National Security and Intelligence Committee of Parliamentarians

Annual Report 2020

Submitted to the Prime Minister on December 18, 2020 pursuant to subsection 21(1) of the *National Security and Intelligence Committee of Parliamentarians Act*
(Revised version pursuant to subsection 21(5) of the *NSICOP* Act)

Canada

Ottawa, ON

National Security and Intelligence Committee of Parliamentarians

Annual Report 2020 (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP100E (Print)
ISSN 2562-5101 (Print)

CP100E-PDF (Online)
ISSN 2562-511X (Online)

ANNUAL REPORT 2020

The National Security and Intelligence Committee of Parliamentarians

The Honourable David McGuinty, P.C., M.P.
Chair

Submitted to the Prime Minister on December 18, 2020
Revised version tabled in Parliament in March 2021

Revisions

Consistent with subsection 21(1) of the National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), the Committee must submit an annual report to the Prime Minister. Consistent with subsection 21(5) of the NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the annual report that does not contain information the Prime Minister believes the disclosure of which would be injurious to national security, national defence or international relations or is information that is protected by solicitor-client privilege.

This document is a revised version of the Annual Report provided to the Prime Minister on 18 December 2020. Revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national security, national defence or international relations or which constitutes solicitor-client privilege. Where information could simply be removed without affecting the readability of the document, the Committee noted the removal with three asterisks (***) in the text of this document. Where information could not simply be removed without affecting the readability of the document, the Committee revised the document to summarize the information that was removed. Those sections are marked with three asterisks at the beginning and the end of the summary, and the summary is enclosed by square brackets (see example below).

EXAMPLE: [*** Revised sections are marked with three asterisks at the beginning and the end of the sentence, and the summary is enclosed by square brackets. ***]

Chair's Message

Ottawa, ON – December 18, 2020

This past year has been one of challenge and adaptation for the Committee, the national security and intelligence community, the government, Canadians and the world. The pandemic has had a significant impact on all aspects of our lives, but we continue to persevere.

This annual report – our third – is a result of that perseverance.

In February 2020, NSICOP was reconstituted following its dissolution prior to the 2019 federal election. We welcomed new members from all recognized parties and groups in both Houses of Parliament. In the weeks following their appointment, our newest members devoted themselves to learning about the complex world of security and intelligence and familiarizing themselves with NSICOP's past reviews. Together, both new and returning members demonstrated their commitment to NSICOP's mandate and put aside partisan differences to work on issues that affect the security and rights of all Canadians.

In March 2020, NSICOP's 2019 Annual Report and its separate special report on the collection of information on Canadians by the Department of National Defence and the Canadian Armed Forces were tabled in Parliament. Those reports demonstrate NSICOP's ability to delve into complex and sensitive issues. We hope that our findings and recommendations continue to strengthen the accountability and effectiveness of the security and intelligence community. In that context, the Committee was encouraged to see the Prime Minister direct the Ministers of National Defence and Public Safety and Emergency Preparedness to introduce a framework for defence intelligence, pursuant to recommendations made by the Committee in 2018 and 2019.

In the days following the tabling of our 2019 annual report and special report, a nation-wide shutdown was put into effect to assist in "flattening the curve" of Covid-19. Our operations were curtailed and our work plan was disrupted in the early weeks of the pandemic due to constraints of physical distancing and limits on in-person gatherings. The Committee remained in regular contact and seized opportunities for safe engagement, such as participating in podcasts in Canada and abroad to discuss the Committee's reviews. The Committee is encouraged to see more frequent references to NSICOP reports in the media, academia and in Parliament itself; we believe this will increase Canadians' understanding of the security and intelligence community and the challenges it faces.

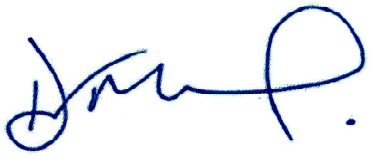
Since September, we have resumed regular Committee meetings, albeit at an altered pace and through different formats. NSICOP's 2020 Annual Report is unlike its predecessor reports. While the Committee has agreed on two important reviews in 2020 – the national security and intelligence activities of Global Affairs Canada and the government's framework and activities to defend its systems and networks from cyber attack – those reviews will be completed in 2021. We are actively examining material, obtaining

briefings and conducting hearings with relevant departments and agencies, academics and civil society organizations.

As a result, this annual report focuses on updating the important threat assessment first undertaken by the Committee in its 2018 Annual Report. Specifically, the assessment covers threats to Canada from terrorism, foreign interference and espionage, cyber attacks, organized crime and weapons of mass destruction. Despite the challenges in mitigating the risks of the pandemic, the dedicated members of the national security and intelligence community provided relevant and helpful material in the preparation of this threat assessment. The Committee wishes to thank them for their support.

The foreword of NSICOP's 2019 Annual Report reflected on the lessons and challenges of the Committee's first two years. As described, both the Committee and the security and intelligence community had much to learn from the new reality of parliamentary review. During the past year, productive discussions with the National Security and Intelligence Advisor to the Prime Minister (NSIA) have helped address significant and pressing challenges faced by the Committee in accessing information "that is under the control of a department and that is related to the fulfilment of the Committee's mandate," as stated in section 13(1) of the NSICOP Act. The Committee is confident that the NSIA will continue to provide the necessary leadership to support its broad and, with the explicit restrictions identified in statute, unfettered access to information.

Finally, I would like to extend my sincere gratitude to my NSICOP colleagues for their commitment to the Committee's important work and the Secretariat for their unfailing dedication and their resiliency in these difficult times.



The Honourable David McGuinty, P.C., M.P.
Chair
National Security and Intelligence Committee of Parliamentarians

THE NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS

The Hon. David McGuinty, P.C., M.P. (Chair)

Mr. Don Davies, M.P.

The Hon. Dennis Dawson, Senator

Mr. Ted Falk, M.P.

The Hon. Frances Lankin, P.C., C.M., Senator

The Hon. Vernon White, Senator

Mr. Glen Motz, M.O.M., M.P.

Ms. Christine Normandin, M.P. (resigned February 20, 2020)

Ms. Jennifer O'Connell, M.P.

Ms. Brenda Shanahan, M.P.

National Security and Intelligence Committee of Parliamentarians

Chair

Comité des parlementaires sur la sécurité nationale et le renseignement

Président

March 2021

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister and Privy Council
Ottawa, ON
K1A 0A2

Dear Prime Minister,

On behalf of the National Security and Intelligence Committee of Parliamentarians, it is my pleasure to present you with the revised version of our Annual Report for 2020. The Report presents an update to the national security threat assessment first included in the Committee's 2018 Annual Report. This overview examines the most significant threats, including terrorism, espionage and foreign interference, cyber threats, major organized crime, and weapons of mass destruction.

Consistent with subsection 21(5) of the *National Security and Intelligence Committee of Parliamentarians Act*, the Report was revised to remove information the disclosure of which would be injurious to national security, national defence or international relations, or is information subject to solicitor-client privilege.

Yours sincerely,

The Honourable David McGuinty, P.C., M.P.
Chair
National Security and Intelligence Committee of Parliamentarians

P.O. Box 8015, Station "T" / C.P. 8015, Succursale « T »
Ottawa, Canada K1G 5A6

TABLE OF CONTENTS

Introduction

1. The National Security and Intelligence Committee of Parliamentarians (the Committee, or NSICOP) is pleased to present the Prime Minister with its third annual report. This year's report differs in style and substance from the Committee's previous work. It not only reflects the unprecedented events and the resulting constraints of 2020, but it also marks the beginning of the second iteration of the Committee, which was reconstituted in February 2020. The Committee's 2019 annual and special reports were tabled in Parliament in March 2020 and, shortly thereafter, a nationwide lockdown came into effect. The Committee was forced to pause its operations in the interest of curbing the spread of COVID-19. The Committee adjusted its work plan in the months following the lockdown and resumed regular meetings only when it was safe to do so.

The Committee's 2020 activities

2. In accordance with the National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), the Committee was dissolved in September 2019 when the federal election was called. In February 2020, the Committee was reconstituted. The Committee welcomed five new members and four returning members representing all major parties and recognized groups in the Senate and the House of Commons. Between February and March 2020, the Committee held seven meetings focused on building members' knowledge of the Committee's mandate and the roles and authorities of the core organizations in the security and intelligence community. The Committee dedicated several meetings to preparations for the tabling of its 2019 reports, including to discuss the government's process to identify information in the reports the disclosure of which would be injurious to national security, national defence or international relations or which constituted solicitor-client privilege, and to then to determine how it would remove that information prior to the tabling of the reports. During this period, the Committee was able to conduct a site visit to the Canadian Security Intelligence Service (CSIS) and to meet with academics to discuss important issues facing the national security and intelligence community. New Committee members spent additional hours outside of the regular meeting times to familiarize themselves with the Committee's past reports, and to learn more about the Committee's legislation and procedures.

3. On March 12, 2020, the government tabled the Committee's Annual Report 2019 and its Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and the Canadian Armed Forces Defence Intelligence Activities. Together, the reports contained four substantive reviews. Their tabling coincided with the start of the nationwide lockdown to slow the spread of COVID-19. The reports nevertheless received significant domestic and international media coverage at that time, and the Committee Chair conducted outreach with academics and Canadians in the months that followed. Continued media interest in the Committee's reviews, particularly those regarding foreign interference and diversity and inclusion, underlines their ongoing relevance for Canadians. The Chair conducted further outreach when he

appeared before the House of Commons Standing Committee on Public Safety and National Security on November 23, 2020, to discuss the Committee's 2019 reports.

4. The nationwide shutdown disrupted the Committee's operations and forced the Committee to adjust its work plan for 2020. Public health guidance prevented the Committee from meeting in person, and the sensitive nature of the Committee's work and its security requirements limited the Committee's ability to meet virtually. The NSICOP Secretariat continued work on the Committee's behalf through April, May and June. During this period, the Committee met three times to discuss and determine its intentions for its 2020 annual report and its review plan for 2021. Members' flexibility during this period allowed the Committee's work to continue, albeit at a slower pace, until conditions were in place for a safe return to secure meetings.

5. Since the start of the pandemic, the Committee has reduced the frequency and duration of its meetings. Nonetheless, with technological and accommodation support from CSIS, the Committee met 16 times over the course of 2020 for a total of 54 hours. During this time, the Committee launched two reviews, met with senior officials in the security and intelligence community, held three hearings and prepared this annual report. The Committee has an ambitious plan for 2021 and work on those reviews is well under way.

