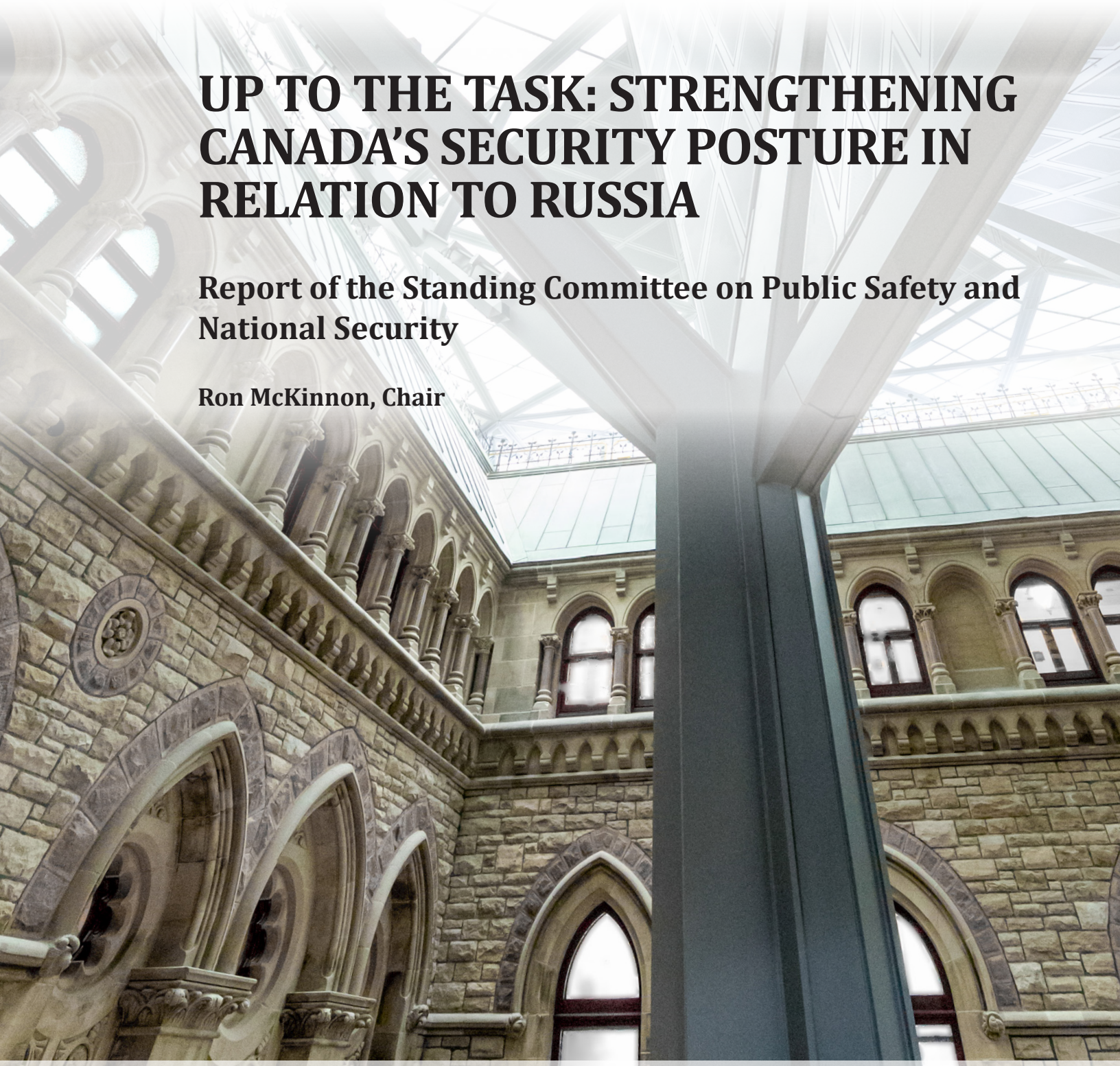
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

UP TO THE TASK: STRENGTHENING CANADA'S SECURITY POSTURE IN RELATION TO RUSSIA

Report of the Standing Committee on Public Safety and National Security

Ron McKinnon, Chair



MARCH 2023
44th PARLIAMENT, 1st SESSION

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

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Standing Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

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

UP TO THE TASK: STRENGTHENING CANADA'S SECURITY POSTURE IN RELATION TO RUSSIA

Report of the Standing Committee on Public Safety and National Security

Ron McKinnon
Chair

MARCH 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 PUBLIC SAFETY AND NATIONAL SECURITY

CHAIR

Ron McKinnon

VICE-CHAIRS

Raquel Dancho
Kristina Michaud

MEMBERS

Paul Chiang
Pam Damoff
Iqwinder Gaheer
Peter Julian
Dane Lloyd
Glen Motz
Taleeb Noormohamed
Peter Schiefke
Doug Shipley

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Jim Carr
Kody Blois
Scot Davidson
Stephen Ellis
Michael Kram
Viviane Lapointe
Alistair MacGregor
Robert J. Morrissey
Kyle Seeback
Jake Stewart
Tako Van Popta

Karen Vecchio
Len Webber
Sameer Zuberi

CLERK OF THE COMMITTEE

Simon Larouche

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Lyne Casavant
Allison Goody

THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

has the honour to present its

SEVENTH REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied assessment of Canada's security posture in relation to Russia and has agreed to report the following:

TABLE OF CONTENTS

CHAIR'S FOREWORD

As Members from different parties, there are inevitably times when we are not able to reach agreement on the policy issues before us. The report that follows, however, reflects – unequivocally – a shared concern and our common resolve. The Committee's months of work, studying the security threat posed by Russia, revealed a national security landscape that is increasingly multifaceted and complex. The Committee believes that its recommendations can strengthen Canada's security posture to meet that challenge.

Our work would not have been possible without the valuable insights of those who appeared as witnesses before the committee or submitted documentation. The Committee is grateful for these contributions.

Most of this study was conducted under the leadership of the Honourable Jim Carr, who sadly passed away on 12 December 2022. He was our chair from December 2021 to September 2022. As a former federal minister, committed parliamentarian and notable public figure, Jim Carr guided the Committee through its important and busy agenda, setting the tone of collegiality and seriousness that its Members endeavour to follow.

The Committee would like to dedicate this report – our collective work – to his memory.

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 continue to –

- **impose severe costs on Russia for its aggression against Ukraine;**
- **support Ukraine's sovereignty, independence, and territorial integrity;**
- **work with allies and partners to uphold the rules-based international order; and**
- **accelerate efforts to deter and defend against any conventional and unconventional threats to Canada's national security. 15**

Recommendation 2

That the Government of Canada work with provincial and territorial partners to create and promote accredited post-secondary cyber defence training programs 23

Recommendation 3

That the Government of Canada, in consultation with relevant stakeholders, build on the *National Cyber Security Strategy* to ensure that –

- **operators and enterprises of all sizes connected to critical infrastructure have the cyber security experts, expertise, and resources they need to defend against and recover from malicious cyber activity; and**
- **cyber security standards are met and reported on. 23**

UP TO THE TASK: STRENGTHENING CANADA'S SECURITY POSTURE IN RELATION TO RUSSIA

OVERVIEW

Introduction

On 3 March 2022, the House of Commons Standing Committee on Public Safety and National Security (the committee) agreed to the following motion:

> That pursuant to standing order 108(2), the committee immediately begin a study of Canada's emergency preparedness for the range of threats posed by Russia, including threats to Canada's public safety and national security, to Canada's critical infrastructure (both physical and cyber), the prevalence and impact of Russian misinformation, as well as the threat that Russia could resort to the use of espionage, sabotage, and weapons of mass destruction[.][1]

To complete this study, the committee received testimony during eight meetings held between 5 April 2022 and 6 October 2022, hearing from a wide range of academics and other experts, as well as Canada's Minister of Emergency Preparedness, Minister of Public Safety, Chief of the Defence Staff, and Chief of the Communications Security Establishment.

The report that follows puts forward the committee's key findings and recommendations on Canada's security posture in relation to Russia. It begins with an overview of the context that informed the committee's work. It then examines the main concerns that were raised about Russia during the committee's study, namely: malicious cyber activity that targets critical infrastructure; campaigns that spread disinformation and disrupt democratic systems; corruption that supports aggression; and weaponry that challenges continental defence. The report's conclusion examines the broader policy implications of a threat environment that has become increasingly complex.

1 House of Commons, Standing Committee on Public Safety and National Security (SECU), *Minutes of Proceedings*, 3 March 2022.

Context of the Committee's Study

Russia's War against Ukraine

On 24 February 2022, Russia launched a full-scale invasion of Ukraine. The massing of tanks, soldiers, aircraft, and missiles on Ukraine's borders, which were then deployed along multiple vectors of attack, showed an unmistakeable intent to use force to achieve Russia's geopolitical objectives and a willingness to violate international law, which left open questions about the full extent of Russia's aims.

Months of combat have since exposed weaknesses with Russia's conventional military forces, including with respect to training, logistics and the ability to integrate combined arms.[2] After Russian units were forced to retreat from a Ukrainian counter-offensive in the Kharkiv region, and while announcing that staged "referendums" would be held in occupied Ukrainian territory, President Vladimir Putin warned in September 2022 that Russia would make use of all weapon systems at its disposal if its territorial integrity were threatened.[3] That rhetoric – understood as a reference to Russia's nuclear arsenal – was followed by Putin's announcement that Russia would be annexing the four Ukrainian regions,[4] an act that has been denounced as illegal by the international community.[5] Russia does not hold all the Ukrainian territory it has purported to claim, as was shown immediately after Putin's speech when Russian forces retreated from Lyman, in Donetsk, which they had being using as a logistics hub.[6]

Beyond the battlefield, Russia's war – and the pressure tactics it has relied on – have had global ramifications. William Browder, Chief Executive Officer, Hermitage Capital

---

2 SECU, *Evidence*, 6 October 2022, 1135 (General Wayne D. Eyre, Chief of the Defence Staff, Canadian Armed Forces, Department of National Defence). Commenting on the failures that have been observed at the strategic level, General Eyre observed that Russia's "political ends have not matched their military ways and means." Nevertheless, while noting that most of Russia's land forces have been deployed in furtherance of its war against Ukraine, General Eyre indicated that Russia "still has many other forces." Its air, naval, and strategic forces remain a threat.

3 "Read Putin's national address on a partial military mobilization," *The Washington Post*, 21 September 2022. Also see Anton Troianovski, "With Annexation Plans, Putin Escalates Battle of Wills With the West," *The New York Times*, 29 September 2022.

4 Ann M. Simmons and Yuliya Chernova, "Russia Announces Annexation of Four Regions of Ukraine," *The Wall Street Journal,* 30 September 2022; and David E. Sanger, Anton Troianovski and Julian E. Barnes, "In Washington, Putin's Nuclear Threats Stir Growing Alarm," *The New York Times*, 1 October 2022.

5 United Nations, UN News, *Ukraine: UN General Assembly demands Russia reverse course on 'attempted illegal annexation'*, 12 October 2022.

