and Indigenous governments to provide a detailed list of critical infrastructure to Treasury Board and the Communications Security Establishment and update it annually.

Recommendation 20

That the Government of Canada increase funding to the Canadian Centre for Cyber Security to improve coordination between federal and provincial cybersecurity systems to better address incidents.

Recommendation 21

That the Parliament of Canada create a special joint committee on cybersecurity, information warfare and artificial intelligence.

Recommendation 22

That the Government of Canada immediately undertake a comprehensive review and expeditious reform of the procurement process for military equipment, including cyberwarfare equipment—this would include Treasury Board guidelines on competition and sole sourcing—with the intent to bring project times down from years to months or weeks.

Recommendation 23

That the Government of Canada adapt and develop a comprehensive plan for the recruitment and retention of cyber operators which is competitive with the private sector to ensure positions are filled and the cyber skills gap is closed in the Canadian Armed Forces and the Communications Security Establishment.

Recommendation 24

That the Government of Canada develop and deploy "persistent engagement" capacity in collaboration with the Canadian Armed Forces.

Recommendation 25

That the government of Canada implement a system for allowing veterans to maintain security clearances equivalent to the clearances they had with the Canadian Armed Forces when transferring out of service thus enabling a seamless continuity in clearance in order to facilitate their employment in the Department of National Defence. The government should also examine a system of fast-tracking security clearance for veterans seeking employment in other federal departments.

Recommendation 26

That the Government of Canada take steps to clearly define the duties and responsibilities of the Canadian Armed Forces and the Communications Security Establishment as they relate to cyber security in Canada and abroad.

Recommendation 27

That the Government of Canada take immediate steps to address logistical support issues in the Canadian Armed Forces, including the Cyber Forces.

Recommendation 28

That the Government of Canada ensure the future viability of the CAF Cyber Forces by creating a retention program for its Cyber Operators and supplying them with the necessary cyber infrastructure.

Recommendation 29

That the Government of Canada continuously update the legal framework for dealing with cyberattacks, which includes guidelines for attribution, response and liability.

Recommendation 30

That the Government of Canada work with our allies to update international laws, such as the Rome Statute and the Geneva Convention, to include state-sponsored cyberwarfare as a war crime.

Recommendation 31

That the Government of Canada immediately adopt all outstanding recommendations of the Auditor General's Report 7—Cybersecurity of Personal Information in the Cloud, tabled to Parliament on November 15, 2022.

Recommendation 32

That the Government of Canada use existing sanctions regimes to target individuals and entities targeting Canadians with misinformation, disinformation and/or malinformation.

Recommendation 33

That the Government of Canada impose effective sanctions on countries which condone or deploy cybercriminals for purposes such as theft of funds, theft of intellectual property, information warfare, and other malicious intents.

Recommendation 34

That the Government of Canada open a review of existing cyber-defence policy and hold bilateral conversations with allies, such as the US, to ensure cohesive and consistent policies are being used.

Recommendation 35

That the Government of Canada share Finland and Sweden's cognitive warfare education for civilians with the provinces.

Recommendation 36

That the Government of Canada establish clear boundaries in the operations of the Communications Security Establishment between their signals intelligence and cybersecurity mandates, including ministerial authorization processes and reporting mechanisms.

Recommendation 37

That the Government of Canada appoint a cybersecurity ambassador.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Centre for International Governance Innovation	2023/02/07	48
Aaron Shull, Managing Director and General Counsel		
Wesley Wark, Senior Fellow		
Communications Security Establishment	2023/02/07	48
Sami Khoury, Head, Canadian Centre for Cyber Security		
Alia Tayyeb, Deputy Chief of Signals Intelligence (SIGINT)		
As an individual	2023/02/10	49
Kristen Csenkey, Ph.D. Candidate, Balsillie School of International Affairs, Wilfrid Laurier University		
Thomas Keenan, Professor, University of Calgary		
Alexander Rudolph, Ph.D. Candidate, Department of Political Science, Carleton University		
Université du Québec à Montréal	2023/02/10	49
Alexis Rapin, Research Fellow, Raoul-Dandurand Chair in Strategic and Diplomatic Studies		
As an individual	2023/02/14	50
Marcus Kolga, Senior Fellow, Macdonald-Laurier Institute		
Department of National Defence	2023/02/14	50
RAdm Lou Carosielli, Cyber Force Commander, Canadian Armed Forces		
Jonathan Quinn, Director General, Continental Defence Policy		

Organizations and Individuals	Date	Meeting
As an individual Christian Leuprecht, Professor, Royal Military College of Canada	2023/03/10	53
Canadian Association of Defence and Security Industries Christyn Cianfarani, President and Chief Executive Officer	2023/03/10	53
Sectigo Tim Callan, Chief Experience Officer	2023/03/10	53
As an individual Tadej Nared, Chairman of the Board, Slovenian Certified Ethical Hackers Foundation	2023/03/31	55
BlackBerry John de Boer, Senior Director, Government Affairs and Public Policy, Canada	2023/03/31	55
International Civil Liberties Monitoring Group Tim McSorley, National Coordinator	2023/03/31	55

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Turnbull, John

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 48, 49, 50, 53, 55, 63, and 64) is tabled.