Update on the government's response to the Committee's recommendations

6. When it was reconstituted in 2020, the Committee took time to reflect on the government's response to the Committee's first two years of work. Since the tabling of its first special report in December 2018, the Committee has made 23 recommendations to the government aimed at increasing the effectiveness and accountability of the security and intelligence community.[1]

7. The government's response to the Committee's reports has been limited. Immediately prior to its dissolution in September 2019, the Committee received a letter from the Prime Minister acknowledging the Committee's work and stating that the Committee's recommendations were under consideration. The Prime Minister's December 2019 mandate letters to the ministers of National Defence and of Public Safety and Emergency Preparedness directed them to "introduce a new framework governing how Canada gathers, manages and uses defence intelligence, as recommended by the National Security and Intelligence Committee of Parliamentarians."[2] The Committee received a copy

---

[1] For a complete list of the Committee's past recommendations see: National Security and Intelligence Committee of Parliamentarians (NSICOP), *Special Report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, December 3, 2018, p. 37, https://nsicop-cpsnr.ca/reports/rp-2018-12-03/intro-en/html; NSICOP, *Annual Report 2018*, April 9, 2019, p. 115, https://nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-en/html; NSICOP, *Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities*, March 12, 2020, p. 46, https://nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/intro-en/html ; and NSICOP, *Annual Report 2019*, March 12, 2020, pp. 175-177, https://nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/intro-en/htm.

[2] Prime Minister Justin Trudeau, "Minister of National Defence Mandate Letter," December 13, 2019, https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-national-defence-mandate-letter; and Prime Minister Justin

of a letter from the Office of the Privacy Commissioner to the Department of National Defence and the Canadian Armed Forces (DND/CAF) offering assistance and privacy expertise to DND/CAF for the implementation of that commitment. The Committee and its Secretariat have also received informal feedback from senior officials on aspects of the Committee's reviews.

8. The Committee spends considerable time deliberating on its recommendations to ensure they are reasonable, actionable and effective. Its reviews are the product of significant work by both the Committee and organizations in the security and intelligence community. The Committee recognizes that the government is not required to respond to its recommendations; however, the Committee believes that regular and substantive responses would contribute to strengthening the accountability and increasing the transparency of the security and intelligence community. In that respect, it is noteworthy that NSICOP's international counterpart, the United Kingdom's Intelligence and Security Committee of Parliament, receives regular government responses to its reports. The Committee therefore asks the government to consider formally responding to Committee reviews, as it does for organizations like the Office of the Auditor General and for parliamentary committees.

Looking ahead

9. The Committee has an ambitious agenda and announced its upcoming reviews in September 2020. The second iteration of the Committee will continue conducting "framework" reviews (under paragraph 8(*a*) of the NSICOP Act) and "activity" reviews (under paragraph 8(*b*)). For its framework review, the Committee will examine the government's framework to defend its systems and networks from cyber attacks. For its activity review, the Committee will examine the national security and intelligence activities of Global Affairs Canada. Work is already under way for both reviews and the Committee is looking forward to exploring these issues in the year ahead. The Committee also remains committed to engaging civil society and academics to ensure that its work is informed by a multitude of perspectives.

Reporting requirements

10. The NSICOP Act imposes a number of reporting obligations on the Committee. Subsection 21(1) requires the Committee to note in its annual report its findings and recommendations from the preceding year. As noted earlier, the Committee did not complete a review in 2020 and has no findings or recommendations to report. The NSICOP Act also requires the Committee to note the number of times in the preceding year that an appropriate minister determined that a review proposed by the Committee under its activity review mandate would be injurious to national security. The Committee must also report the number of times an appropriate minister refused to provide information to the Committee due to his or her opinion that the information constituted special operational information and that providing it would be injurious to national security. In 2020, no reviews proposed by the

---

Trudeau, "Minister of Public Safety and Emergency Preparedness Mandate Letter," December 13, 2019, https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-public-safety-and-emergency-preparedness-mandate-letter.

Committee were deemed injurious to national security and no information requested by the Committee was refused by a minister on the grounds that it constituted special operational information and that providing it would be injurious to national security.

11. The Committee also notes that it received annual reports from twelve of thirteen organizations on their application of Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities, pursuant to section 8(1) of the *Avoiding Complicity in Mistreatment by Foreign Entities Act*. That direction requires departments and agencies to put in place or update policies and procedures to ensure compliance with the Act. The Committee received reports from the Canada Border Services Agency; the Canada Revenue Agency; CSIS; the Communications Security Establishment; the Department of National Defence and the Canadian Armed Forces; the Financial Transactions and Reports Analysis Centre of Canada; Fisheries and Oceans Canada; Global Affairs Canada; Immigration, Refugees and Citizenship Canada; the Royal Canadian Mounted Police; Public Safety Canada; and Transport Canada. A report was not received from the Privy Council Office.

12. In September 2020, the government provided the Committee with the classified *Report on the Assessment of the Critical Election Incident Public Protocol*. The Protocol and the report were mandated by a July 2019 Cabinet directive that laid out an approach for informing the public about incidents of foreign interference that threatened the integrity of the 2019 federal election. Part of the approach included the creation of a panel of five senior public servants who would be responsible for determining whether to inform Canadians of any such incident. The directive included a requirement for an independent review of the Protocol to assess its implementation and its effectiveness, and to determine whether it should be permanently established and how it could be improved. The directive also included a requirement to provide the Committee with the final report of this review. Jim Judd, a former director of CSIS and a former Deputy Minister of National Defence, conducted this review.

13. The Committee carefully considered Mr. Judd's report. It was heartened to see the government take concrete measures to respond to the issue of foreign interference. As documented in the Committee's 2019 annual report, Canada is the target of significant and sustained foreign interference activities. Foreign actors seek to interfere in Canada's political process across all levels of government, effectively threatening our sovereignty and the integrity of our democratic institutions. The Committee therefore supports key recommendations in Mr. Judd's report, notably that the Protocol mechanism be re-established well in advance of the next federal election and that its mandate be extended to include the pre-writ period.

14. The Committee believes the government should consider four issues as it deliberates the report's recommendations:

- First, the Protocol's mandate should capture all forms of foreign interference, from cyber interference to more traditional methods. In its 2019 review, the Committee found that traditional forms of foreign interference are pervasive across the Canadian polity and pose a significant threat to the rights and freedoms of Canadians.

- Second, the membership of the Panel may benefit from the inclusion of eminent Canadians, potentially including retired jurists. The Committee is concerned that senior public servants appointed to the panel may be preoccupied with transition preparations during the writ period, and notes that an intervention by a non-partisan and high-profile group that includes prominent Canadians may carry more weight in the highly politicized context of an election.
- Third, the government should engage frequently and substantively with political parties on the Protocol's purpose and operation to ensure the widest understanding of the Panel's non-partisan role and the process for intervention.
- Finally, further thought should be given to how the panel would inform Canadians of an incident of foreign interference, including issues of attribution.

15. The Committee communicated its views on the Judd report in a letter to the Prime Minister in December 2020, and will pursue its discussions on the Protocol with the Clerk of the Privy Council in his capacity as Chair of the Panel.

Format of the annual report

16. The 2020 annual report is different from the Committee's past reports. Given the reconstitution of the Committee in February 2020 and the disruption caused by the pandemic, the Committee could not finish a substantive review in 2020 for inclusion in the annual report. After lengthy deliberation, the Committee decided to provide an update to the 2018 threat assessment included in the Committee's first annual report. It decided to do so for several reasons. First, the government does not produce a publicly accessible overview of the main national security threats to Canada. The Committee identified this gap in its 2018 annual report and it continues to believe that such an overview will increase the public's awareness of security threats to Canada. Second, the Committee expects that its 2020 update will continue to contribute to a more informed debate on security and intelligence issues in Canada. Finally, the past two years have seen important shifts in the domestic and international security environments, including challenges arising from the COVID-19 pandemic.

17. The following chapter provides an update on the main national security threats facing Canada. These are terrorism, espionage and foreign interference, malicious cyber activities, major organized crime, and weapons of mass destruction. This update will set the stage for the Committee's reviews in the years to come.

18. NSICOP's 2018 overview of national security threats did not include military threats facing the country. The Committee notes that DND/CAF requested that the 2020 overview include a description of their assessment of these threats. According to DND/CAF, "over the past years, our adversaries, notably Russia and China, have heavily prioritized their defence apparatus and have become increasingly assertive in their efforts to change the international rules-based order, with the clear intent to counter Western influence and interests. Canada's adversaries have studied our military capabilities and

developed weapons specifically designed to counter our defences and exploit our vulnerabilities."[3] In order to better understand the nature and extent of military threats to Canada's security, the Committee may follow up with DND/CAF and other security organizations in the near future.

[3] Department of National Defence and the Canadian Armed Forces (DND/CAF), Letter from the Deputy Minister of DND to the Executive Director, NSICOP, dated November 27, 2020.

Threats to Canada: An Overview

19. In its 2018 annual report, the Committee outlined a number of threats to Canada's national security. The Privy Council Office briefed the Committee on these threats in 2018 and their continued relevance was validated by the security and intelligence community in 2020. This year, the Committee decided to update and expand on those threats with a specific focus on the five issues identified by the security and intelligence community: terrorism; espionage and foreign interference; malicious cyber activities; major organized crime; and weapons of mass destruction. The Committee has addressed some of these issues in greater depth through its reviews. For example, the Committee examined foreign interference in its 2018 Special Report on the Prime Minister's trip to India and its 2019 review of the government response to foreign interference, and it will release its examination of the government's defensive cyber capabilities in 2021.

20. This chapter addresses the five threats in turn. Each section describes the threat and its evolution since 2018, including any implications from the pandemic, and key conclusions.

Terrorism

Overview

21. In its 2018 annual report, the Committee noted that the national security and intelligence community identified terrorism as the primary threat to national security. The government also stated that individuals or groups inspired by Salafi-jihadi ideology posed the greatest terrorist threat to Canada. This assessment has evolved based on a number of trends and events. These include the liberation of Daesh-controlled territory in Iraq and Syria, the subsequent detention of Canadian extremist travellers (also known as foreign fighters) in Syria, attacks against Canadians by extremist individuals and organizations, and the rise of ideologically motivated violent extremism. These issues are described below.