6 See Mary Ilyushina, Emily Rauhala and Isabelle Khurshudyan, "Ukraine hammers Russian forces into retreat on east and south fronts," *The Washington Post*, 4 October 2022.

Management Ltd, told the committee that Russia is "weaponizing everything that they can weaponize."[7]

In the early stages of the war, Russian forces seized Ukraine's Zaporizhzhia nuclear power plant, the largest such plant in Europe. Military activity around the plant has generated significant concerns about nuclear safety.[8] Furthermore, Russia has sought to apply pressure on energy markets, by first reducing gas flows to European countries, before shutting down the Nord Stream 1 pipeline altogether.[9] Russia has also weaponized food. While it agreed in July 2022 to a deal brokered by Turkey and the United Nations to establish a maritime corridor,[10] Russia had prevented the export of millions of tonnes of grain from Ukrainian ports,[11] driving up the already high prices of food staples around the world.

A Pattern of Behaviour

While these events formed the immediate backdrop to the committee's study, concern about Russia's behaviour and intentions had been building for years. In 2008, Russia engaged in a war with Georgia, and in 2014 Russia occupied and then moved to annex Ukraine's Crimea region, before destabilizing eastern Ukraine. That aggression was carried out alongside a multi-year program to modernize Russia's military forces. Yet, the threat was not limited to the foreign policy context. There were also hybrid campaigns being carried out that appeared designed to weaken norms and challenge democratic systems.

Multiple incidents have shed light on these campaigns. The United States Central Intelligence Agency, Federal Bureau of Investigation and National Security Agency assessed that "Russian President Vladimir Putin ordered an influence campaign in 2016

---

7 SECU, *Evidence*, 17 May 2022, 1200 (William Browder, Chief Executive Officer, Hermitage Capital Management Ltd, As an Individual).

8 International Atomic Energy Agency (IAEA), *Nuclear Safety, Security and Safeguards in Ukraine: 2nd Summary Report by the Director General, 28 April – 5 September 2022*; and IAEA, *Update 112 – IAEA Director General Statement on Situation in Ukraine*, 5 October 2022.

9 Max Seddon, David Sheppard and Henry Foy, "Russia switches off Europe's main gas pipeline until sanctions are lifted," *Financial Times*, 5 September 2022.

10 United Nations, UN News, *The Black Sea Grain Initiative: What it is, and why it's important for the world*, 16 September 2022.

11 Matina Stevis-Gridneff, "Russia Agrees to Let Ukraine Ship Grain, Easing World Food Shortage," *The New York Times*, 23 July 2022.

aimed at the US presidential election."[12] This campaign included a social media operation and computer-intrusions.[13] In a separate incident, Canada and its allies determined that, in October 2019, cyber units of Russia's military intelligence agency had carried out a large-scale cyber attack that was "part of a concerted effort by the Russian Government to sow discord in advance of Georgia's 2020 parliamentary elections."[14]

There have been other targets and other forms of disruption in the cyber domain. In 2015 and 2016, Russian state-sponsored cyber actors shut off part of Ukraine's electricity grid.[15] Furthermore, Canada and its allies assessed that "actors in Russia were responsible for developing NotPetya," malware that was indiscriminately attacking "critical financial, energy, government, and infrastructure sectors around the world in June 2017."[16]

Reports of malicious cyber activity continued to emerge. Joining the United States and other partners, Canada's ministers of foreign affairs, national defence, and public safety and emergency preparedness issued a joint statement in April 2021 regarding a "Russian cyber-espionage campaign that exploited the SolarWinds Orion platform."[17] The company's supply chain was compromised through a backdoor that was inserted in a software update, which allowed the installation of additional malware into the networks of a subset of the company's clients.[18] The networks of more than 100 Canadian entities were compromised, which necessitated "costly mitigation activities and may have undermined public confidence in downloading software updates."[19] Canada assessed that APT29, also known as "The Dukes" or "Cozy Bear," was responsible for this malicious activity.[20] The statement indicated that the group was almost certainly

12 United States, Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections: Intelligence Community Assessment*, 6 January 2017, p. ii.

13 Special Counsel Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I of II*, United States Department of Justice, March 2019, p. 1.

14 Communications Security Establishment (CSE), *CSE Statement on Malicious Russian Cyber Activity Targeting Georgia*.

15 Canadian Centre for Cyber Security, *Cyber threat bulletin: The cyber threat to Canada's electricity sector*, based on information available as of 29 September 2020.

16 CSE, *CSE Statement on the NotPetya Malware*.

17 Global Affairs Canada, *Statement on SolarWinds Cyber Compromise*, Statement, 15 April 2021.

18 Global Affairs Canada, *SolarWinds Cyber Compromise*, Backgrounder.

19 Global Affairs Canada, *Statement on SolarWinds Cyber Compromise*, Statement, 15 April 2021.

20 Ibid.

operating "as part of Russian Intelligence Services (SVR)."[21] It was those same services – the SVR – that targeted Canadian research and development of COVID-19 vaccines in 2020.[22]

In early 2022, the Canadian Centre for Cyber Security – which is part of the Communications Security Establishment (CSE) – issued two threat bulletins, urging operators of critical infrastructure in Canada to raise their awareness, proactively monitor networks, and take mitigations against known Russian-backed cyber threat activity.[23] In April 2022, after Russia had invaded Ukraine, the cyber security authorities of Canada, the United States, Australia, the United Kingdom, and New Zealand issued a joint advisory, indicating that "there is an increased risk to critical infrastructure organizations globally from Russian state-sponsored advanced persistent threat (APT) actors, their proxies, and independent cybercriminal groups."[24] The possible threats outlined in the advisory included the deployment of ransomware, as well as distributed denial of service attacks for the purpose of disrupting or harming critical industrial control system and operational technology functions.[25]

In general, concern about Russia is heightened because it has shown a willingness to cross internationally recognized red lines. The use of a chemical nerve agent against a former double agent and his daughter in Salisbury, United Kingdom, in 2018, was attributed to officers from the Russian military intelligence service and assessed as having been "almost certainly approved at a senior government level."[26] Dr. Jeffrey Mankoff, Distinguished Research Fellow at the National Defense University, told the committee that this operation and the earlier poisoning of a defector from the Russian security service with polonium, also on British soil, "show a clear willingness to use not

21 Ibid.

22 Global Affairs Canada, *Statement on Russia's malicious cyber activity affecting Europe and Ukraine*, Statement, 10 May 2022.

23 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity*, 26 January 2022; and Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre reminds Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity*, 13 February 2022.

24 Canadian Centre for Cyber Security, *Joint cyber security advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure*, 20 April 2022.

25 Ibid.

26 Prime Minister of Canada, Justin Trudeau, *Joint Statement by the Leaders of France, Germany, the United States, Canada and the United Kingdom on the Salisbury Attack*, 6 September 2018.

only violence, but also to cross internationally recognized red lines regarding the use of chemical and radiological weapons."[27]

THREATS ASSOCIATED WITH RUSSIA

Assessing the Overall Threat to Canada's National Security

Russia's disruptive behaviour is by now well established, particularly in the cyber realm and as concerns the countries nearest to it in Europe. Nevertheless, different perspectives were brought to the committee's attention regarding the nature and severity of the threat that Russia poses directly to Canada and, more particularly, to Canada's public safety and national security. Where some see a clear danger, others suggested a long-term challenge and one that should be understood in the context of the broader threat environment and the geopolitical landscape.

Dr. Robert Huebert, an Associate Professor in the Department of Political Science at the University of Calgary, emphasized his understanding that "Russia is an existential threat to Canada" and one that is "growing." He observed that, since assuming the presidency at the end of 1999, Putin has moved to "reconsolidate the Russian empire" and protect his regime. According to Professor Huebert, Russia's willingness to use its way of war – which he referred to as "multi-domain processes of warfare" – to achieve Russia's objectives "places it on a direct collision course with [the North Atlantic Treaty Organization, NATO]."[28]

Dr. Charles Burton, Senior Fellow at the Macdonald-Laurier Institute, considers that the threat Russia poses to Canada's public safety and national security has "increased significantly" since the West responded to Russia's invasion of Ukraine with significant sanctions and weapons transfers. An angry and resentful President Putin, equipped "with dangerous capabilities to lash out at Canada," is likely – in his assessment – "to make common cause with China, which will magnify the threat to [Canada]."[29]

Dr. David Perry, President of the Canadian Global Affairs Institute, sees Russia "challenging Canadian and Western interests in multiple places around the world and

27 SECU, *Evidence*, 17 May 2022, 1205 (Dr. Jeffrey Mankoff, Distinguished Research Fellow, National Defense University, As an Individual).

28 SECU, *Evidence*, 5 April 2022, 1110 (Dr. Robert Huebert, Associate Professor, Department of Political Science, University of Calgary, As an Individual).

29 SECU, *Evidence*, 3 May 2022, 1135 (Dr. Charles Burton, Senior Fellow, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute, As an Individual).

with many different means, including cyber and disinformation activities." His position is that Russia's war against Ukraine demonstrates that "Russia is prepared to employ its modernized military without provocation in ways that are fundamentally anathema to Canadian interests and values, and that we in Canada find difficult to comprehend."[30]

Dr. Jonathan Paquin, Full Professor in the Department of Political Science at Laval University, also pointed to evidence suggesting that Russia "is a threat to our country's security." The evidence includes Russia's history of cyber-attacks against the critical infrastructure of countries that Russia considers to be hostile to its interests. Because "Canada is currently very hostile to Moscow's interests," it is – he said – "potentially a prime target for the Kremlin." Professor Paquin further noted Russia's funding of disinformation campaigns and the nuclear threats it has made since invading Ukraine. He advised Canada and its allies to adopt even greater vigilance "now that Western countries have expanded their objectives in the Ukrainian conflict and have openly sought to degrade Russia's capabilities."[31] To enhance its security, Professor Paquin recommends that Canada adopt a dual strategy of deterrence: through the prospect of retaliation (via participation in NATO) and through denial (via cyber resilience, education, and "renewed continental defence").[32]

Although Russia has made nuclear threats, as a form of deterrence, Dr. Jeffrey Mankoff observed that Russia may be more inclined to use some of the disruptive tools and non-conventional weapons at its disposal owing to the "relative weakness" of Russia's conventional military forces. He assesses that the danger of such disruptive attacks "will only grow as the relationship with Moscow deteriorates and Putin grows more desperate as Russian losses in Ukraine mount." While they continue their support for Ukraine, Dr. Mankoff believes that Canada and other NATO Allies "must all remain alert to the possibility that Russia will cross lines previously thought to be uncrossable." The posture that this analysis compels, he said, is not one of "timidity," but rather "preparedness and prudence."[33]

Dr. James Fergusson, Deputy Director of the Centre for Defence and Security Studies at the University of Manitoba, does not see a threat that should be understood as originating on

30 SECU, *Evidence*, 5 April 2022, 1220 (Dr. David Perry, President, Canadian Global Affairs Institute, As an Individual).