Respectfully submitted,

Hon. John McKay
Chair

The New Democratic Party supports the intent behind the Standing Committee on National Defence's report on cybersecurity and the threat of cyberwarfare. Canadians are rightly concerned about the threat posed by advancing cybertechnology in the midst of escalating global tensions. Artificial Intelligence, misinformation, state-sponsored hackers, and advancements in cloud storage are creating unique threats to Canadians and our critical infrastructure. It is with these emerging threats in mind that the Standing Committee on National Defence began our study, with the aim to inform meaningful reforms that will protect Canadians.

New Democrats approach cybersecurity with the aim to protect Canadians first. We must modernize our cybersecurity laws to protect the private information of Canadians and the critical infrastructure upon which we rely. We need to ensure that Canadian's Charter rights to privacy are protected from hostile actors and ensure our critical infrastructure are robustly defended from attacks.

Many of the recommendations we adopted should be actioned immediately, particularly the recommendations relevant to building a more adaptive and robust cybersecurity policy for the Federal government, critical infrastructure, and response to disinformation.

However, the committees report does not adequately reflect two major challenges to our cybersecurity policy: the growing role of monopolies on our critical infrastructure, and the lack of accountability for Canada's intelligence agencies.

The Role of Monopolies in Canada's Critical Infrastructure

Last July, more than 12 million Canadians lost access to internet and cellular networks. Interac was taken offline, multiple public transport agencies had outages, and multiple government websites were unavailable. Canadians became incredibly aware of the impact an attack on our critical infrastructure could pose.

But this threat was not posed by a foreign state actor – this was an internal breakdown of systems by the telecoms giant Rogers. If Canada is going to become serious about our cybersecurity vulnerabilities, we need to approach the growing monopolies of critical infrastructure through a national security lens. The committee would have benefited from challenging this vulnerability.

Further, throughout the committee we discussed the domain of social media for foreign disinformation extensively. We heard from Marcus Kolga from the Macdonald-Laurier Institute on the how cognitive warfare is "an extremely important tool in [the] tool kit" of our adversaries, and that this is often done through spreading disinformation through social media.

While we extensively discussed the use of social media as domain for cognitive warfare, the Committee's report did not discuss the dangerous role of social media giants themselves. We heard from Dr. Wesley Wark from the Canadian Institute for Governance Innovation that "we clearly need better restrictions on efforts to use consent on the part of social media companies. I think there is a real role for the Government of Canada to play in that regard n terms of setting guidelines, as challenging as that might be, because the giant social media platforms will not like it”.

Social media, as a domain in which foreign disinformation occurs, is in the hands of a few billionaires that pursue surveillance capitalism. The drive to monetize Canadian’s data by these billionaires produces advanced algorithms that pose major national security threats, and the committee would have benefited from studying this issue further.

Finally, New Democrats do support the intent behind recommendations 3 and 12, which aim to bolster cybersecurity measures taken by contractors with the federal government. While our public servants work diligently to protect Canadian’s privacy everyday, too often the government outsources to private companies that do not follow the same standards. Deloitte, the major benefactor to government outsourcing, has had multiple historic breaches of consumer and citizen data.

New Democrats raised the example of an incident in 2017, when Deloitte suffered a major data breach that led to the leaking of passwords, IP addresses and identifiable data in relation to a contract with the U.S. Department of Defence, Department of Homeland Security, the State Department and the National Institute of Health. Companies like Deloitte must be held accountable when they do not follow cybersecurity best practices, and the security of Canadian data should be considered when outsourcing.

Canada’s Intelligence Community

Halfway through this study, the National Security and Intelligence Review Agency released a letter sent to the commissioner of the Canada Revenue Agency (CRA) to commence an investigation of the CRA’s Review and Analysis Division related to systemic islamophobia in the audits of Muslim charities.

This investigation was sparked by revelations from organizations like the International Civil Liberties Monitoring Group that 75% of the organizations whose charitable status were revoked following Review and Analysis Division audits were Muslim charities.

When Tim McSorley from the International Civil Liberties Monitoring Group was asked about this, he stated:

“The BC Civil Liberties Association found in their research that CSE was sharing intelligence with the CRA in order to bolster their efforts to counter terrorist financing. However, what we have found in our research is that the CRA, through its efforts to counter terrorist fundraising, has taken a prejudiced approach to Muslim charities in Canada. It has been operating from an idea that because there are terrorist threats from Muslim-linked organizations, the Muslim community must be placed under greater suspicion. That results in greater surveillance, greater information gathering and sharing and greater repercussions as compared to other communities in Canada”.

In light of this, the New Democratic Party is concerned with the recommendations put forward by the committee to greater integrate the collaboration of the Communications Security Establishment with other government agencies within meaningful oversight.

While we fully understand that a whole-of-government approach is needed to meet Canada's cybersecurity needs, New Democrats remember Canada's rejection of expanded intelligence agency powers under the Harper Government's Bill C-51. We are disappointed by the Liberal government's decision to continue or expand many of these powers under Bill C-59. As we have seen with intelligence sharing between intelligence agencies and the Canada Revenue Agency, systemic racism can manifest in the policing of marginalized communities.

As we heard from the Communication Securities Establishment's Sami Khoury and Alia Tayyeb, the CSE has a dual mandate: Establishing and maintaining cybersecurity for the Federal government and industry partners, and signals intelligence. Their role in providing cybersecurity protections are vital to the functioning of our federal government, but we are concerned that the space between this defensive role is blurred with their signal intelligence mandate.

We heard from Tim McSorley that CSE is not "appropriately delineating between the two kinds of activities, despite each requiring a different approval process". New Democrats firmly believe that before we expand the mandate of CSE further, we must enshrine clear barriers between signals intelligence and their cybersecurity operations.