Description of the threat

22. The Canadian Security Intelligence Service (CSIS) stated in its 2018 public report that terrorism was the primary threat to Canada's national security.[4] In the same year, Public Safety Canada noted in its *Public Report on the Terrorist Threat to Canada* that individuals or groups inspired by violent *Salafi-jihadi* ideology, such as that of Daesh or al-Qaida, pose the greatest terrorist threat to Canada and Canadian interests. Since October 2014, Canada's National Terrorism Threat Level has held at *medium*, meaning that a terrorist attack could occur in Canada and that additional measures are in place to keep Canadians safe.[5] Between July 2018 and September 2020, the RCMP conducted *** terrorism-related investigation(s).[6] In that same period, CSIS conducted warranted terrorism-related investigation(s) into *** target(s) and *** organization(s). CSIS also reported to the Committee there has only been one foiled terrorist plot in Canada during that period.[7]

23. The nature of the global terrorism threat is changing. The 2019 liberation of Daesh-controlled territory in Iraq and Syria was a major international counter-terrorism victory, but has led to a number of challenges with respect to the deradicalization of extremist travellers and the repatriation of those individuals and their families. (CSIS defines Canadian extremist travellers as individuals with a nexus to Canada, such as citizens, permanent residents or visa holders, who are suspected of having travelled abroad to engage in terrorism-related activity.[8]) In West Africa, Daesh- and al-Qaida-aligned groups continue to pose threats to Canadian Armed Forces (CAF) personnel, civilians and businesses. Individuals within Canada continue to finance terrorist groups, including Hizballah and those associated with ***. At

---

[4] Canadian Security Intelligence Service (CSIS), *2018 CSIS Public Report*, 2018, www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_ENGLISH_Digital.pdf.
[5] Integrated Terrorism Assessment Centre (ITAC), *Canada's National Terrorism Threat Levels*, 2020. www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.
[6] Royal Canadian Mounted Police (RCMP), *Tiered Project Activity Report*, November 27, 2020.
[7] CSIS, Email response to NSICOP Secretariat, December 10, 2020.
[8] CSIS, *2018 CSIS Public Report*, 2018, www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_ENGLISH_Digital.pdf.

the same time, new threats have come to the fore. A string of ideologically motivated violent extremism-inspired attacks in Canada and other countries has made clear that that this type of extremism poses a growing threat to Canadian national security.

International terrorism environment

24. International trends and events affect Canada's terrorism threat environment. One of the most significant terrorism-related events in recent history was the emergence of Daesh and the related onset of conflict in Iraq and Syria in 2011. At its peak, Daesh controlled approximately one-third of Syrian territory and 40 percent of Iraqi territory.[9] In 2015 alone, the group's revenue ranged from US$1 billion to US$2.4 billion.[10] Daesh's initial success – exemplified by its battlefield victories, control of territory and financial resources – allowed it to create a safe haven for terrorist planning, expand its network of affiliates beyond the borders of Iraq and Syria, and inspire individuals around the world to conduct attacks in support of the organization and its goals. Estimates suggest that over 40,000 extremist travellers from more than 110 countries, including Canada, travelled to Daesh-controlled territory in Iraq and Syria.[11]

25. Daesh-controlled territory in Iraq and Syria was liberated in 2019. Daesh had declared that territory as a "caliphate" and used it to raise funds, recruit, train, influence and direct attacks. Its liberation was a blow to Daesh capabilities and resulted in the Syrian Democratic Forces holding over 100,000 Daesh-affiliates and their relatives in detention facilities.[12] This poses both a foreign policy and counter-terrorism challenge to states, who must decide whether to repatriate detained individuals and how to manage the risk posed by those returnees.

26. Extremist travellers continue to be a security concern for Canada. CSIS estimates that at least 200 extremist travelers with a connection to Canada have travelled overseas to join Daesh and other terrorist groups since 2013, with 122 in Syria, Iraq and Turkey, and the rest in Afghanistan, Pakistan, Lebanon and Somalia.[13] As noted by the Minister of Public Safety and Emergency Preparedness, not all of these individuals were involved in fighting: "[s]ome of them have become battlefield combatants. Others did fundraising, operational planning, online propaganda, recruitment, training and other

---

[9] Wilson Center, *Timeline: The Rise, Spread, and Fall of the Islamic State*, October 28, 2019.
[10] Colin P. Clarke et al., *Financial Futures of the Islamic State of Iraq and the Levant*, RAND Corporation, 2017.
[11] Richard Barrett, *Beyond the Caliphate: Foreign Fighters and the Threat of Returnees*, Soufan Center, October 2017; United Nations (UN) Security Council, *Tenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat,* February 2020, https://undocs.org/S/2020/95.
[12] United States, Bureau of Counterterrorism, *Country Reports on Terrorism 2018*, October 2019, www.state.gov/wp-content/uploads/2019/11/Country-Reports-on-Terrorism-2018-FINAL.pdf; UN Security Council, *Tenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat,* February 2020, https://undocs.org/S/2020/95; Leah West, Amarnath Amarasingam and Jessica Davis, "Where's the Plan for Canadian ISIS Members in Custody Overseas?," *Policy Options*, June 2019.
[13] CSIS, *2018-2019 Report to the Minister on Operational Activities*, December 19, 2019; ITAC, Email response to NSICOP Secretariat, November 30, 2020.

complicit activity," while others "were just camp followers."[14] Nonetheless, their return to Canada or their continued activities abroad remain a security challenge. Of the approximately 200 extremists who travelled abroad from Canada, 61 have returned.[15] According to CSIS, as of November 2020, there are 122 extremist travellers in Turkey, Syria and Iraq. Of this total, *** are suspected dead. Of the remaining ***, *** are in Syria (*** detained, *** at large), *** are in Turkey (*** detained, *** at large), and *** are in Iraq (*** detained, *** at large).[16] Global Affairs Canada and Public Safety Canada continue to manage the process of Canadian extremist travellers seeking to return, and cooperate with the Royal Canadian Mounted Police (RCMP) and other Canadian police to mitigate potential associated risks. To date, no returnee has conducted an attack in Canada, but individuals who either aspired or were thwarted in their plans to fight abroad have.

27. Despite their gradual weakening, Daesh and al-Qaida continue to operate. They direct affiliated groups and inspire other groups and individuals around the world to engage in terrorism. Daesh remains active in parts of Iraq and Syria, and securing the border between the two countries is a persistent challenge.[17] Daesh fighters pose a threat to CAF personnel in Iraq, where Canada supports two missions: its own Operation IMPACT and the NATO Mission Iraq. While the CAF has withdrawn some personnel from Iraq, *** remain in the country in support of the two missions. Outside of Iraq and Syria, Daesh branches in Afghanistan, Indonesia, Malaysia and the Philippines pose persistent threats to state and regional security.[18] Daesh affiliates in West Africa and the Greater Sahara and al-Qaida affiliates in the Sahel are also particularly active.

28. Daesh and al-Qaida affiliates in Africa pose threats to Canadians. Between August 2018 and August 2019, the CAF deployed an aviation task force in Mali in support of a United Nations (UN) peacekeeping mission. Canada currently maintains multiple peacekeeping contributions in Mali, including up to 10 CAF members and civilian police officers. In Burkina Faso, a 2019 attack on a convoy transporting workers of a Canadian-owned mine killed 39 individuals and injured 60 others, forcing the company to suspend operations, which in turn negatively affected Canadian business interests. Canadians have also been kidnapped and, in some cases, murdered, in the region. For example, Daesh claimed responsibility for the January 2019 murder of a Canadian man who was kidnapped from a Canadian-owned mine in Burkina Faso. In another example, a Canadian woman was kidnapped in Burkina Faso in December 2018 [*** Two sentences were revised to remove injurious or privileged

---

[14] The Honourable Ralph Goodale, Speech to Johnson Shoyama Graduate School of Public Policy, Saskatchewan, January 15, 2019, www.canada.ca/en/public-safety-canada/news/2019/01/speech-on-canadas-evolving-national-security-architecture-in-a-constantly-changing-and-very-difficult-world.html#wb-cont.

[15] ITAC, Email response to NSICOP Secretariat, November 30, 2020.

[16] ITAC, Email resposne to NSICOP Secretariat, November 30, 2020.

[17] UN Security Council, *Tenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat,* February 2020, https://undocs.org/S/2020/95.

[18] UN Security Council, *Tenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat,* February 2020, https://undocs.org/S/2020/95.

information. The sentences describe some intelligence related to the kidnapping and a CSIS assessment. ***][19] *** [20]

29. Terrorist activity continues in Canada.[21] Since 2018, two fatal attacks have resulted in charges of terrorist activity, as defined in section 83.01 of the *Criminal Code*. In February 2020, an individual was charged with first-degree murder and terrorist activity following a Daesh-inspired hammer attack that killed one woman in Toronto.[22] In May 2020, the same charges were laid against an individual inspired by the involuntary celibate (or "Incel") ideology, a subculture of violent misogyny, who killed a woman in a massage parlour in Toronto.[23] The *Criminal Code* also contains provisions for offences related to facilitating terrorist activity, leaving Canada to join a terrorist group and participating in the activities of a terrorist group. Since 2018, five individuals have been charged with such offences: one in Kingston, Ontario, in January 2019; one in Guelph, Ontario, in December 2019, and that individual's spouse in Markham, Ontario, in August 2020; one in Calgary, Alberta, in July 2020; and a related case in Calgary, Alberta, in September 2020.[24] ITAC assesses that the "greatest terrorist threat to Canada remains domestic extremists who have been inspired by ideologies promoted by groups such as Daesh, al-Qaida or the ideologically motivated (IMV) extremist milieu."[25]

30. Canada also continues to face exposure to terrorism financing risks. In its *2018 Public Report on the Terrorist Threat to Canada*, Public Safety Canada listed Daesh, al-Qaida and Hizballah as the groups of highest-concern from a terrorism financing perspective. The same report notes that some Canadians continue to support groups associated with ***, including through financing of suspected terrorist groups.[26] ITAC assesses that a small number of extremists in Canada support terrorism-related activities, ***[27]

Ideologically motivated violent extremism

31. Ideologically motivated violent extremism has been growing since 2018. This form of extremism encompasses xenophobic violence, anti-authority violence, gender-driven violence and "other grievance-driven and ideologically motivated violence."[28] According to CSIS, what unites these groups