31 SECU, *Evidence*, 3 May 2022, 1250 (Dr. Jonathan Paquin, Full Professor, Department of Political Science, Université Laval, As an Individual). Professor Paquin subsequently commented that, "if Russia were to lose the war or if Russia were unable to win in eastern and Southern Ukraine, it's a safe bet that there will be retaliation and that, essentially, the Russians will not maintain the status quo." See Ibid., 1310.

32 SECU, *Evidence*, 3 May 2022, 1250 (Dr. Jonathan Paquin).

33 SECU, *Evidence*, 17 May 2022, 1205 (Dr. Jeffrey Mankoff).

24 February 2022 or necessitating panic within Canada. While Russia's war against Ukraine has certainly "heightened the attention," he argued that "these vulnerabilities have been here for a long time now." Notwithstanding the adversarial relationship that exists between Russia and the West, the situation today, in Dr. Fergusson's estimation, "is not a new Cold War." He believes there "are other issues and other threats out there which have to be taken into account in trying to respond to the Russian side of this equation."[34]

Outlining Canada's response to Russia's aggression, the Honourable Bill Blair, Minister of Emergency Preparedness, informed the committee that the government has worked to impose severe costs on Russia, while it has also remained "on the lookout for all potential Russian threat activity within Canada and affecting Canadians' interests around the world."[35] Canada's national security agencies have assumed "heightened vigilance," the minister said, in relation to "any form of interference, including cyber, that could take place in this country."[36]

While the committee's study focused on threats emanating from Russia, it is not the only source of strategic concern. Dr. Andrea Charron, Director and Associate Professor, Centre for Defence and Security Studies, University of Manitoba, emphasized that Russia is "an acute threat to North America," but also noted that "China is the longer-term peer challenger to the U.S.'s waning hegemony."[37]

The testimony of General Wayne D. Eyre, Chief of the Defence Staff, Canadian Armed Forces, adopted this wider lens. He framed the geopolitical landscape as follows:

> We once again find ourselves in a chaotic and dangerous world where those with power, namely, Russia and China, are determined to remake the world order to suit their own ends and where the rights and freedoms of smaller, less powerful states are discarded.[38]

This determination, and the response to it, can be understood as a contest between an international order that is based on rules, and one based on might.[39] Yet, General Eyre warned that the rules-based order, "which has underpinned world stability and indeed

34 SECU, *Evidence*, 5 April 2022, 1105 (Dr. James Fergusson, Deputy Director, Centre for Defence and Security Studies, University of Manitoba, As an Individual).

35 SECU, *Evidence*, 2 June 2022, 1100 (the Honourable Bill Blair, Minister of Emergency Preparedness).

36 Ibid., 1155.

37 SECU, *Evidence*, 7 April 2022, 1205 (Dr. Andrea Charron, Director and Associate Professor, Centre for Defence and Security Studies, University of Manitoba, As an Individual).

38 SECU, *Evidence*, 6 October 2022, 1100 (Gen Wayne D. Eyre).

39 Ibid.

our national prosperity for generations, is faltering." The task ahead, he said, is to defend it.[40]

Based on these considerations, the committee recommends:

Recommendation 1

That the Government of Canada continue to –

- **impose severe costs on Russia for its aggression against Ukraine;**
- **support Ukraine's sovereignty, independence, and territorial integrity;**
- **work with allies and partners to uphold the rules-based international order; and**
- **accelerate efforts to deter and defend against any conventional and unconventional threats to Canada's national security.**

Malicious Cyber Activity and Critical Infrastructure

The Stakes

Testimony suggested that cyber-related threats from Russia are among the most serious and relevant for Canada's public safety and national security, particularly in relation to critical infrastructure. The importance of such infrastructure – most of which is cyber-enabled – is implied by the term itself. Critical infrastructure refers to "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[41] It includes a range of sectors, from energy and utilities to food. The Government of Canada's National Strategy for Critical Infrastructure acknowledges that disruptions "could result in catastrophic loss of life and adverse economic effects."[42]

Indeed, Errol Mendes, Professor of Constitutional and International Law at the University of Ottawa, believes there is a need, in conjunction with allies, to frame cyber warnings – like the bulletins issued by the CSE in relation to critical infrastructure protection prior to Russia's invasion of Ukraine – in terms of grave violations of

40 Ibid., 1105.

41 Public Safety Canada, *National Strategy for Critical Infrastructure*.

42 Ibid.

international law. That would potentially include international humanitarian law if an attack involved the endangerment of many lives, such as attacks against hospitals or water supplies.[43]

A Multitude of Cyber Actors and Targets

The national security dimensions of cyberspace are complex because threats do not emanate from states alone, nor are they limited to government targets. Jennifer Quaid, Executive Director, Canadian Cyber Threat Exchange, reminded the committee that there are both "nation-states who are conducting espionage and statecraft through the Internet, and criminals who are engaging in cybercrime for financial gain."[44] Caroline Xavier, Chief of the CSE, indicated that cybercrime "is the most prevalent and most pervasive threat to Canadians and Canadian businesses." At the same time, she observed that the "state-sponsored cyber programs of China, North Korea, Iran and Russia pose the greatest strategic threat to Canada."[45] Foreign cyber threat activities include attempts to target Canadian critical infrastructure operators, as well as their operational and information technology.[46]

Several factors complicate the protection of critical infrastructure from cyber-attacks and the endeavour of building cyber resilience. Dr. James Fergusson noted that, unlike the defence domain, which is dominated by government, Canada's critical infrastructure "is by and large in the hands of the private sector."[47] In fact, David A. Etkin, Professor in Disaster and Emergency Management at York University, indicated that "about 85% of Canada's critical infrastructure is owned within the private sector."[48]

There are also structural issues to consider when comparing the defence and cyber domains. When it comes to aerospace and maritime threats, Canada's defence partnership with the United States is underpinned by the binational North American Aerospace Defense Command (NORAD).[49] Dr. Fergusson observed that there is no

43 SECU, *Evidence*, 17 May 2022, 1210 (Errol Mendes, Professor, Constitutional and International Law, University of Ottawa, As an Individual).

44 SECU, *Evidence*, 3 May 2022, 1140 (Jennifer Quaid, Executive Director, Canadian Cyber Threat Exchange).

45 SECU, *Evidence*, 6 October 2022, 1110 (Caroline Xavier, Chief, Communications Security Establishment).

46 Ibid.

47 SECU, *Evidence*, 5 April 2022, 1105 (Dr. James Fergusson).

48 SECU, *Evidence*, 7 April 2022, 1100 (David A. Etkin, Professor, Disaster and Emergency Management, York University, As an Individual).

49 National Defence, *North American Aerospace Defense Command (NORAD)*, Backgrounder.

equivalent structure "to coordinate responses to potential Russian cyber-attacks, whether they are for espionage reasons or attempts to undermine or sabotage critical infrastructure."[50] Testimony also suggested the need to address cross-border emergency management capacity. Using the scenario of a cyber-attack against the auto industry in Detroit, Juliette Kayyem, Belfer Senior Lecturer in International Security at the Harvard Kennedy School of Government, noted that the response would essentially need to be "borderless."[51]

The range of potential targets for malicious cyber activity strains preparedness. Caroline Xavier told the committee that critical infrastructure operators and large enterprises are some of the most "lucrative targets" for cyber criminals.[52] However, the committee also heard that many small- and medium-sized enterprises, which generally have fewer resources and less cyber expertise at their disposal to identify threats and recover from incidents, are vulnerable. Jennifer Quaid indicated that 44% of the smaller members in her organization do not have "any form of cyber-defence," while 60% have no insurance.[53] Regarding the threat posed by Russian cyber actors, Dr. Ken Barker, Professor in the Institute for Security, Privacy, and Information Assurance at the University of Calgary, indicated that small- and medium-sized enterprises "are unlikely to be a specific target from Russia unless they exist in certain cybersecurity sectors and/or are suppliers to the critical infrastructure."[54]

Established Capabilities

Witnesses referenced Russia's cyber capabilities, both those associated with the state and non-state actors, and the malicious activity that has been attributed to Russia, as summarized at the beginning of this report.

According to Dr. Christian Leuprecht, Professor at the Royal Military College of Canada and Queen's University, the SolarWinds attack illustrates that Russia, China, and a handful of others can build deliberate and targeted exploits.[55] David Shipley, Chief

50 SECU, *Evidence*, 5 April 2022, 1105 (Dr. James Fergusson).

51 SECU, *Evidence*, 7 June 2022, 1240 (Juliette Kayyem, Belfer Senior Lecturer in International Security, Harvard Kennedy School of Government, As an Individual).

52 SECU, *Evidence*, 6 October 2022, 1110 (Caroline Xavier).

53 SECU, *Evidence*, 3 May 2022, 1155 (Jennifer Quaid).

54 SECU, *Evidence*, 7 June 2022, 1205 (Dr. Ken Barker, Professor, Institute for Security, Privacy, and Information Assurance, University of Calgary, As an Individual).

55 SECU, *Evidence*, 17 May 2022, 1120 (Dr. Christian Leuprecht, Professor, Royal Military College of Canada, Queen's University, As an Individual).

Executive Officer of Beauceron Security, similarly told the committee that Russia's capability to use technology and control harm is "well documented," and that the threat is not notional. He said: "Cyber-attacks from Russian criminal gangs have crippled Canadian municipalities, health care organizations and more, with costs into the tens of millions of dollars."[56]

However, testimony also indicated that Russia's cyber activity since invading Ukraine has not been as destructive or escalatory as some observers had feared would be the case. Significant cyber operations have been carried out, focused against Ukraine's government, military, economic functions, and infrastructure.[57] Yet, Professor Barker observed that there had not been an increase in what are known as "zero-day attacks" – i.e., attacks that are of unknown origin or that target unknown vulnerabilities – since the war began.[58]

According to Dr. Nora Cuppens, Professor at Polytechnique Montréal, this situation may reflect poor preparation on Russia's part or be a sign that Russia is waiting for the "right moment" to launch a cyber war.[59] Another assumption that could be made is that "either of the two camps starting a massive cyber-attack would without a doubt be seen as a crossing of the famous red line, which would inevitably lead to conflict escalation."[60] For Juliette Kayyem, the best explanation – so far – is that "maybe, much like military capacity, Russian cyber-capacity to destroy as compared to disrupt—disruptions we can handle—was overestimated."[61] Another factor could be the NATO Alliance's invocation of its collective security article in relation to any attack on critical infrastructure that has an impact on civilians, which she said may have had a "disciplining effect."[62]

---

56 SECU, *Evidence*, 7 June 2022, 1215 (David Shipley, Chief Executive Officer, Beauceron Security).

57 There have also been cyber incidents beyond Ukraine, including an operation that disrupted the majority of Viasat's European KA-SAT satellite communications service network. See Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*, based on information available as of 22 June 2022. The cyber threat bulletin also indicates that, "From as early as January 2022, evolving intelligence indicates that Russian cyber threat actors are exploring options for potential counterattacks against the United States, Canada, and other NATO/Five Eye allies, including against critical infrastructure."

58 SECU, *Evidence*, 7 June 2022, 1205 (Dr. Ken Barker).

59 SECU, *Evidence*, 3 May 2022, 1240 (Dr. Nora Cuppens, Professor, Polytechnique Montréal, As an Individual).

60 Ibid.

61 SECU, *Evidence*, 7 June 2022, 1210 (Juliette Kayyem).

62 Ibid.

Enhancing Resilience and Building Expertise

The Honourable Marco Mendicino, Minister of Public Safety, told the committee that cyber activities targeting systems that underpin Canada's critical infrastructure "are a constant concern."[63] Public Safety Canada works within government and internationally "to attribute malicious cyber-activity to state or state-sponsored actors when it can, with confidence, link the malicious activity to a particular actor."[64] In terms of the work that takes place within Canada, Minister Mendicino mentioned the framework provided by the *National Cyber Security Strategy*, which is in the process of being reviewed and renewed,[65] and he highlighted the technical advisory role of the Canadian Centre for Cyber Security. Furthermore, he indicated that the Royal Canadian Mounted Police (RCMP) now has a unit focused on law enforcement operations against cybercriminals.[66]

While recognizing measures the government has taken, witnesses outlined additional steps they believe could help to bolster Canada's cyber resilience and its preparedness to manage emergencies more broadly.

Some testimony touched on skills, knowledge, and research. Professor Etkin suggested that Canada could benefit from "an interdisciplinary national centre of excellence on disaster studies." Regarding critical infrastructure, he told the committee that the "interconnections" between critical infrastructure are not well understood. Professor Etkin would therefore recommend funding a long-term study that would examine "the interconnections and vulnerabilities of critical Canadian infrastructures."[67]

For cyber security, Professor Barker identified the "critical shortage" of experts as the key issue.[68] Dr. Frédéric Cuppens, Professor at Polytechnique Montréal, emphasized the importance of developing a program for bachelor's and master's degrees, but also certificates, micro-programs, and ongoing training for professional development. At the research level, he said, work on "cyber weapons as a deterrent" could be expanded.[69] Research could address such issues as the attribution of cyber attacks, the monitoring of

63 SECU, *Evidence*, 9 June 2022, 1105 (the Honourable Marco Mendicino, Minister of Public Safety).

64 Ibid.

65 See Public Safety Canada, *Secure and Prosperous Digital Canada: Consulting on Canada's Approach to Cyber Security*.

66 See Royal Canadian Mounted Police (RCMP), *The National Cybercrime Coordination Unit (NC3)*.

67 SECU, *Evidence*, 7 April 2022, 1100 (Professor David A. Etkin).

68 SECU, *Evidence*, 7 June 2022, 1205 (Dr. Ken Barker).

69 SECU, *Evidence*, 3 May 2022, 1245 (Dr. Frédéric Cuppens, Professor, Polytechnique Montréal, As an Individual).

internal threats in relation to targeted infrastructure, the measurement of the full impact of a cyber attack, and the ability to resist such attacks.[70]

Cyber incident reporting and the implementation of cyber standards were other key themes from the committee's study. Beyond obligations under the *Personal Information Protection and Electronic Documents Act*, BlackBerry emphasized in its brief that there are no regulations in Canada "to govern – much less obligate – critical infrastructure operators and owners to report, prepare for, and prevent cybersecurity incidents."[71] While port administrators, marine and ferry facilities are required by regulation to report cyber incidents to law enforcement and Transport Canada, "there is no specific reporting period, and there is no guidance on the cybersecurity measures that they should put in place."[72]

When asked about this issue, the Chief of the CSE, Caroline Xavier, explained the current practice as follows:

> We're also working closely with organizations that report having been victims of cyber-attacks. However, as you said, many organizations don't report it. Nevertheless, we continue to discuss it openly with industry.
>
> We do a lot of outreach and awareness sessions to let people know that we're there to provide the support they need. We also put out a lot of advisories to explain the risks so that they can protect themselves and prevent possible attacks.
>
> We're concerned about this, obviously.[73]

She also indicated that this challenge was not limited to Canada.[74]

BlackBerry informed the committee that the U.S. government acted in the wake of cyber incidents that targeted U.S. critical infrastructure, including through an executive order that mandates "preventive cybersecurity measures such as the implementation of a Zero Trust Architecture across US government agencies and measures to strengthen the

70 Ibid.

71 BlackBerry, written brief, 15 June 2022, p. 1.

72 Ibid.

73 SECU, *Evidence*, 6 October 2022, 1125 (Caroline Xavier).

74 Ibid.

security of the government's software and IT supply chain."[75] Moreover, pursuant to the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, designated critical infrastructure entities in the United States will be required "to report cybersecurity incidents to government within 72 hours, and ransomware payments within 24 hours."[76] According to BlackBerry, the European Union has put in place similar requirements for critical infrastructure owners and operators and "plans to levy fines of up to €10M or 2 percent of annual revenue (whichever is greater), to those that are found non-compliant."[77]

Dr. Frédéric Cuppens referenced the requirements that have been put in place in France. There, once a company whose activities relate to a critical sector has been designated an "operator of vital importance," it is "required to meet a certain number of obligations to comply with the [country's] military programming law." While this requirement applies to large companies, he noted that "it also includes small or medium-sized ones if they engage in activities related to a critical sector."[78]

On this issue, David Shipley shared the view that Canada is "lagging behind the United States and Europe."[79] He urged the implementation of mandatory cyber-incident reporting, going beyond federally regulated industries to also include "health care as well as vital supply chains, including manufacturing and food." Shipley explained that most organizations will not engage voluntarily with the Government of Canada about such incidents because of the perception held by legal, risk and insurance advisers that there would be "limited gains" and "much to lose" from doing so.[80]

Michael Doucet, Executive Director, Office of the Chief Information Security Officer, Optiv Canada Federal, spoke in favour of an approach that would apply to "select critical

---

75 BlackBerry, written brief, 15 June 2022, p. 2. For additional background, see United States, The White House, *Executive Order on Improving the Nation's Cybersecurity*, 12 May 2021; and Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies*, 26 January 2022. The Zero Trust Model is a shift in approach from verification at the perimeter to "continual verification of each user, device, application, and transaction."

76 BlackBerry, written brief, 15 June 2022, p. 2. Mandatory rulemaking activities must be completed before the Act's reporting requirements go into effect. See United States, Cybersecurity & Infrastructure Security Agency, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*.

77 BlackBerry, written brief, 15 June 2022, p. 2. For additional background, see European Commission, *Commission welcomes political agreement on new rules on cybersecurity of network and information systems*, News release, 13 May 2022.

78 SECU, *Evidence*, 3 May 2022, 1320 (Dr. Frédéric Cuppens).

79 SECU, *Evidence*, 7 June 2022, 1215 (David Shipley).

80 Ibid.

infrastructure players." After noting the expansive scope of the 10 critical infrastructure sectors in Canada, he explained his call for a nuanced approach by remarking, "Are we going to ask for mandatory reporting from a dairy farmer with 60 head of cattle?"[81]

If the move were made to mandatory reporting, Doucet believes the reporting and the actions taken in response would need to be safeguarded, while also finding a way to share the knowledge nationally. From his perspective, "the last thing we want to do is have organizations report on breaches and have that disseminated where we don't want it disseminated." He cautioned the committee: "When you aggregate all that information, that's a lot of information."[82]

Jennifer Quaid believes that the Government of Canada could facilitate information-sharing through what she characterized as "safe harbour" legislation. It would be designed to encourage businesses and organizations to voluntarily share information, beyond statutory requirements, "by protecting them from legal repercussions."[83]

Another issue is the voluntary nature of cyber standards. David Shipley would like to see cyber-hygiene standards made mandatory nationally. While he characterized CyberSecure Canada – a certification program for small and medium-sized organizations – as a "great start," he maintained that "voluntary uptake will continue to be low." There are lessons to be drawn, Shipley suggested, from programs in the United Kingdom that have tied access to government procurement with the achievement of basic cybersecurity standards.[84]

Referencing the role played by the Agence nationale de la sécurité des systèmes d'information in France, Dr. Nora Cuppens called for a "similar institution" in Canada, which would operationalize "the protection of our systems and infrastructure." In addition to cyber-surveillance, the institution she envisions "would push for regulation and verify that the rules are being applied."[85]

A final consideration in relation to resilience and expertise is the cybersecurity capacity of actors beyond the federal government and large enterprises, as noted earlier. From David Shipley's perspective, entities in Canada's subnational public sector require "dedicated funding from the federal government to improve their security as quickly as

81 SECU, *Evidence*, 3 May 2022, 1225 (Michael Doucet, Executive Director, Office of the Chief Information Security Officer, Optiv Canada Federal).

82 Ibid.

83 SECU, *Evidence*, 3 May 2022, 1140 (Jennifer Quaid).

84 SECU, *Evidence*, 7 June 2022, 1215 (David Shipley).

85 SECU, *Evidence*, 3 May 2022, 1305 (Dr. Nora Cuppens).

possible." In the private sector, he said, small- and medium-sized enterprises "desperately need help affording the security tools they need in an increasingly hostile environment."[86]

Aaron Shull, Managing Director, Centre for International Governance Innovation, noted that the CSE has already established baseline cyber security controls for small and medium organizations.[87] He suggested that, if companies implemented those baseline controls, "chances are that they'd be fine because no state-level threat actor is going to go after a small business, especially if they're hard to get into. It's just not worth it."[88] Nevertheless, Mr. Shull told the committee that most companies have not done so. To incentivize them, he "would consider looking at a tax credit of some sort."[89]

Given the threat that malicious cyber activity could pose to Canada's national interests, including the services that Canadians rely on for their safety and well-being, the committee agrees that it is time to make reporting of serious cyber incidents mandatory for critical infrastructure, with careful thought given to the administration of the required reporting. On this issue, and based on all the testimony it received in relation to malicious cyber activity and critical infrastructure protection, the committee recommends:

Recommendation 2

That the Government of Canada work with provincial and territorial partners to create and promote accredited post-secondary cyber defence training programs.

Recommendation 3

That the Government of Canada, in consultation with relevant stakeholders, build on the *National Cyber Security Strategy* to ensure that –

- **operators and enterprises of all sizes connected to critical infrastructure have the cyber security experts, expertise, and resources they need to defend against and recover from malicious cyber activity; and**

- **cyber security standards are met and reported on.**

---

86 SECU, *Evidence*, 7 June 2022, 1215 (David Shipley).

87 For additional information, see Canadian Centre for Cyber Security, *Introduction to the baseline controls*.

88 SECU, *Evidence*, 17 May 2022, 1120 (Aaron Shull, Managing Director, Centre for International Governance Innovation).

89 Ibid.

Recommendation 4

That the Government of Canada instruct the Communications Security Establishment to broaden the tools used to educate small- and medium-sized enterprises about the need to adopt cyber security standards.

Recommendation 5

That the Government of Canada establish incentives, including – but not limited to – an accelerated capital cost allowance or other tax measures, for small- and medium-sized enterprises to make the investments necessary to follow the Communications Security Establishment's baseline cyber security controls.

Recommendation 6

That the Government of Canada require critical infrastructure operators – from appropriately designated sectors – to prepare for, prevent and report serious cyber incidents, and that it put in place accompanying reporting timelines, technical assistance, and protections for the information that would be reported to the Communications Security Establishment and the lessons-learned that would be shared with industry, and that it then table annual reports to Parliament on these efforts.