---

[19] CSIS, *** July 2, 2020.
[20] CSIS, *** December 19, 2019.
[21] Public Safety Canada, *2016 Public Report on the Terrorist Threat to Canada,* 2016, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-pblc-rpr-trrrst-thrt/2016-pblc-rpr-trrrst-thrt-en.pdf.
[22] Stewart Bell, "Suspect's Alleged Statements About ISIS led to Terrorism Charge Over Toronto Hammer Attack: Sources," *Global News,* March 2020, www.globalnews.ca/news/6661038/toronto-hammer-attack-by-isis-supporter.
[23] Stewart Bell, Andrew Russell and Catherine McDonald, "Deadly Attack at Toronto Erotic Spa was Incel Terrorism, Police Allege," *Global News*, May 2020. https://globalnews.ca/news/6910670/toronto-spa-terrorism-incel.
[24] The Canadian Press, "Youth arrested in Kingston terrorism case appears for bail hearing," *CTV News*, March 12, 2019, https://ctvnews.ca/canada/youth-arrested-in-kingston-terrorism-case-appears-for-bail-hearing-1.4332212 ; Rachel Browne, "Guelph man now facing terrorism charges," *Global News*, December 6, 2019, https://globalnews.ca/news/6263053/ikar-mao-terrorism-charges/; Demi Knight, "RCMP lay terrorism charges against 2nd Calgary man in ongoing investigation," *Global News*, September 25, 2020, https://globalnews.ca/news/7359488/2nd-calgary-man-facing-terrorism-charges/.
[25] ITAC, *The National Terrorism Threat Level for Canada*, TA 20/45, July 30, 2020.
[26] Public Safety Canada, *2018 Public Report on the Terrorist Threat to Canada*, 2019.
[27] ITAC, *** March 29, 2019.
[28] CSIS, *2019 Public Report*, 2020.

and individuals is a common belief that "the success or survival of society/civilization cannot be separated from the need for ongoing violence against a perceived threatening group (e.g. the elite, visible minorities, religious groups, corporations, immigrants, capitalists, the government, etc.)."[29] While CSIS uses the term ideologically motivated violent extremism to describe attacks motivated by extreme ideologies across the political spectrum, CSIS's recognition of this form of extremism is in part a response to the evolving threat of right-wing extremism.

32. In Canada, individuals and groups who harbour such views are particularly active online. They exchange ideas using chat forums, conventional social media platform and those dedicated specifically to ideologically motivated violent extremism, and online networks.[30] A 2020 study by the Institute for Strategic Dialogue found that Canadians are highly active across 6,600 identified right-wing extremist channels, pages, groups and accounts. The study also pointed to one prominent message board, on which Canadians are more active than American or British users.[31]

33. Generally, individuals inspired by ideologically motivated violent extremism are less likely to be formally affiliated with a group than those inspired by the ideology of Daesh or al-Qaida. That said, research suggests that as of 2015, at least 100 white supremacist and neo-Nazi groups existed across Canada, with the vast majority of ideologically motivated violent extremism activity in southwestern Ontario, southern Quebec and southern Alberta.[32] More recent estimates suggest that there are closer to 300 such groups across Canada.[33]

34. Neo-Nazi groups are active and growing. CSIS reports that one such group, the Atomwaffen Division, [*** This sentence was revised to remove injurious or privileged information. The sentence summarizes a CSIS assessment of the group. ***][34] Other ideologically motivated violent extremism groups such as the Azov Battalion in Ukraine seem to be trying to create a more united transnational movement using social media. The Canada Border Services Agency (CBSA) notes that a report from the non-profit research group the Soufan Center claims that at least 14 Canadians have travelled to Ukraine to train with extremists.[35]

35. The threat of ideologically motivated violent extremism is growing around the world. According to the 2019 Global Terrorism Index, incidents of this form of extremism in the West increased by 320

---

[29] CSIS, *Defining Violent Extremism in the Changing Canadian Threat Environment*, *** October 16, 2019.
[30] Public Safety Canada, *2018 Public Report on the Terrorist Threat to Canada*, 2019.
[31] Jacob Davey, Mackenzie Hart and Cécile Guerin, "An Online Environmental Scan of Right-wing Extremism in Canada," *Institute for Strategic Dialogue*, 2020, www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf.
[32] Barbara Perry and Ryan Scrivens, *Right-Wing Extremism in Canada*, Palgrave Macmillan, 2019.
[33] Alex Boutilier, "Researchers to probe Canada's evolving far-right movements," *Toronto Star,* March 6, 2019, www.thestar.com/politics/federal/2019/03/06/researchers-to-probe-canadas-evolving-far-right-movements.html.
[34] CSIS, *** 2019.
[35] Canada Border Services Agency (CBSA), *The Increasingly Transnational Nature of Right Wing Extremism*, IOAD_2020-January-001, January 2020.

percent from 2013 to 2018.[36] An April 2020 report released by the UN Counter-Terrorism Committee Executive Directorate similarly warns that "there has been a recent increase in . . . frequency and lethality" of ideologically motivated violent extremism attacks.[37] Since the Committee's last overview in 2018, there have been multiple such attacks. The most prominent among them are listed below. In Christchurch, New Zealand, in March 2019, an individual killed 51 people and injured 49 others in two consecutive attacks on mosques. The attacks were cited as the inspiration of a racist, anti-immigrant attack in El Paso, Texas in August 2019, which killed 22 people and injured another 26. In Halle, Germany, in October 2019, an individual with far-right, anti-Semitic motives killed two people after attempting to storm a synagogue. Four months later, in a racist, anti-immigrant attack, an individual shot and killed nine individuals in Hanau, Germany.

36. Violent attacks by Incel-inspired extremists also pose a growing threat. The Incel subculture is growing and increasingly overlapping with other types of violent extremism. CSIS notes that "violent misogyny is intertwined with other concepts of [ideologically motivated violent extremism], including white supremacy. Hatred for women connects many white supremacists, Incels and other individuals/groups within the broader manosphere."[38] The mobilization of these individuals and groups has been heavily influenced by social media, which serves as a type of echo chamber to potentially radicalize and embolden actors to violence.[39] Canada has experienced three Incel-inspired attacks in the past two years. In April 2018, a member of the misogynistic Incel movement killed 10 individuals and injured another 16 in a van attack in Toronto, Ontario.[40] In June 2019, an individual inspired by the 2018 van attack stabbed a woman and injured her child in Sudbury, Ontario.[41] In February 2020, an individual motivated by the Incel ideology stabbed and killed one individual and injured another in Toronto, Ontario.[42] This latter incident marked the first time in Canada in which an individual was charged with a terrorism-related offence for an Incel-inspired attack (see paragraph 29).

37. States have adopted a number of measures to address the growing threat of ideologically motivated violent extremism. The United Kingdom has listed National Action (also known as Scottish Dawn, NS131 and System Resistance Network) and Sonnenkrieg Division as terrorist entities.[43] In April 2020, the United States listed the Russian Imperial Movement, and in 2019, Canada added Blood &

---

[36] Institute for Economics & Peace, *Global Terrorism Index 2019,* 2019, www.visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf.

[37] UN Security Council Counter-Terrorism Committee Executive Directorate, *Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism*, April 2020, www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf.

[38] CSIS, *Violent Misogyny within the INCEL subculture*, *** January 15, 2020.

[39] ITAC, *The National Terrorism Threat Level for Canada*, TA 19/127-Corrected, December 5, 2019.

[40] "Toronto van attack: 'Incel' killer Minassian pleads not criminally responsible," *BBC*, November 10, 2020, https://www.bbc.com/news/world-us-canada-54895219.

[41] Arron Pickard, "Sudbury 'incel' knife attacker told police he was 'out to murder a little white girl'," *Timmins Today*, January 13, 2020, https://www.timminstoday.com/local-news/sudbury-incel-knife-attacker-told-police-he-was-out-to-murder-a-little-white-girl-2018572.

[42] Nick Boisvert, "Homicide at Toronto massage parlour was an act of incel terrorism, police say," *CBC*, May 19, 2020; https://www.cbc.ca/news/canada/toronto/incel-terrorism-massage-parlour-1.5575689.

[43] Home Office, United Kingdom, *Proscribed Terrorist Groups or Organizations,* February 2020, www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2.

Honour and Combat 18 to its list of terrorist entities (a link to the complete list of designated terrorist entities is included in the footnote below).[44] Following the Christchurch mosque attacks, New Zealand targeted right-wing extremists' use of the Internet by criminalizing the possession and distribution of the attacker's manifesto and live-streamed video.[45] Similarly, Australia adopted legislation that imposes fines and potential jail time for firms that do not expeditiously remove "abhorrent violent material" from their websites.[46]

Terrorist tactics and targets

38. In Canada, the main terrorist threat – from any group or individual – remains low-sophistication attacks on unsecured public spaces. Such attacks require minimal skills and resources, but can result in mass casualties and attract public attention. Soft targets, such as hotels, shopping centres and restaurants, are easily accessible and often crowded.[47] ITAC assesses that while most extremists would prefer to conduct a large-scale, highly sophisticated attack, they will likely resort to what is achievable, namely, low-skill attacks on soft targets.[48]

COVID-19 pandemic

39. The pandemic has affected the accessibility of targets, the planning of violent extremists and the radicalization of individuals. ITAC assesses that the reductions in mass gatherings and the closure of public spaces will cause potential attackers to adjust their planning rather than forgo a potential attack. In some cases, the pandemic and the concurrent anti-racism protests have increased anti-government online rhetoric connected to ideologically motivated violent extremism.[49] CSIS notes that restrictions put in place for the pandemic, such as limits on travel, have disrupted *** terrorist facilitation efforts. However, those groups are readjusting to exploit pandemic measures *** to further their objectives.[50]

40. While violent extremists have adapted their activities, the potential for an increase in radicalization also exists. The RCMP assesses that the restrictions, including lockdown measures, put in place during the pandemic could result in people looking for advice or information over the Internet and accessing extremist echo chambers. This risk is magnified by the challenges of social isolation and

---

[44] See the full list of designated terrorist entities here: Public Safety Canada, *Currently Listed Entities*, 2020, www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx. Department of State, *United States, United States Designates Russian Imperial Movement an Leaders as Global Terrorists*, April 7, 2020, www.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists; Public Safety Canada, *Currently Listed Entities*, 2020, www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx.