Ensuring a Coordinated, Coherent and Effective Response

When reflecting on Canada's overall security posture, Dr. Wesley Wark, Senior Fellow at the Centre for International Governance Innovation, identified Canada's capacity to defend against cyber attacks and probes threatening its critical infrastructure as a "top-tier threat."[90] However, the committee also learned that some 12 federal departments and agencies have cyber responsibilities.[91] Part of the mandate of the CSE, for example, is to be "the country's lead technical authority for cybersecurity."[92] It reports to the Minister of National Defence. The "policy lead for cybersecurity" is Public Safety Canada.[93]

90 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark, Senior Fellow, Centre for International Governance Innovation).

91 BlackBerry, written brief, 15 June 2022, p. 5.

92 SECU, *Evidence*, 6 October 2022, 1105 (Caroline Xavier). The legislated mandate of the CSE – Canada's signals intelligence agency – encompasses five aspects: foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations, and technical and operational assistance.

93 Public Safety Canada, *Cyber Security in the Canadian Federal Government*.

In addition to the policy instruments that exist, Minister Mendicino indicated that the Deputy Minister of Public Safety plays a "chairing role that brings together different officials across the government," as a means "to share information, coordinate efforts, identify threats and determine how best to introduce mitigating strategies."[94] The minister acknowledged the importance of continuing these efforts "to avoid a kind of stovepiping, which can lead to the fracturing of a coordinated response."[95] Noting the step that was taken in the United States to establish a White House National Cyber Director, BlackBerry wrote that Canada "should consider [e]stablishing a Cabinet position responsible for ensuring government-wide coherence and action on cybersecurity."[96]

As a starting point, the committee believes that a review of Canada's machinery of government in relation to cybersecurity should be undertaken with the objective of ensuring there are no seams or gaps in Canada's cyber preparedness and defences.

Based on these considerations, the committee recommends:

Recommendation 7

That the Government of Canada ensure that the cyber roles, responsibilities, and structures that exist across the federal government maximize coherence, coordination, and timely action in relation to cybersecurity, and that it submit annual reports to Parliament on these efforts.

Recommendation 8

That the Government of Canada emphasize the importance and modernization of cybersecurity in departmental mandates.

Recommendation 9

That the Government of Canada explore options for a Canada–United States cyber defence command structure.

94 SECU, *Evidence*, 9 June 2022, 1130 (the Honourable Marco Mendicino).

95 Ibid.

96 BlackBerry, written brief, 15 June 2022, p. 5.

Disinformation

Several witnesses discussed Russia's information operations, particularly the spread of disinformation. While similar views were expressed about the methods involved and the objectives behind these disruptive operations, there were different perspectives about their impact and how they should be countered.

Russia's Tactics and Intentions

Marcus Kolga, Senior Fellow at the Macdonald-Laurier Institute, explained that Russia's use of information warfare has built on the expertise the Soviet Union developed during the Cold War. He conveyed that President Putin, a former intelligence officer, "restored cognitive warfare 20 years ago as a primary tool to repress his own people, undermine Western democracies and erode cohesion within the NATO alliance."[97]

Kolga sees the objectives of Putin's cognitive warfare as being "mostly agnostic of any mainstream ideology," but he indicated that "it does align with his support for both far-left and far-right groups."[98] To achieve societal polarization, issues identified as being sensitive are amplified by a "complex Russian information laundromat," which includes Russian state media and a "constellation of proxy groups and platforms, including right here in Canada, that regurgitate this information."[99]

According to Dr. Ahmed Al-Rawi, Assistant Professor at Simon Fraser University, Russia's government "has an ongoing interest in interfering in Canadian politics using a variety of information operations, propaganda and disinformation."[100] After examining datasets from Facebook and Twitter that were released a few years ago, Professor Al-Rawi determined that "Russian trolls were the most invested in targeting Canada, far more than Iranian and other state-run trolls from China and Saudi Arabia were."[101] He believes

97 SECU, *Evidence*, 7 April 2022, 1210 (Marcus Kolga, Senior Fellow, Macdonald-Laurier Institute, As an Individual).

98 Ibid.

99 Ibid.

100 SECU, *Evidence*, 5 April 2022, 1210 (Dr. Ahmed Al-Rawi, Assistant Professor, Simon Fraser University, As an Individual). The Government of Canada defines disinformation as "deliberately false information." See Government of Canada, *Canada's efforts to counter disinformation - Russian invasion of Ukraine*.

101 SECU, *Evidence*, 5 April 2022, 1210 (Dr. Ahmed Al-Rawi).

that, in addition to sowing division and creating tension, the purpose of these information operations is to "confuse people about what is real or fake."[102]

A key challenge is the variety of communications platforms and methods that are used. The state-backed outlet *RT* – formerly known as *Russia Today* – was removed from the list of services and stations authorized for broadcasting in Canada.[103] Nevertheless, Dr. Veronica Kitchen, Associate Professor in the Department of Political Science, University of Waterloo, indicated that Russian disinformation campaigns are "still prevalent on social media and in forums frequented by adherents of other kinds of populist conspiracy."[104]

Professor Al-Rawi highlighted the social media activity of Russia's diplomatic missions, which he said have been Russia's "main means to spread propaganda" through social media platforms.[105] According to him, Russia's diplomatic presence online is being used to weaponize fact-checking practices. He said the Russian embassy "is trying to create a direct link with the Canadian public that cannot be blocked by the [Canadian Radio-television and Telecommunications Commission]," including through direct messages.[106]

Contrasting what has been done by other NATO Allies and European Union partners, who have expelled more than 500 Russian officials from their territory since the invasion of Ukraine, Dr. Wesley Wark noted that the government "has yet to take any action" to expel Russian intelligence officers from Canada. It is his view that "Canada needs to take forceful action to impede Russian espionage and interference operations."[107]

The Impact of Disinformation

Witnesses had different perspectives regarding the impact of Russia's disinformation and the degree to which it poses a threat to Canada's national security and public safety. Dr. James Fergusson is "not one who believes that Russian disinformation, Chinese disinformation or anyone's disinformation campaigns really have much of an effect at

102 Ibid.

103 Canadian Radio-television and Telecommunications Commission, *Broadcasting Decision CRTC 2022-68*, 16 March 2022.

104 SECU, *Evidence*, 5 April 2022, 1115 (Dr. Veronica Kitchen, Associate Professor, Department of Political Science, University of Waterloo, As an Individual).

105 SECU, *Evidence*, 5 April 2022, 1210 (Dr. Ahmed Al-Rawi).

106 Ibid.

107 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark).

all." He sees the threat as "highly overblown and exaggerated."[108] However, Professor Al-Rawi told the committee that the influence of Russian disinformation on the Canadian population has not yet been fully quantified or understood.[109]

According to Professor Veronica Kitchen, "Russian disinformation campaigns connect the invasion of Ukraine to QAnon and other deep state conspiracy theories that feed hate crimes and distrust of the Canadian government."[110] While Professor Kitchen said there is "a risk that adherents of these conspiracy theories will commit violent acts," she reminded the committee that "the political action of supporters of populist extremism can also have harmful effects that don't escalate to the level of security threat or crime."[111] It is Professor Kitchen's view that "only a narrow swath of Canadians will be attracted to these ideas and influenced by Russian misinformation."[112] Nevertheless, she also noted that these ideas are "easily amplified by bots" (i.e., things that act automatically through Internet platforms), which may necessitate long-term solutions.[113]

Professor Christian Leuprecht stated that, "Russian misinformation and disinformation on open source social media platforms are undermining police and the sitting government."[114]

In consideration of the above testimony, the committee recommends:

Recommendation 10

That the Government of Canada examine the full extent of Russian disinformation – and other state-backed disinformation – targeting Canada, the actors, methods, messages and platforms involved, and the impact this disinformation is having on the Canadian population and Canada's national security, and that it report its findings to Parliament annually.

108 SECU, *Evidence*, 5 April 2022, 1105 (Dr. James Fergusson).

109 SECU, *Evidence*, 5 April 2022, 1235 (Dr. Ahmed Al-Rawi).

110 SECU, *Evidence*, 5 April 2022, 1115 (Dr. Veronica Kitchen).

111 Ibid.

112 Ibid.

113 Ibid.

114 SECU, *Evidence*, 17 May 2022, 1100 (Dr. Christian Leuprecht).

Determining How to Respond

Even if the overall purpose of Russian disinformation is clear, the most effective way of countering these campaigns is less certain.

In Professor Al-Rawi's view, "the best way to protect Canadians from this kind of disinformation is by debunking, by fact-checking, anything that is related to Canada or Canadians in relation to the war on Ukraine."[115] Dr. Paul Goode, McMillan Chair of Russian Studies at Carleton University, also emphasized the importance of education and training. Because disinformation "typically plays on emotive characteristics or emotive themes," he thinks that "having a dispassionate response, a trained response, is perhaps the most efficient way to be able to counter it, because widespread suppression is not a democratic response to this kind of threat."[116]

In Professor Kitchen's view, while media literacy can help in some instances, working with private companies and Canada's allies "to improve our technological responses to disinformation is essential."[117] She cited as positive steps the government's recent creation of an expert advisory group on online safety[118] and its formation of the Security and Intelligence Threats to Elections Task Force.[119] Dr. Kitchen indicated that targeting bots might be an area where regulation "does become helpful," working with companies that are open to "trying to control extremism" on their platforms.[120]

These comments echoed Aaron Shull's advice to the committee, which was to focus on "amplification." Given that "39% of all Internet traffic is from bad bots,"[121] his testimony suggested that efforts could concentrate on curbing the money that is powering this automated traffic (i.e., by making it harder for the trolls who are controlling the "bad

115 SECU, *Evidence*, 5 April 2022, 1240 (Dr. Ahmed Al-Rawi). The Government of Canada publishes a "sample" of Russian disinformation about Ukraine, which is compared against the facts. See Government of Canada, *Countering disinformation with facts - Russian invasion of Ukraine*.

116 SECU, *Evidence*, 7 April 2022, 1135 (Dr. Paul Goode, McMillan Chair of Russian Studies, Carleton University, As an Individual).

117 SECU, *Evidence*, 5 April 2022, 1115 (Dr. Veronica Kitchen).

118 See Canadian Heritage, "Expert advisory group," *The Government's commitment to address online safety*.

119 See Government of Canada, *Protecting democracy*. Minister Blair advised the committee that he had not received any information that Russia was involved in any effort at foreign interference in the 2021 federal election. See SECU, *Evidence*, 2 June 2022, 1110 (the Honourable Bill Blair).