[45] Damien Cave, "New Zealand Bans the Christchurch Suspect's Manifesto," *The New York Times*, March 22, 2019, www.nytimes.com/2019/03/22/world/asia/new-zealand-christchurch-shooter-manifesto.html.

[46] "Australia Targets Tech Firms with 'Abhorrent Material' Laws," *BBC News*, April 4, 2019, https://www.bbc.com/news/world-australia-47809504.

[47] Public Safety Canada, *2018 Public Report on the Terrorist Threat to Canada*, 2019.

[48] ITAC, *The National Terrorism Threat Level for Canada*, TA 19/127-Corrected, December 5, 2019.

[49] ITAC, *Update: The National Terrorism Threat Level for Canada*, TA 20/45-E, July 30, 2020.

[50] CSIS, *COVID-19: The Evolving Terrorism Threat*, *** 2020.

financial hardship during restrictions. These same restrictions also make it difficult for others to identify individuals who may be on a path to radicalization.[51]

Key conclusions

41. Individuals or groups inspired by *Salafi-jihadi* ideology, such as Daesh and al-Qaida, posed the greatest terrorist threat to Canada in 2018. While Daesh and al-Qaida have been relatively weakened in the past two years, they continue to pose a threat to Canada and Canadian interests domestically and abroad. At the same time, CSIS has uncovered extensive ideologically motivated violent extremism activities in the past two years (notably right-wing extremist groups), as demonstrated through online activity and physical attacks. The sizable increase in this activity throughout 2020 suggests the terrorist threat landscape is shifting. The primary physical threat to Canada remains low-sophistication attacks on unsecured public spaces. These trends mirror those experienced by Canada's closest allies.

[51] RCMP, *Potential for Radicalization to Violence due to COVID-19*, May 1, 2020.

Espionage and Foreign Interference

Overview

42. In 2018, the Committee identified espionage and foreign interference as growing threats that will likely require a more significant response in the years ahead. Espionage and foreign interference threaten Canada's sovereignty, prosperity and national interests. These threats target communities, governments, businesses, universities and technology. In 2019, the Committee reviewed the government's response to foreign interference and found that foreign interference activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. In 2020, CSIS stated that hostile state actors pose the greatest danger to Canada's national security. Media reports, speeches from officials and information on criminal cases all demonstrate that the threat continues to grow not just in Canada, but among its allies as well.

Description of the threat

43. Espionage has long been a substantive threat to the security of Canada and other nations. While espionage played a critical role in the Cold War, the threat from it has evolved. In particular, the growth of the Internet and an increasingly interconnected society and economy have led to the proliferation of cyber activities as a vector of espionage, and an increase in the risk posed by 'non-traditional collectors' such as students and researchers.[52] Espionage activities primarily involve foreign states trying to obtain political, economic and military information, or proprietary business information, through clandestine means.

44. Foreign interference continues to be a significant threat to the security of Canada. Foreign states use direct and indirect contact to influence democratic and electoral institutions and processes by manipulating ethnocultural communities, persons in positions of authority or influence, and the media. In a speech to the Economic Club of Canada in late 2018, CSIS Director David Vigneault identified foreign interference and espionage as the greatest threats to Canada's national prosperity and national interests. State-sponsored espionage in Canada can be categorized as both cyber and traditional human espionage, independently and in combination.[53] Several recent examples of espionage in Canada show that the threat remains pervasive. Between July 2018 and September 2020, the RCMP conducted *** priority investigation(s) related to espionage and foreign interference.[54] In the same period, CSIS conducted warranted investigation(s) related to espionage and foreign interference against *** target(s) and *** organization(s).[55]

---

[52] CSIS, *** 2019.

[53] David Vigneault, Remarks at the Economic Club of Canada, December 2018, www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.

[54] RCMP, *Tiered Project Activity Report*, November 27, 2020.

[55] CSIS, Email response to NSICOP Secretariat, December 10, 2020.

Espionage

45. Foreign states are increasingly targeting Canada's science and technology sector, in which Canada is recognized as a world leader. CSIS assesses that foreign threat actors represent a significant threat to Canada's long-term economic and national security interests. These actors use a combination of traditional and non-traditional intelligence collection methods to access expertise, data and organizations. As a result of this growing concern, the government established the Deputy Minister Tiger Team on Science and National Security in October 2019 to assess and address security vulnerabilities in the government's science sector.[56]

46. CSIS assesses that while countries such as the Russian Federation, *** have targeted Canadian science and technology, the *** threat from China *** In many cases, these actors are targeting the same types of science and technology in which the Government of Canada is investing. China uses "talent programs" and academic exchanges to exploit Canadian expertise. Its Thousand Talents Program, established in 2008 to encourage Chinese scientists abroad to bring their research to China, is currently under investigation by the U.S. Justice Department.[57] [*** This sentence was revised to remove injurious or privileged information. The sentence describes circumstances in Canada. ***] The result of this program is that intellectual property is often transferred to China, *** [*** This sentence was revised to remove injurious or privileged information. The sentence describes a CSIS assessment. ***][58]

47. New technologies are increasingly targeted by foreign states. CSIS notes that fields essential to Canada's knowledge based-economy, such as artificial intelligence, quantum technology, 5G and biopharma, are actively targeted.[59] CSIS's 2018 public report also characterized economic espionage as a threat of importance that has serious consequences for Canada's economy, including lost jobs, lost tax revenues and diminished competitive advantage.[60]

---

[56] CSIS, *Foreign Threats to Canadian Science and Technology*, *** 2019; and CSIS, Email response to NSICOP Secretariat, October 15, 2020.
[57] Barry, Ellen and Gina Kolata, "China's Lavish Funds Lured US Scientists. What did it get in return?," *The New York Times*, February 6, 2020.
[58] CSIS, *Foreign Threats to Canadian Science and Technology*, *** 2019; CSIS, *** 2020; and CSIS, *** 2020.
[59] Remarks by Director David Vigneault at the Economic Club of Canada, CSIS, December 2018, www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.
[60] CSIS, *CSIS 2018 Annual Public Report*, June 2019, www.canada.ca/en/security-intelligence-service/corporate/publications/2018-public-report.html.

Insider threats

48. Insider threats are another form of espionage that involves an individual with knowledge or access to an organization who intentionally or unwittingly misuses their access to harm that organization, including its personnel, assets, interests or reputation.[61] In Canada, two recent examples of alleged insider activities have resulted in criminal charges: Cameron Ortis and Qing Quentin Huang.

49. Cameron Ortis, a director general of intelligence at the RCMP, was arrested on September 12, 2019. He was initially charged under three sections of the *Security of Information Act* and two sections of the *Criminal Code*, but three additional charges under the *Security of Information Act* were laid in January 2020.[62] He has been accused of sharing special operational information with a foreign entity and preparing to share sensitive information with a foreign entity. The charges relate to incidents that occurred between 2015 and 2019. The RCMP publicly acknowledged that Ortis had access to both domestic and allied intelligence.[63]

50. Qing Quentin Huang was initially charged in 2013 with attempting to communicate secrets to a foreign entity. Specifically, Huang, at the time an employee of Lloyd's Register,[64] was accused of conspiring to sell military (naval) secrets to China.[65] In November 2019, the Attorney General of Canada issued a certificate blocking the disclosure of information and overruling a federal court judge's decision that would have revealed sensitive information stemming from CSIS collection operations against the Chinese embassy in 2013. Such a certificate has never before been issued.[66] In September 2020, two charges against Huang were stayed to protect intelligence. At the time of writing, Huang was out on bail and remained charged with two criminal offences.[67]

51. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes RCMP and CSIS investigations. ***][68]

---

[61] Public Safety Canada, *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk*, 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncgn-crtcl-nfrstrctr-en.pdf.

[62] *Security of Information Act*, R.S.C., 1985, subsections 14(1), 22(1)(*b*) and 22(1)(*e*); and *Criminal Code*, R.S.C. 1985, c. C-46, sections 122, 342.1(1).

[63] Leyland Cecco, "Canada: arrest of ex-head of intelligence shocks experts and alarms allies," *The Guardian*, September 16, 2019, www.theguardian.com/world/2019/sep/16/concern-mounts-after-canadas-ex-head-of-intelligence-accused-of-leaking; Catharine Tunney, "Alleged RCMP spy Cameron Ortis faces 3 new charges under Canada's secrets act," *CBC*, January 27, 2020, www.cbc.ca/news/politics/cameron-ortis-espionage-rcmp-1.5442231; and Amanda Connolly, Mercedes Stephenson, Stewart Bell, Sam Cooper and Rachel Browne, "RCMP intel director charged in major case was top adviser to former force head: sources," *Global News*, September 13, 2019, https://globalnews.ca/news/5899146/senior-rcmp-arrested-charged.

[64] Lloyd's Register is an "international provider of classification, compliance and consultancy services to the marine industry." See: Lloyd's Register, "Marine and Shipping," www.lr.org/en/marine-shipping.

[65] The Canadian Press, "Case of Hamilton man allegedly spying for China, tangled in secrecy," *CBC*, June 28, 2019, www.cbc.ca/news/canada/hamilton/case-of-hamilton-man-allegedly-spying-for-china-tangled-in-secrecy-1.5193658.

[66] Andrew Russell, "Canada's attorney general blocks disclosure of evidence in case of Ontario man accused of spying," *Global News*, November 21, 2019, globalnews.ca/news/6199672/attorney-general-blocks-disclosure-of-evidence-ontario-spying-case.

[67] Colin Freeze, "Prosecutors stay charges against Qing Quentin Huang in probe of naval leaks to China," *The Globe and Mail*, September 18, 2020, www.theglobeandmail.com/canada/article-prosecutors-stay-charges-against-qing-quentin-huang-in-probe-of-naval.

[68] CSIS, *2018-2019 Annual Report to the Minister on Operational Activities*, December 19, 2019.

Foreign interference

52. In 2019, the Committee conducted a review of the government's response to foreign interference. In that review, the Committee found that some foreign states conduct sophisticated and pervasive foreign interference activities against Canada. Those activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. The Committee recommended that the government develop a comprehensive strategy to counter foreign interference and build institutional and public resiliency, and support this comprehensive strategy through sustained central leadership and coordination.

53. The Committee noted that states target Canada and seek to exploit the openness of our society and penetrate our fundamental institutions to meet their objectives. They target ethnocultural communities, corrupt the political process, manipulate the media and attempt to curate debate on postsecondary campuses. Each of these activities poses a significant risk to the rights and freedoms of Canadians and to the country's sovereignty, and the Committee concluded that they are a clear threat to the security of Canada.

54. Since the Committee conducted its review in the 2019 annual report, the threat persists. China *** [*** Two sentences were revised to remove injurious or privileged information. The sentences describe a CSIS investigation. ***][69] Domestically, following the federal election in 2019, [*** Three sentences were revised to remove injurious or privileged information. The sentences describe a CSIS assessment. ***][70]

55. The Russian Federation also continues to exploit Russian diaspora and compatriot organizations in Canada. [*** Two sentences were revised to remove injurious or privileged information. The sentences describe Russian methods and objectives. ***][71]

56. Other states continue to actively engage in foreign interference in Canada. [*** Three sentences were revised to remove injurious or privileged information. The sentences describe a CSIS assessment of one state's methods and objectives. ***][72]

COVID-19 pandemic

57. Espionage related to science and technology and, specifically, to vaccine development for COVID-19, has increased during the pandemic. Research networks in the United States, Canada and the United Kingdom have been targeted by intelligence collection efforts of China, Russia and Iran. The *New York Times* notes that the pandemic "has prompted one of the fastest peacetime mission shifts in recent times for the world's intelligence agencies, pitting them against one another in a new grand game of spy

---

[69] CSIS, *2018-2019 Annual Report to the Minister on Operational Activities*, December 19, 2019.
[70] CSIS, *** 2020.
[71] CSIS, *** 2019.
[72] CSIS, *** 2019.

versus spy."[73] The Communications Security Establishment (CSE) notes that Russia is primarily responsible for this espionage, using clandestine cyber operations to steal proprietary data.[74]

58. In Canada, CSIS has assessed that *** is globally exploiting the pandemic to gain economic and technological advantage. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes CSIS's assessment of a country's methods and objectives, and notes the increased vulnerability of Canadian small businesses and Canada's biopharma and healthcare sectors to that country's efforts. ***][75] ***[76]

Key conclusions

59. The threat from espionage and foreign interference is significant and continues to grow. Several states are responsible for conducting such activities in Canada, but intelligence shows that China and Russia remain the primary culprits. Though the effects of espionage and foreign interference are not as readily apparent as those of terrorism, they are the most significant long-term threats to Canada's sovereignty and prosperity. The pandemic, meanwhile, has provided a new impetus for foreign states to conduct espionage activities against the Canadian health sector and Canadian organizations working in science and technology.

---

[73] Julian E Barnes and Michael Venutolo-Mantovani, "Race for Coronavirus Vaccine Pits Spy Against Spy," *The New York Times*, September 5, 2020, https://nyti.ms/2F2oAPd.

[74] Communications Security Establishment (CSE), *CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development*, July 16, 2020, https://www.cse-cst.gc.ca/en/media/2020-07-16.

[75] CSIS, *** 2020.

[76] CSIS, *** undated.

Malicious Cyber Activities

Overview

60. In its 2018 overview, the Committee characterized malicious cyber activities as a significant risk to national security and specifically pointed to the threat China and Russia pose to government networks. Cyber threats are pervasive. They affect government systems, critical infrastructure providers, the private sector and Canadians. Cyber threat actors range from low-sophistication cyber criminals to highly capable state-sponsored actors. Their motivations also vary, and include the theft of personal information for fraud-related purposes or of intellectual property and confidential business information for industrial espionage, and the interruption of critical services. In 2020, cyber threats continue to be a national security concern for Canada, and Russia and China continue to be the most sophisticated state-sponsored actors targeting Canadian government systems.[77] Over the past year, cyber threat actors have also taken advantage of the global health crisis caused by the COVID-19 pandemic to further their objectives. Malicious state and non-state actors have targeted the health sector and government services, and conducted online disinformation campaigns aimed at manipulating public opinion and undermining confidence in the functioning of key public health systems.

Description of the threat

61. *** states represent the most significant state-sponsored cyber threats to Canada. In 2019 and 2020, CSE identified the most significant state-sponsored cyber threats as emanating from China, the Russian Federation, Iran, the Democratic People's Republic of North Korea (North Korea), ***.[78] CSE has continued to see cyber activity consistent with each actor's national strategic objectives, including in cyber activity against Canadian government networks, private sector systems and critical infrastructure systems.

62. China and Russia continued to be the main drivers of cyber threat activity targeting the government since 2018. This activity has been consistent, year over year, and focused across numerous government sectors, including: [*** This paragraph was revised to remove injurious or privileged information. The paragraph lists the sectors and government organizations. ***][79]

63. CSE identified an increase in cyber attacks by state-sponsored actors against Canadian targets in the first half of 2020.[80] Between January and June 2020, CSE observed *** attempted compromises of Canadian targets by *** Chinese actors. Approximately *** of those attempts, including *** successful compromises, targeted the *** sector. During this period, *** Russian actors attempted to compromise

---

[77] Canadian Centre for Cyber Security (CCCS), *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[78] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[79] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[80] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.

*** Canadian targets, of which CSE assesses that *** were very likely successful. While *** sector targets also made up a portion of *** targeting, that nation's cyber efforts also involved targeting [*** This sentence was revised to remove injurious or privileged information. The sentence describe targeted areas. ***]

64. CSE's 2020 *National Cyber Threat Assessment* describes several key trends in the cyber threat environment.[81] First, CSE assesses that the number and sophistication of cyber threat actors is increasing. Second, CSE assesses that state-sponsored programs from China, Russia, Iran and North Korea pose the greatest strategic threat to Canada, and that state-sponsored actors are likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure. Third, it notes that state-sponsored actors will continue to conduct commercial espionage against businesses, academic and government to steal intellectual property and information. Fourth, CSE states that online foreign influence campaigns are ongoing and are not limited to major political events like elections. Finally, it states that cyber crime remains the threat most likely to affect Canadians and Canadian organizations, and that large Canadian enterprises and critical infrastructure will continue to be targeted in ransomware attacks. Between July 2018 and September 2020, the RCMP conducted *** priority investigation(s) related to cyber-crime.[82] In that same period, CSIS conducted warranted investigation(s) related to cyber threats against *** target(s) and *** organization(s).[83]

65. Among the broader trends in cyber threat activity, those that relate most closely to national security and intelligence are: information theft for espionage purposes; the compromise of critical infrastructure networks; online foreign influence campaigns through coordinated manipulation of social media and opinions; and the cyber-enabled tracking and surveillance of dissidents and individuals. These areas are discussed below.

Information theft for espionage purposes

66. The state-sponsored theft of information can affect government networks and those of other public institutions. These networks are valuable targets because of the essential nature of their services and the sensitivity of the information they manage.[84] For government networks in particular, CSE has noted that cyber threat actors target confidential and sensitive information, such as *** or details related to *** The continued digitization of government services presents new vulnerabilities to sensitive and confidential information, including through the move to greater use of cloud computing environments.[85] CSE and its allied counterparts assess that state-sponsored adversaries have both the intent and the greatest capability to direct cyber operations against government networks.

---

[81] CCCS, *National Cyber Threat Assessment 2020*, https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020.
[82] RCMP, *Tiered Project Activity Report*, November 27, 2020.
[83] CSIS, Email response to NSICOP Secretariat, December 10, 2020.
[84] CSE, "Public Institutions and Sensitive Information," *National Cyber Threat Assessment 2018*, December 2018, www.cyber.gc.ca/en/guidance/public-institutions-and-sensitive-information.
[85] CSE, "Public Institutions and Sensitive Information," *National Cyber Threat Assessment 2018*, December 2018, www.cyber.gc.ca/en/guidance/public-institutions-and-sensitive-information.

67. Canada and its allies have attributed cyber espionage activity to both China and Russia. CSE assesses that both countries have among the world's most sophisticated cyber capabilities.[86] China uses its cyber operations to target governments, companies and academic institutions globally in order to gain commercial, diplomatic and military intelligence in support of its strategic objectives.[87] CSE assesses that China's cyber capabilities are [*** Two sentences were revised to remove injurious or privileged information. The sentences describe CSE's assessment. ***][88] ***[89] While Russia also uses sophisticated cyber espionage tactics to support its strategic objectives, CSE assesses that [*** This sentence was revised to remove injurious or privileged information. The sentence describes CSE's assessment. ***][90]

68. State-sponsored espionage against private networks is also of significant concern. Intellectual property, confidential business information, and information related to a company's strategic partnerships or research and development plans can be of direct use to a foreign state and its industries. Cyber espionage activities targeting the private sector can result in a loss of competitive advantage, particularly in specialist areas of research and development. For advanced economies such as Canada and its allies, cyber espionage against private networks carries significant risks.