120 SECU, *Evidence*, 5 April 2022, 1155 (Dr. Veronica Kitchen)

121 SECU, *Evidence*, 17 May 2022, 1100 (Aaron Shull).

bots" to get paid).[122] In this regard, he pointed to the model of the sanctions that have been imposed on Russia since it invaded Ukraine. Shull also discussed the technical architecture of the Internet, indicating that "large bot farms" could be addressed through the domain name system. Such "bad bots" could also be defined internationally, he said, with action then taken to limit their flow.[123]

Other testimony placed greater emphasis on the responsibilities of the digital service platforms. While acknowledging concerns that would likely arise in relation to freedom of expression, Professor Errol Mendes encouraged Canada to start looking at what the European Union is proposing in terms of putting the onus on those platforms "to have annual assessments and independent audits, and ultimately to back those up with a regulatory framework that could potentially have massive fines."[124]

In addition to reiterating the recommendations pertaining to digital safety in its report on ideologically motivated violent extremism (IMVE),[125] the committee recommends:

Recommendation 11

That the Government of Canada, in collaboration with allies and domestic partners, continue to expose and counter Russian and other state-backed disinformation campaigns targeting Canadians.

Recommendation 12

That the Government of Canada work with experts, Internet Service Providers, social media platforms and international partners to counteract online bots that are amplifying state-sponsored disinformation, and that it report the findings and actions to Parliament.

Support for independent voices might be another tool. Dr. Paul Goode urged Canada to "provide refuge for scholars, journalists and activists who are persecuted for opposing Russia's war." From his perspective, the Russian diaspora are needed "as allies rather than bystanders," a cause that he said can be advanced "by providing shelter for Russia's moral and intellectual leaders."[126]

122 Ibid., 1130.

123 Ibid., 1100.

124 SECU, *Evidence*, 17 May 2022, 1210 (Professor Errol Mendes).

125 SECU, *The Rise of Ideologically Motivated Violent Extremism in Canada*, sixth report, June 2022.

126 SECU, *Evidence*, 7 April 2022, 1105 (Dr. Paul Goode).

Dr. Alexander Cooley, Claire Tow Professor of Political Science at Barnard College and Academy Adjunct Faculty at Chatham House, also drew attention to those who have left Russia in the wake of its war against Ukraine. He said that independent Russian media outlets are trying to operate from the Baltic states or via Telegram, and information technology workers have fled to places like Georgia, Armenia and Uzbekistan, while academics and analysts are "looking for new types of affiliations and academic homes." According to Dr. Cooley, these new networks could be enhanced and strengthened "as they try to promote independent thought and affect, as much as they can from outside, the disinformation propaganda within [Russia]." Policies in support of those efforts would aim to be "a force multiplier as the Kremlin tries to decouple from the West, to ensure that these independent and critical voices can be encouraged from outside of the country."[127]

Based on these considerations, the committee recommends:

Recommendation 13

That the Government of Canada support independent Russian journalists and academics who are working to expose the regime's propaganda and disinformation.

Wealth Derived from Repression

Some witnesses discussed the wealth that has been accumulated by the upper echelons of the Putin regime from the perspective of sanctions implementation.

In response to Russia's aggression against Ukraine, the Government of Canada has sanctioned more than 370 entities and more than 1,600 individuals since 2014 in accordance with the *Special Economic Measures Act*.[128] Other measures – pursued in concert with Canada's allies – have imposed restrictions on advanced goods and technology, as well as services.[129] The federal government has also introduced legislation to amend the *Immigration and Refugee Protection Act*, with the objective of

127 SECU, *Evidence*, 5 April 2022, 1215 (Dr. Alexander Cooley, Claire Tow Professor of Political Science, Barnard College, and Academy Adjunct Faculty, Chatham House, As an Individual).

128 Government of Canada, *Sanctions – Russian invasion of Ukraine*, accessed 7 February 2023.

129 Ibid.

ensuring that all foreign nationals designated for sanctions under the *Special Economic Measures Act* are inadmissible to Canada.[130]

Under the *Special Economic Measures Act*, the Commissioner of the RCMP is empowered to assist in matters related to the seizure or restraint of any property in Canada – that is owned, held or controlled directly or indirectly by a foreign state, any person in that foreign state, or a national of that foreign state who does not ordinarily reside in Canada – when an order has been made by the Governor in Council.[131] Every person in Canada and all Canadians outside Canada are required to disclose to the RCMP "the existence of property in their possession or control that is believed to be owned or controlled by a designated person."[132] Further to its information collection role, the RCMP reported on 23 December 2022 that, since 24 February 2022, the equivalent of approximately $122 million of assets in Canada had been effectively frozen, while the equivalent of approximately $292 million in financial transactions had been blocked further to the Act's Russia regulations.[133]

William Browder, who has campaigned internationally for targeted ("Magnitsky") sanctions against human rights violators, characterized the West's imposition of wide-ranging sanctions after Russia invaded Ukraine – in an effort "to cripple Vladimir Putin's war effort" – as an "impressive" response.[134] Even so, from his perspective, the problem lies with the amount of money that has been frozen. He estimates that, since 2000, Putin and other Russian elites "have taken a trillion dollars out of Russia and that money is sitting in the West." The amount frozen through sanctions, Browder said, is "a tiny, de minimis portion of that money that's been taken out of Russia."[135] The gap comes from tactics that are used to evade sanctions. Browder explained that individuals designated

130 SECU, *Evidence*, 9 June 2022, 1105 (the Honourable Marco Mendicino); Canada Border Services Agency, *Government to ban sanctioned Russians from entering Canada*, News release, 17 May 2022; and Bill S-8, An Act to amend the Immigration and Refugee Protection Act, to make consequential amendments to other Acts and to amend the Immigration and Refugee Protection Regulations, 44th Parliament, 1st Session. As the committee was finalizing its report, Bill S-8 had progressed through the Senate of Canada and was at Second Reading in the House of Commons.

131 *Special Economic Measures Act (S.C. 1992, c. 17)*, subsections 4(1) and 6.2(1).

132 RCMP, *Update on the reporting of frozen assets under the Special Economic Measures Act - Russia Regulations*, Statement, 23 December 2022. In this context, the term "designated persons" refers to individuals and entities who are subject to asset freezes and dealings prohibitions (i.e., sanctions) pursuant to the *Special Economic Measures Act, S.C. 1992, c. 17* and the *Special Economic Measures (Russia) Regulations, SOR/2014-58*.

133 RCMP, *Update on the reporting of frozen assets under the Special Economic Measures Act - Russia Regulations*, Statement, 23 December 2022.

134 SECU, *Evidence*, 17 May 2022, 1200 (William Browder).

135 Ibid.

for sanctions have used various measures and structures – e.g., holding and trust companies, family members and custodians – to keep their money hidden.[136]

The testimony of Professor Alexander Cooley also addressed these Russian oligarchs, which he identified as one of the transnational networks that "reverberate back into Western societies."[137] In addition to the challenges associated with asset freezes, he suggested that reputations must be considered. Here, Dr. Cooley drew attention to the "service professionals" in Western countries who take the money of oligarchs, "put them into luxury real estate, purchase shell companies and hide them in complex networks of bank accounts."[138] There are also public relations agencies, reputation management firms and lobbyists, he indicated, "who try to recast them, not as politically exposed persons with links to the Kremlin but rather as global philanthropists."[139]

Dr. Cooley believes that "the move to a federal beneficial ownership registry is an absolute national security requirement."[140] The idea behind such registries is to include information on the natural persons who ultimately own or control a corporation – i.e., the actual individuals who are the corporation's beneficial owners – rather than their legal ownership, which could be a trust or another corporation.[141] Dr. Cooley raised this issue because he is of the view that "every country needs to know what the anonymous shell companies are and who's behind them that are buying luxury real estate but also other assets."[142]

Mr. Browder put forward a specific proposal to address the role played by service professionals, as discussed above. He suggested that sanctions legislation could be amended to stipulate that any professional service firm that has "provided information, advice or consultation on the holding and structuring of assets of a person who has been sanctioned by the Canadian government" would be required to "explain the information"

136 Ibid.

137 SECU, *Evidence*, 5 April 2022, 1215 (Dr. Alexander Cooley).

138 Ibid.

139 Ibid.

140 Ibid., 1300.

141 Innovation, Science and Economic Development Canada, *Public consultations on strengthening corporate beneficial ownership transparency in Canada: What we heard*, 6 April 2021.

142 SECU, *Evidence*, 5 April 2022, 1300 (Dr. Alexander Cooley).

they have on the sanctioned person. Imposing this requirement, Browder argued, would effectively turn such service professionals "into whistle-blowers by law."[143]

The committee recognizes that the legal, policy and enforcement issues connected with sanctions are complex. The committee also recognizes the national security implications of wealth, reaching Canada, that is derived from the corruption of repressive regimes. While holding the view that further study of these issues is warranted, the committee recommends:

Recommendation 14

That the Government of Canada urgently work with its international and domestic partners to combat sanctions evasion, including by taking appropriate steps to ensure all property of sanctioned Russian individuals and entities situated in Canada has been identified and frozen.

Military Threats

While much of the committee's study focused on non-conventional threats to Canada's security, including Russia's tools of disruption, some witnesses focused their remarks on defence. Testimony highlighted the need for investments in surveillance and deterrence capabilities in the face of advanced weaponry that could be launched against targets in North America from long range. This reality was put in stark terms by General Eyre, who told the committee that the "distance and geographic isolation that Canada has enjoyed for so long is no longer a viable defensive strategy."[144]

Advanced Weaponry and Deterrence by Denial

Building on the support Canada has provided to Ukraine and allies in eastern Europe, Dr. David Perry is of the view that Canada "should act with similar urgency and ingenuity to ensure that Canada and North America are better defended against potential Russian aggression closer to home." To make this case, he noted that, following two decades of military modernization, "Russian aircraft, ships and submarines can now carry advanced cruise missiles that could accurately hit targets in North America at long ranges, as can other long-range Russian missiles, including hypersonic glide vehicles."[145] The long-range missiles Russia possesses and those still being developed, Dr. James Fergusson

143 SECU, *Evidence*, 17 May 2022, 1235 (William Browder).

144 SECU, *Evidence*, 6 October 2022, 1105 (Gen Wayne D. Eyre).

145 SECU, *Evidence*, 5 April 2022, 1220 (Dr. David Perry).

explained, are "nuclear and conventional capable."[146] According to him, there are "significant gaps and vulnerabilities which have existed for over a decade in terms of the ability of NORAD, and as a result Canada, to be able to detect these threats, to track them, to discriminate, and then to be able to cue interception capabilities."[147]

Strategic implications arise from such gaps and vulnerabilities. According to Dr. Andrea Charron, "Russia has come to believe it can exploit our continental defence vulnerabilities, thus emboldening it to undertake a regional challenge by threatening actions to deter an overseas response." Russia has been further emboldened, she suggested, by North America's multi-decade reliance on "deterrence by punishment." What that means, she explained, is that "we promise a cost so high to adversaries that they wouldn't dare attack us." Dr. Charron warned that relying on this approach alone "risks uncontrollable escalation and narrows our response options considerably." She argued for a shift toward "deterrence by denial." Realizing this shift would mean ensuring that North America is "resilient to a variety of attacks, especially below the threshold of use of force," and ensuring that "attacks are identified and addressed quickly to prevent escalation." Put another way, Dr. Charron believes there is a need "to change Russia's calculus to strip away the benefits of attacks on North America, rather than focusing solely on increasing the costs."[148]