69. Russia and China have conducted cyber espionage against the Canadian *** sectors.[91] For Russia, these efforts support *** intelligence priorities.[92] For China, these activities support the [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a CSIS assessment of China's objectives and a specific example of China's cyber espionage. ***][93]

70. Allied countries likely have had similar experiences with Chinese and Russian cyber espionage. In early 2019, China likely launched cyber attacks against the Australian Parliament and its three largest political parties prior to the Australian general election.[94] More recently, in June 2020, China likely conducted another large-scale cyber attack against Australia, targeting Australian companies, hospitals, schools and government officials.[95] For this attack, Chinese-sponsored cyber actors reportedly used spear-phishing tactics to breach sensitive networks and conduct reconnaissance. In October 2020, the United Kingdom's National Cyber Security Centre revealed that Russia's military intelligence services

---

[86] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[87] CCCS, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, January 30, 2019; CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[88] CCCS, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, January 30, 2019.
[89] CCCS, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, January 30, 2019.
[90] CCCS, *Government of Canada Cyber Threat Report – Q3 & Q4 2018*, undated; CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[91] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019; and CSE, "Cyber Threats to Canadian Infrastructure," National Cyber Threat Assessment 2018, December 2018, www.cyber.gc.ca/en/guidance/cyber-threats-canadian-critical-infrastructure.
[92] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[93] CSIS, *** 2020.
[94] Colin Packham,"Exclusive: Australia concluded China was behind hack on parliament, political parties – sources," *Reuters*, September 15, 2019, www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF.
[95] Charlie Moore and Tim Stickins, "China is blamed for huge cyber attack on Australian businesses, schools and hospitals amid increasing war of words between Canberra and Beijing over call for international inquiry into COVID-19," *Daily Mail*, June 20, 2020, www.dailymail.co.uk/news/article-8438205/Huge-cyber-attack-aimed-Australian-government.html.

conducted extensive cyber reconnaissance in preparation for a cyber attack on the 2020 Tokyo Olympic and Paralympic Games.[96]

Compromise of critical infrastructure

71. The targeting of critical infrastructure has the potential to compromise public safety and national security. These systems, which are increasingly controlled through remote Internet access, support the provision of critical services such as health networks and hospitals, electricity, transportation, energy, and food distribution systems.[97] Canada and its closest security and intelligence partners have reported on cyber attacks and network compromises of energy utilities, banks, and telecommunications and communications infrastructure, as well as the networks of cloud-based service providers.[98]

72. According to CSE, Russia, China and Iran have all demonstrated an intent to develop cyber attack capabilities against industrial control systems linked to critical infrastructure.[99] CSE has previously assessed that, *** cyber attack capabilities against those systems.[100] A notable demonstration of this capability took place in 2017, when CSE alerted its partners in the United States to a compromise of an industrial control system in the energy sector. Officials at the U.S. Department of Homeland Security subsequently stated that Russian cyber threat actors had advanced to the point where they could have disrupted power flows in North America.[101] According to CSE, [*** Two sentences were revised to remove injurious or privileged information. The sentences describe a CSE assessment of a state's methods, objectives and targets. ***][102] ***[103] However, CSE also notes that, in the absence of a major crisis or armed conflict with Canada or the United States, the intentional disruption of Canadian critical infrastructure remains unlikely.

---

[96] Patrick Wintour, "Russia planned cyber-attack on Tokyo Olympics, says UK," *The Guardian*, October 19, 2020, www.theguardian.com/world/2020/oct/19/russia-planned-cyber-attack-on-tokyo-olympics-says-uk.

[97] Canada has identified 10 critical infrastructure sectors. Public Safety Canada, *Critical Infrastructure*, undated, www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx; and Public Safety Canada, *National Cyber Security Strategy*, May 28, 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[98] CSE, "Cyber Threats to Canadian Infrastructure," National Cyber Threat Assessment 2018, December 2018, www.cyber.gc.ca/en/guidance/cyber-threats-canadian-critical-infrastructure; CSE, "Malicious Cyber Activity Targeting Managed Service Providers," April 4, 2017, www.cyber.gc.ca/en/alerts/malicious-cyber-activity-targeting-managed-service-providers; and PricewaterhouseCoopers, "Operation Cloud Hopper," April 2017, www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

[99] According to CSE, Iran's ***. Chinese cyber threat actors have attempted to access ***. CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019; and CSE, *** Strategic Cyber Threat Assessment, March 2018.

[100] CSE, *** Strategic Cyber Threat Assessment, March 2018.

[101] Smith, Rebecca, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *The Wall Street Journal*, 24 July 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110; and U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors," March 15, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

[102] CSE, *** Strategic Cyber Threat Assessment, March 2018.

[103] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.

Online foreign influence campaigns

73. Advanced cyber threat actors have also refined their ability to conduct disinformation campaigns online. Threat actors conduct these campaigns on social media to amplify societal differences, sow discord and undermine confidence in fundamental government institutions. For example, CSE has previously observed Twitter accounts connected to a Russian troll farm tweeting about several high-profile events in Canada, including the January 2017 Québec City mosque shooting, and the increase in asylum-seeker border crossings in summer 2017.[104] However, CSE assessed that the majority of disinformation campaigns by Russia with a link to Canada are likely ***[105] Nevertheless, according to CSE, the number of states conducting online influence activities has grown since January 2019 and state-sponsored online activity will likely continue to target Canadian political discourse.[106]

74. Elections are a valuable target for disinformation and online influence. For example, the Russia-based Internet Research Agency promoted divisive and inflammatory content before the 2016 U.S. presidential election, for which it, and several of its employees, were indicted by the U.S. Department of Justice for "operations to interfere with elections and political processes."[107] Canada's 2019 federal election does not appear to have been a significant target of online influence and misinformation. The final *Report on the Assessment of the Critical Election Incident Public Protocol*, provided to the Committee in September 2020, concluded that there was some media activity of foreign origin during the election period, but that "its impact, as with domestic origin social media activity in this period, does not appear to have been consequential."[108]

Cyber-enabled tracking and surveillance of dissidents and individuals

75. State-sponsored and advanced cyber threat actors have developed sophisticated means of targeting individual persons, such as political opponents or dissidents. These cyber threat activities exploit vulnerabilities in global communication systems to permit eavesdropping or geolocation, or to alter, add or delete content on a targeted user's mobile device.[109]

76. CSE reports that *** to target individuals of interest in Canada.[110] CSE assesses that ***[111] [*** Three sentences were revised to remove injurious or privileged information. The sentences

---

[104] CSE, "Malicious Online Influence Activity," National Cyber Threat Assessment 2018, December 2018, www.cyber.gc.ca/en/guidance/malicious-online-influence-activity.
[105] CSE notes that ***. CCCS, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, January 30, 2019.
[106] CCCS, *** October 2018; and CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[107] United States of America, Department of Justice, "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," February 16, 2018, www.justice.gov/opa/press-release/file/1035562/download.
[108] Jim Judd, *Report on the Assessment of the Critical Election Incident Public Protocol*, May 2020.
[109] CSE, *Statement on continuing coverage related to SS7*, April 25, 2014, www.cse-cst.gc.ca/en/media/2018-04-25; and Brigitte Bureau, Catherine Cullen and Kristen Everson, "Hackers only needed a phone number to track this MP's cellphone," *CBC*, November 22, 2017, www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338.
[110] CCCS, *Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020*, December 1, 2019.
[111] CCCS, *** July 1, 2019.

describe a CSE assessment of the targeting of individuals in Canada. ***][112] ***[113] The 2018 murder of Saudi dissident Jamal Kashoggi is a gruesome example of states using advanced cyber threat capabilities to target human rights activists, dissidents, lawyers and journalists.[114] One study of a prevalent mobile cyber capability suggests that this one cyber tool has enabled the covert cyber tracking, targeting and surveillance of individuals in 45 countries, demonstrating the global use these technologies.[115]

COVID-19 pandemic

77. State and non-state cyber threat actors have taken advantage of the global health crisis caused by the COVID-19 pandemic to pursue their strategic interests. This has led to an increase in cyber activity since January 2020. CSE assesses that state-sponsored actors, primarily from ***, have targeted the Canadian health sector to obtain information, likely in response to new COVID-19 intelligence collection requirements.[116] Specifically, CSE noted that these actors have demonstrated an interest in information related to vaccine research and development, medical equipment, and response coordination. CSE assesses that this threat will likely continue for the duration of the pandemic.[117]

78. Since January 2020, CSE has noted an increase in cyber attacks from *** directed against Canadian targets.[118] Organizations engaged in research and development related to COVID-19 (e.g., related to a vaccine or rapid testing), or who hold sensitive data related to Canada's response to COVID-19, are particularly at risk. CSE notes that approximately *** attempted cyber compromises were directed at the health sector.[119] During the same period, *** directed approximately *** attempted compromises at the health sector.[120] Overall, CSE assesses that the pandemic has [*** This sentence was revised to remove injurious or privileged information. The sentence describes CSE's assessment of the impact of the pandemic on certain states' cyber activities. ***][121]

79. The pandemic has affected other types of cyber threat activity. [*** Two sentences were revised to remove injurious or privileged information. The sentences describe CSIS's assessment of the potential impact of the pandemic on the operations of hostile foreign states. ***][122] ***[123] Finally, CSIS

---

[112] CCCS, *** July 1, 2019.
[113] CCCS, *** July 1, 2019.
[114] Business and Human Rights Resource Centre, "NSO Group allegedly provided software to Saudi Govt. to spy on Khashoggi; Citizen Lab who reported it in turn targeted by undercover agents," January 28, 2019, www.business-humanrights.org/en/nso-group-allegedly-provided-software-to-saudi-govt-to-spy-on-khashoggi-citizen-lab-who-reported-it-in-turn-targeted-by-undercover-agents; and Oren Liebermann, "How a hacked phone may have led killers to Khashoggi," *CNN*, January 20, 2019, www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html.
[115] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak and Ron Deibert, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, Citizen Lab*, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.
[116] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[117] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[118] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[119] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[120] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[121] CCCS, *Cyber Threat Brief: State Activity against Canada January to June 2020*, June 26, 2020.
[122] CSIS, *** 2020.
[123] CSIS, *** 2020; and CSIS, *** 2020.

has pointed to the increased use of mass surveillance technologies across several countries for use in COVID-19 contact-tracing applications, noting the long-term risks posed to personal privacy by these applications outside of Canada.[124]

80. State actors have also shifted the focus of their online influence activities to the pandemic. In late February 2020, U.S. officials accused Russia of spreading disinformation about COVID-19 in a coordinated campaign. Beginning in January, thousands of Twitter, Facebook and Instagram accounts – many of which had previously been tied to Russia – began posting nearly identical messages in English, German, French and other languages, blaming the United States for the pandemic. Some of the messages claimed that the virus was part of a U.S. effort to wage economic war on China; others claimed that it was a biological weapon engineered by the Central Intelligence Agency.[125]

Key conclusions

81. Cyber threats present a serious and growing risk to Canada's national security. State actors, China and Russia in particular, continue to target government networks, public institutions and private companies for cyber espionage. These actors continue to build their capability to target critical infrastructure, conduct online influence campaigns and monitor dissidents abroad. The pandemic put these threats into stark relief, in particular the threats posed to Canada's health sector. The Committee will deliver its review of the government's defensive cyber capabilities to the Prime Minister in 2021.

---

[124] CSIS, *** 2020.

[125] Jessica Glenza, "Coronavirus: US says Russia behind disinformation campaign," *The Guardian*, February 22, 2020, www.theguardian.com/world/2020/feb/22/coronavirus-russia-disinformation-campaign-us-officials; and Bruce Schneier, "Security of Health Information," *Schneier on Security*, March 5, 2020, www.schneier.com/blog/archives/2020/03/security_of_hea.html.