The protection of critical infrastructure and cyber resilience are also part of deterrence by denial. Professor Jonathan Paquin explained that this conception of deterrence aims to "discourage the Kremlin from carrying out such attacks because it would know that the probability of success is low."[149] As General Eyre put it, the idea is to avoid giving Canada's adversaries any "soft targets."[150]

Achieving deterrence by denial from a defence perspective will require, according to Dr. Charron, that there are "no command seams" in North America that can be exploited

146 SECU, *Evidence*, 5 April 2022, 1105 (Dr. James Fergusson).

147 Ibid.

148 SECU, *Evidence*, 7 April 2022, 1205 (Dr. Andrea Charron).

149 SECU, *Evidence*, 3 May 2022, 1250 (Dr. Jonathan Paquin).

150 SECU, *Evidence*, 6 October 2022, 1145 (Gen Wayne D. Eyre).

or through which Canada and the United States can be constrained.[151] Specific capabilities will also be required, including new sensors "for radar's digital transformation" and the means of creating "common operating pictures that can be shared efficiently and appropriately." Dr. Charron indicated there is also a need to integrate data and information "from all domains, working with a range of allies and partners, including with civilian agencies and private companies." In her analysis, the goal of modernizing continental defence, to achieve deterrence by denial, is "to alter adversarial perceptions so that North America cannot be held hostage."[152]

There are specific concerns about the current ability to track all threats in the Arctic, a region that Dr. Adam Lajeunesse of St. Francis Xavier University, framed as an avenue of approach through which Russia could project power. He believes the priority should be upgrading NORAD's aerospace and maritime detection capabilities. What is needed, in his view, is "all-domain awareness," including above-ice and under-ice detection capabilities. That would enable the tracking of incoming Russian weapon systems, but also hybrid threats posed by other actors, such as illegal fishing vessels. In this regard, Dr. Lajeunesse noted that the Arctic "is opening up, and an ice-free or ice-reduced future means that more activity must be monitored and policed." According to him, elements of an all-domain system – including satellites and Arctic patrol ships – have been put in place, while others have been under development for years. However, Dr. Lajeunesse suggested there "has never been a concerted push to realize a system of systems."[153]

In a 2021 joint statement, Canada and the United States agreed to modernize, improve, and better integrate the capabilities required for NORAD to maintain persistent awareness – and understanding – of potential threats to North America in the aerospace and maritime domains, deter acts of aggression, and respond quickly and decisively when required.[154] With the objective of ensuring there are no gaps that could be

151 SECU, *Evidence*, 7 April 2022, 1205 (Dr. Andrea Charron). Later in the meeting, in reply to a question, Dr. Charron cited the example of cyberspace where there are "particular mandates for agencies and no one organization that's responsible for getting an overall cyber operation picture," which means – according to her – that "we really have no idea of where we are being hit with cyber-attacks." Referring to the situation in Canada, she commented that "we simply don't have a cyber-command, like the U.S. has." Commenting more generally in response to a separate question, Dr. Charron noted the tendency "to think there is the defence domain and there is the security and safety domain." Her point is that "we need to bring these together. We cannot work in isolation anymore." See SECU, *Evidence*, 7 April 2022, 1230 and 1240 (Dr. Andrea Charron).

152 SECU, *Evidence*, 7 April 2022, 1205 (Dr. Andrea Charron).

153 SECU, *Evidence*, 7 April 2022, 1110 (Dr. Adam Lajeunesse, Irving Shipbuilding Chair on Canadian Arctic Marine Security, Brian Mulroney Institute of Government, St. Francis Xavier University, As an Individual).

154 National Defence, *Joint Statement on Norad Modernization*, 14 August 2021.

exploited in the defence of North America, in the near or the longer term, the committee recommends:

Recommendation 15

That the Government of Canada accelerate the modernization of the North American Aerospace Defense Command (NORAD).

Defence Capacity and Readiness

Beyond specific military threats to North America, some testimony also addressed Canada's broader defence capacity and readiness.

Dr. Perry observed that, despite the Government of Canada's long-standing focus on improvements to continental defence,

> the pace of implementation has fallen short of expectations. Money has gone unspent year after year, and needed equipment projects have been delayed. The war in Ukraine is demonstrating the importance of having a capable modern military at the moment, when Russia or any other military power precipitates an international crisis, not when we in Canada can get around to doing it.[155]

Building on this point, Dr. Perry further argued that "a bigger defence budget is needed now." In his opinion, "Canada's current defence spending plans are insufficient to deal with the threats posed by Russia and other powers like China."[156] The target set by the NATO Allies to spend 2% of their gross domestic product (GDP) on defence – by 2024[157] – is an "imperfect" measure of contributions, Dr. Perry suggested, but one "that all allies, including Canada, agreed to meet."[158]

The view of Dr. Lajeunesse is that 2% of GDP should be the "minimum target" for Canada's defence spending. However, he would like to see those funds more deliberately targeted in reflection of the current era of strategic competition.[159] According to NATO,

---

155 SECU, *Evidence*, 5 April 2022, 1220 (Dr. David Perry).

156 Ibid.

157 In 2014, the North Atlantic Treaty Organization (NATO) Allies agreed that any Allies whose proportion of gross domestic product spent on defence was below the 2% guideline would aim to move towards the guideline within a decade. See NATO, *Funding NATO*.

158 SECU, *Evidence*, 5 April 2022, 1220 (Dr. David Perry).

159 SECU, *Evidence*, 7 April 2022, 1115 (Dr. Adam Lajeunesse).

Canada was estimated to be allocating 1.27% of its GDP for defence expenditure in 2022, placing it 24th out of 29 Allies when that spending metric is used.[160]

Rather than focusing on a spending figure, Dr. Charron stated that consideration should be given to "whether we have the capacity to spend those monies." On this point, she noted that the Canadian Armed Forces were down some 10,000 personnel.[161] Dr. Perry addressed this same issue. Quickly modernizing air and naval capabilities that were mostly purchased in the 1980s, he said, requires increased capacity in Canada's defence procurement system. Dr. Perry observed that Canada is attempting to make up for the years after the Cold War, "when we invested insufficiently in our forces," with a procurement workforce "that was cut in half in the 1990s and never fully rebuilt."[162]

Capacity strains are not limited to the defence procurement workforce. The Chief of the Defence Staff, General Wayne Eyre, told the committee that he was "very worried" about the Canadian Armed Forces' (CAF) numbers, which is why he has made reconstitution – i.e., their recovery, rebuilding and reequipment – the "priority effort."[163] On the same day that he appeared before the committee, General Eyre published a directive on reconstitution, which defined the problem as follows:

> Owing to personnel and staffing issues that have been compounded by the CAF's heavy commitment to operations, the negative effects of the COVID-19 pandemic, and a culture crisis, National Defence continues to lose its ability to deliver and sustain concurrent operations at the scope and scale necessary to achieve the strategic effects directed by the [Government of Canada].[164]

General Eyre explained the rationale for prioritizing reconstitution by expressing his concern that, "as the threats to the world security situation increase and as the threats at home increase, our readiness is going down within the Canadian Armed Forces."[165]

The committee's mandate is public safety and national security, and it is aware of the work being done by the Standing Committee on National Defence in respect of Canada's overall defence posture and the recruitment of personnel. Nevertheless, in

---

160 Note: there are 30 member countries in the NATO Alliance, but Iceland has no armed forces. NATO, Public Diplomacy Division, "Graph 3: Defence expenditure as a share of GDP (%)," *Defence Expenditure of NATO Countries (2014-2022)*, 27 June 2022.

161 SECU, *Evidence*, 7 April 2022, 1220 (Dr. Andrea Charron).

162 SECU, *Evidence*, 5 April 2022, 1220 (Dr. David Perry).

163 SECU, *Evidence*, 6 October 2022, 1115 (Gen Wayne D. Eyre).

164 National Defence, *CDS/DM Directive For CAF Reconstitution*, 6 October 2022.

165 SECU, *Evidence*, 6 October 2022, 1115 (Gen Wayne D. Eyre).

consideration of the essential roles the Canadian Armed Forces play in support of Canada's security, the committee recommends:

Recommendation 16

That the Government of Canada ensure it has both the capacity and the funding in place to realize Canada's defence procurement objectives, that it take all measures necessary to support the reconstitution of the Canadian Armed Forces, and that it report regularly to Parliament on its efforts to meet both these objectives.

Recommendation 17

That the Government of Canada honour its commitments to its NATO Allies and meet the Alliance's 2% defence spending target.

CONCLUSION: MANAGING AN INCREASINGLY COMPLEX THREAT ENVIRONMENT

While the committee's study focused on Canada's security posture in relation to Russia, some testimony addressed broader concerns about Canada's national security architecture. These policy and structural issues have become more salient amid a threat environment that has become increasingly complex and multifaceted.

An Integrated Approach to National Security

Dr. Wesley Wark cautioned the committee against taking a siloed approach with its study given that the threats "Canada faces include, but range well beyond, those posed currently by Russia."[166] After observing that defence, national security, and innovation policy are "all connected," Aaron Shull told the committee that "adversarial states are leaning into every crack they can with their state power." With adversaries treating these issues "as strategically connected," he argued, "we need to do the same."[167]

These connections were also made by General Eyre. He remarked that "Russia and China do not differentiate between peace and war," and will therefore "use all elements of national power, often acting just below the threshold of large-scale, violent conflict." Nonetheless, as has been shown with Russia's war against Ukraine, they are also "all too

166 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark).

167 SECU, *Evidence*, 17 May 2022, 1150 (Aaron Shull).

willing to cross that threshold."[168] In preparing for "the possibility of open conflict in traditional domains," General Eyre said, "we must also develop our capacity for confrontation in the cyber, space and cognitive domains." What is needed, he emphasized, is "an integrated approach to national security that combines military responses with diplomatic, economic and information actions at the local, regional, national and multinational levels."[169]

Adapting to Emerging Threats

In the face of this evolving threat environment, testimony from some witnesses suggested that Canada's national security architecture needs to further adapt and reinforce areas where cracks may have emerged. Specifically, Professor Christian Leuprecht is of the view that IMVE, seditious activity, and the impact of foreign actor interference "have been underestimated within the regional and national security architecture for some time."[170] He remarked that "[t]hresholds for actively investigating foreign actor interference by federal law enforcement agencies are rather high, often requiring major criminality or establishment of direct ties to a foreign state." From his perspective, that is "too high a bar," which has enabled "a permissible environment for foreign actor influence." Consequently, Professor Leuprecht wants to see Canada's national security architecture take on "a more active and assertive role in addressing IMVE and foreign actor interference."[171]

Besides specific types of threats, other testimony focused on the strategy that guides Canada's approach to national security, as well as the capacity underpinning it. Dr. Wark underlined "the stunning fact that Canada currently possesses no comprehensive national security strategy," with the "last and only one" having been produced in 2004.[172] Referencing the findings of a special report published by the Centre for International Governance Innovation, Dr. Wark also conveyed that the last review of Canadian national security capabilities had been conducted by an external examiner, in 1970.[173]

168 SECU, *Evidence*, 6 October 2022, 1100 (Gen Wayne D. Eyre).

169 Ibid., 1105.

170 SECU, *Evidence*, 17 May 2022, 1100 (Dr. Christian Leuprecht).

171 Ibid.

172 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark).

173 Ibid. See Aaron Shull and Wesley Wark, *Reimagining a Canadian National Security Strategy*, CIGI Special Report, Centre for International Governance Innovation (CIGI), 2021.

Dr. Wark believes that Russia's invasion of Ukraine "has presented us with an opportunity to rethink our approach to national security," which would recognize that "we live in a borderless world of threats." In the face of those threats, Dr. Wark said: "We must develop a sovereign capacity to understand their global points of origin and impact," equipped with "an enhanced global intelligence collection and assessment capacity."[174] Canada must also be prepared "to wield an offensive response capacity, including the use of intelligence and cyber-enabled tools."[175]

A reimagining of Canada's approach to national security could also involve greater transparency. Dr. Charles Burton expressed his concern about the disclosure practices of Canada's national security agencies, questioning whether they "have been sufficiently accountable to the public safety and national security concerns of Parliament as represented by this Commons committee."[176] His concern with transparency encompasses such issues as the prosecution of espionage and technology transfer to foreign states, as well as the ability to know whether "Canadians influential in Canada's policy process have received benefits from a foreign state that put them in a conflict of interest that threatens Canadian security and sovereignty." To address this specific issue, Dr. Burton believes Canada should urgently put in place a foreign agents registry act, or a measure equivalent to Australia's Foreign Influence Transparency Scheme Act.[177]

While recognizing the impact parliamentary committees can have on the "broad framework and governance and strategic issues," Dr. Wark noted the difficulties associated with parliamentary committees getting "into the details of intelligence and national security, because of the lack of access to classified information and classified briefings." From his perspective, that role "can be played by the National Security and Intelligence Committee of Parliamentarians, as Parliament intended."[178]

Within this larger debate, Aaron Shull offered two concrete suggestions as a starting point. He suggested there could be an annual threat assessment tabled in Parliament,

---

174 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark). Dr. Wark subsequently acknowledged the "limited foreign intelligence capabilities" of the CSE and Global Affairs Canada, but argued that there "is a lot more we could do." He commented that "Canada has often faced quiet criticism from its Five Eyes partners for being a bit of a freeloader, a free rider, in the alliance partnership." See Ibid., 1115.

175 SECU, *Evidence*, 17 May 2022, 1105 (Dr. Wesley Wark).

176 SECU, *Evidence*, 3 May 2022, 1135 (Dr. Charles Burton).

177 Ibid.

178 SECU, *Evidence*, 17 May 2022, 1135 (Dr. Wesley Wark).

and an annual discussion of intelligence priorities.[179] The CSE and the Canadian Security Intelligence Service produce annual and public reports, respectively, and there have been reports that address specific issues, including cyber threats and foreign interference threats to Canada's democratic process.[180] However, there is not an equivalent to the Annual Threat Assessment released by the U.S. Director of National Intelligence, which contains the U.S. intelligence community's strategic assessment of worldwide threats to U.S. national security.[181]

The testimony cited above suggested that a review of Canada's national security architecture is warranted with the objective of ensuring it is calibrated, resourced, and empowered to meet the emerging threat landscape. In the span of only three years, Canada and its allies have had to grapple with the fallout from a global pandemic, natural disasters that have become more frequent and intense with climate change, and the worst armed conflict in Europe since the Second World War, alongside accelerated technological change. Such rapidly evolving events and trends, in the committee's view, underline the importance of being guided by strategy and the ability to assess threats, capabilities and intentions, while preserving the capacity to look ahead. Therefore, the committee concludes its study by recommending:

Recommendation 18

That the Government of Canada put in place a register of foreign agents or a measure equivalent to the Australian Foreign Influence Transparency Scheme Act.

Recommendation 19

That the Government of Canada publish a comprehensive and integrated national security strategy, which takes into account an internal review of Canada's national security capabilities.

179 SECU, *Evidence*, 17 May 2022, 1135 (Aaron Shull). The CIGI report recommends that an annual statement on worldwide threats to Canada should be presented to Parliament by the prime minister and coordinated by the national security and intelligence advisor. See Aaron Shull and Wesley Wark, *Reimagining a Canadian National Security Strategy*, CIGI, 2021, p. 5.

180 See Canadian Security Intelligence Service, *Publications*; CSE, *Reports*; and Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023-2024*.

181 See United States, Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*.

Recommendation 20

That, pursuant to Section 34 of the *National Security and Intelligence Committee of Parliamentarians Act*, the House of Commons designate the Standing Committee on Public Safety and National Security as the House committee responsible for conducting a comprehensive review of the provisions and operation of the Act.

Recommendation 21

That the Government of Canada present to Parliament an annual assessment of threats to Canada's national security.

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
As an individual	2022/04/05	17
Dr. Ahmed Al-Rawi, Assistant Professor, Simon Fraser University		
Dr. Alexander Cooley, Claire Tow Professor of Political Science, Barnard College and Academy Adjunct Faculty, Chatham House		
Dr. James Fergusson, Deputy Director, Centre for Defence and Security Studies, University of Manitoba		
Dr. Robert Huebert, Associate Professor, Department of Political Science, University of Calgary		
Dr. Veronica Kitchen, Associate Professor, Department of Political Science, University of Waterloo		
Dr. David Perry, President, Canadian Global Affairs Institute		
As an individual	2022/04/07	18
Dr. Andrea Charron, Director and Associate Professor, Centre for Defence and Security Studies, University of Manitoba		
David A Etkin, Professor, Disaster and Emergency Management, York University		
Dr. Paul Goode, McMillan Chair of Russian Studies, Carleton University		
Marcus Kolga, Senior Fellow, Macdonald-Laurier Institute		
Dr. Adam Lajeunesse, Irving Shipbuilding Chair on Canadian Arctic Marine Security, Brian Mulroney Institute of Government, St. Francis Xavier University		

Organizations and Individuals	Date	Meeting
As an individual	2022/05/03	21
Dr. Charles Burton, Senior Fellow, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute		
Dr. Frédéric Cuppens, Professor, Polytechnique Montréal		
Dr. Nora Cuppens, Professor, Polytechnique Montréal		
Dr. Jonathan Paquin, Full Professor, Department of Political Science, Université Laval		
Canadian Cyber Threat Exchange	2022/05/03	21
Jennifer Quaid, Executive Director		
Optiv Canada Federal	2022/05/03	21
Michael Doucet, Executive Director, Office of the Chief Information Security Officer		
As an individual	2022/05/17	25
William Browder, Chief Executive Officer, Hermitage Capital Management Ltd		
Dr. Christian Leuprecht, Professor, Royal Military College of Canada, Queen’s University		
Dr. Jeffrey Mankoff, Distinguished Research Fellow, National Defense University		
Errol P. Mendes, Professor, Constitutional and International Law, University of Ottawa		
Centre for International Governance Innovation	2022/05/17	25
Aaron Shull, Managing Director		
Dr. Wesley Wark, Senior Fellow		
Department of Public Safety and Emergency Preparedness	2022/06/02	27
Hon. Bill Blair, P.C., M.P., Minister of Emergency Preparedness		
Rob Stewart, Deputy Minister		

Organizations and Individuals	Date	Meeting
As an individual	2022/06/07	28
Dr. Ken Barker, Professor, Institute for Security, Privacy, and Information Assurance, University of Calgary		
Juliette Kayyem, Belfer Senior Lecturer in International Security, Harvard Kennedy School of Government		
Beauceron Security	2022/06/07	28
David Shipley, Chief Executive Officer		
Canada Border Services Agency	2022/06/09	29
John Ossowski, President		
Scott Harris, Vice-President, Intelligence and Enforcement Branch		
Canadian Security Intelligence Service	2022/06/09	29
Michelle Tessier, Deputy Director, Operations		
Department of Public Safety and Emergency Preparedness	2022/06/09	29
Hon. Marco Mendicino, P.C., M.P., Minister of Public Safety		
Rob Stewart, Deputy Minister		
Royal Canadian Mounted Police	2022/06/09	29
D/Commr Michael Duheme		
Supt Denis Beaudoin, Director, Financial Crime		
Communications Security Establishment	2022/10/06	37
Caroline Xavier, Chief		
Sami Khoury, Head, Canadian Centre for Cyber Security		

Organizations and Individuals	Date	Meeting
Department of National Defence	2022/10/06	37
Gen Wayne D. Eyre, Chief of the Defence Staff, Canadian Armed Forces		
VAdm J.R. Auchterlonie, Commander of the Canadian Joint Operations Command		
MGen Michael Wright, Commander, Canadian Forces Intelligence Command and Chief of Defence Intelligence		

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.

BlackBerry

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. 17, 18, 21, 25, 27 to 29, 34, 37, 47, 48, 55 and 58) is tabled.

Respectfully submitted,

Ron McKinnon
Chair

SUPPLEMENTARY REPORT OF THE BLOC QUÉBÉCOIS
Up to the task: strengthening Canada's security posture in relation to Russia

The Bloc Québécois would like to thank the members of the Committee and the staff of the Library of Parliament for their work on this study. This also extends to all the witnesses, individuals and organizations who informed the study and the experts who contributed to the public debate on the topic by submitting their observations through letters and briefs. This input will undoubtedly be worth revisiting in the near future. Canada's security posture raises important issues. Our hope is that over the next few years, the public will become increasingly aware of the issue and that this will provide an opportunity to address the shortcomings noted during this study.

While the Bloc Québécois supports the principle behind Recommendation 2, that the Government of Canada should promote post-secondary cyber defence training programs, it is of upmost importance to keep in mind that education is exclusively under the jurisdiction of Quebec and the provinces. Therefore, it is not up to the federal government to create such programs, and only the provinces have the jurisdiction to do so. The role of the federal government in this case is to return the money taken from Quebeckers and the provinces through unconditional transfers. The Government of Canada must keep in mind that Quebec has a unique post-secondary education network and therefore expertize in an area where the federal government has no jurisdiction.

The Bloc Québécois also supports the recommendation that the Government of Canada, in consultation with relevant stakeholders, build on the National Cyber Security Strategy, but with some reservations. The federal government tries to find every and any excuse to interfere in areas that are clearly under provincial jurisdiction. However, examples of federal mismanagement are the norm rather than the exception. Any national cyber security strategy must stick to federally regulated businesses and infrastructure. The strategy must ensure that the owners and operators of federal critical infrastructure of all sizes have access to the cyber security specialists, expertise, and resources they need to address and recover from a cyber attack. It must also ensure that cyber security standards are complied with and reported on. The Government of Canada must consult Quebec on this issue. It must keep in mind that when the Government of Quebec does not have complete control, federal policies aimed at standardization often duplicate Quebec programs and make their application more complex. Therefore, the National Cyber Security Strategy must be implemented in collaboration with Quebec, not imposed on it, in addition to sticking to federally regulated entities. Given the federal government's many failures in managing its own areas of jurisdiction, it is imperative that the Committee remind the federal government to stick to what is under its responsibility. This would avoid creating conflicts with Quebec and the provinces.