Major Organized Crime

Overview

82. In its 2018 annual report, the Committee stated that the impact of organized crime was significant and insidious. Organized crime groups pursue traditional criminal activities such as the illegal trafficking of drugs, weapons, illicit goods and people, and financial crimes, such as fraud, illegal gaming and market manipulation. The illegal activities of major organized crime groups continue to carry significant costs for society and pose substantial risks to Canada. Over the past two decades, these activities have grown in complexity and sophistication. The nature of the threat has not markedly changed since 2018.

Description of the threat

83. Major organized crime remains an important national security threat. Organized crime groups continue to pursue traditional criminal activities such as the illegal trafficking of drugs, weapons, illicit goods and people, and financial crimes, such as fraud, illegal gaming and market manipulation. They launder money to conceal the profits of their crimes and use extreme violence, including murder, to operate. Furthermore, the activities of major organized crime groups have grown in complexity and sophistication in the past two decades.[126] The same technological enhancements that have facilitated faster flows of people, money, information and goods have also permitted organized crime groups to establish complex global criminal networks. As the UN Office on Drugs and Crime notes, these networks have enabled organized crime to "flourish, diversify and expand their activities."[127]

84. New areas of organized criminal activities include: cyber crime, identity-related crime, trafficking in cultural property and organ trafficking.[128] Interpol also notes that "with revenues estimated in the billons, their criminal enterprises closely resemble those of legitimate international businesses. They have operating models, long-term strategies, hierarchies, and even strategic alliances, all serving the same purpose: to generate the most profits with the least amount of risk."[129]

Organized crime in Canada

85. In Canada, organized crime is pervasive. The *Criminal Code* defines a criminal organization as consisting of three or more people, inside or outside of Canada, whose main purpose is to commit or facilitate serious offences to obtain material benefits. The RCMP's Criminal Intelligence Service Canada

---

[126] Canada, *Government Response to the Standing Committee on Justice and Human Rights Report entitled The State of Organized Crime*, July 18, 2012, www.ourcommons.ca/DocumentViewer/en/41-1/JUST/report-7/response-8512-411-70.
[127] UN Office on Drugs and Crime, *Organized Crime*, undated, www.unodc.org/unodc/en/organized-crime/intro.html.
[128] UN Office on Drugs and Crime, *Emerging Crimes*, undated, www.unodc.org/unodc/en/organized-crime/intro/emerging-crimes.html.
[129] Interpol, *Organized Crime*, undated, www.interpol.int/en/Crimes/Organized-crime.

(CISC) identified more than 1,850 organized crime groups operating in Canada in 2019,[130] a sharp increase from 2011 when it identified between 700 and 900 groups.[131]

86. The majority of the groups identified by CISC do not pose a national security threat and would not fall within the remit of this Committee. However, CISC identified 14 organized crime groups as highest-level threats, meaning that they have interprovincial networks, almost always possess international connections, engage in multiple criminal markets and use violence to further their criminal interests.[132] The CISC definition of the highest-level threat groups is consistent with the Committee's definition of national security threats, which are threats to the security of Canada defined in the CSIS Act or criminality of national scope or gravity. These 14 organizations primarily engage in large-scale drug trafficking and money laundering, use the legitimate economy to pursue their criminal interests and can operate from abroad. Of the 14 identified by CISC, 12 grew from medium- to high-level threats in the past five years. Two others have maintained their status as a high-level threat, and are well entrenched in Canada. Between July 2018 and September 2020, the RCMP conducted *** priority investigation(s) related to transnational serious organized crime.[133]

Major organized crime in Canada: The illegal drug trade

87. The illegal drug trade is the most lucrative source of funds for organized crime groups in Canada.[134] In 2018, over 90 percent of organized crime groups in Canada were involved in at least one illicit drug market.[135] The 2019 CISC report on organized crime states that five high-level threat groups are involved in the largest cocaine importing networks in Canada, including with ties to Mexican and Colombian drug cartels. These groups import up to 1,000 kilograms of cocaine to Canada per month.

88. According to CISC, the illegal drug trade has been increasing, particularly in fentanyl and methamphetamines. The illicit cannabis market has shrunk with legalization and organized crime groups are moving away from heroin and toward fentanyl, particularly in western Canada.[136] Five high-level threat organized crime groups are involved in large methamphetamine networks, which includes the diversion of unregulated chemicals in Canada and the importation of precursor chemicals from China and Mexico for the production of methamphetamine and fentanyl.[137]

---

[130] Criminal Intelligence Service Canada (CISC), *2019 Public Report on Serious and Organized Crime*, December 2019.
[131] CISC, Testimony before the House of Commons Standing Committee on Justice and Human Rights, February 16, 2012, http://prismweb.parl.gc.ca/IntranetDocuments/CommitteeBusiness/41/1/JUST/Meetings/Evidence/JUSTEVBLUES21.HTML.
[132] CISC, *2019 Public Report on Serious and Organized Crime*, December 2019.
[133] RCMP, *Tiered Project Activity Report*, November 27, 2020.
[134] CISC, *2018-2019 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illicit Drugs*, April 29, 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-eng.htm.
[135] CISC, *2018-2019 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illicit Drugs*, April 29, 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-eng.htm.
[136] CISC, *2018-2019 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illicit Drugs*, April 29, 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-eng.htm.
[137] CISC, *2018-2019 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illicit Drugs*, April 29, 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-eng.htm.

Major organized crime: Money laundering

89. Money laundering on behalf of organized crime is Canada's largest illicit financing threat. The government assesses that money laundering will probably increase in coming years.[138] Major organized crime groups engage in money laundering to clean their own proceeds of crime or to provide the service as a third party to other criminal organizations. The CISC 2019 report on organized crime notes that at least four high-level threat groups provide large-scale money laundering services in Canada for international drug traffickers. Organized crime groups engage in money laundering operations through casinos, the underground banking system, illegal gaming (including illegal gaming houses and illegal gaming websites), shell companies and nominees, trade-based money laundering, and real estate investments.[139] The infusion of illegally obtained revenue into legitimate marketplaces erodes the integrity of Canada's financial systems, distorts marketplaces, creates instability, and enables corruption in industry and government.

90. The UN Office on Drugs and Crime estimates that from 2 to 5 percent of global GDP, or US$800 billion to US$2 trillion, are laundered throughout the world annually.[140] In Canada, the highest estimate for domestically laundered funds is C$100 billion.[141] Money laundering by organized crime in British Columbia through the real estate market and casinos is the most prominent and publicly discussed domestic example.[142] In 2018, the Expert Panel on Money Laundering in B.C. Real Estate estimated that $7.4 billion was laundered in the province, with $5 billion of it channeled through the real estate market.[143] The Expert Panel found that laundered funds inflated housing prices across the province by approximately 5 percent, putting housing out of reach for large segments of the population.[144]

91. Similar increases have occurred in other large Canadian real estate markets. Transparency International Canada estimates that between 2008 and 2018, more than $20 billion entered the Greater

---

[138] Privy Council Office, *National Intelligence Assessment: Global Illicit Financing Issues and Canadian Touchpoints*, NIA 9/2019, 2019.
[139] CISC, *2019 Public Report on Serious and Organized Crime*, December 2019.
[140] UN Office on Drugs and Crime, *Money-Laundering and Globalization*, undated, www.unodc.org/unodc/en/money-laundering/globalization.html.
[141] Meunier includes the $100 billion amount as the top-end estimate in his C.D. Howe commentary paper while the Expert Panel on Money Laundering in B.C. Real Estate notes a 'conservative' estimate of approximately $46.7 billion in 2018. In a separate C.D. Howe piece, Kevin Comeau provides $130 billion, but that the estimate is "extremely rough, and should not be relied upon as anything more than an order of magnitude of the problem." Nonetheless, the figures all represent the stark reality that significant amounts of money are laundered in Canada. Denis Meunier, "Hidden Beneficial Ownership and Control: Canada as a Pawn in the Global Game of Money Laundering," C.D. Howe Institute, Commentary no. 519, September 2018, www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Final%20for%20advance%20release%20Commentary_519_0.pdf.
[142] Sam Cooper, "How Chinese gangs are laundering drug money through Vancouver real estate," *Global News*, June 5, 2018. https://globalnews.ca/news/4149818/vancouver-cautionary-tale-money-laundering-drugs; and Stephanie Ip, "Money Laundering in B.C.: Timeline of how we got here," *Vancouver Sun*, May 15, 2019, https://vancouversun.com/news/local-news/money-laundering-in-b-c-timeline-of-how-we-got-here.
[143] Expert Panel on Money Laundering in B.C. Real Estate, *Combatting Money Laundering in B.C. Real Estate*, Government of British Columbia, March 31, 2019, https://news.gov.bc.ca/files/Combatting_Money_Laundering_Report.pdf.
[144] Expert Panel on Money Laundering in B.C. Real Estate, *Combatting Money Laundering in B.C. Real Estate*, Government of British Columbia, March 31, 2019, https://news.gov.bc.ca/files/Combatting_Money_Laundering_Report.pdf.

Toronto Area real estate market outside of the current legislated regime and therefore without any due diligence or review from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). That estimate included $9.8 billion used in cash transactions, and $10.4 billion in purchases by corporate buyers that used unregulated lenders operating outside Canada's anti-money laundering framework.[145] This is just one example of how organized crime groups evade this framework in the way they distribute their assets and financial transactions to limit the detection of their criminal activity.[146]

92. An increasing area of concern for Canada is trade-based money laundering. The Financial Action Task Force, the international body responsible for establishing anti-money laundering and anti-terrorist financing norms and best practices, defines trade-based money laundering as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin."[147] According to the Financial Action Task Force, a common method of trade-based money laundering involves the misrepresentation of the price, quantity or quality of imports or exports.[148] The scale of trade-based money laundering in Canada is unknown, but CBSA assesses that, at a minimum, it is likely in the hundreds of millions of dollars. It further assesses that this activity is happening particularly in Toronto, Montréal and Vancouver.[149] Intelligence indicates that trade-based money laundering seems to be a key method used by Mexican and Colombian drug cartels.[150]

93. The RCMP is responsible for investigating cases of trade-based money laundering. However, this method of money laundering is not widely identified or understood, and referrals are often limited as a result. For example, FINTRAC does not have the legislative authority to collect transaction information linked to documentary credit information, which creates gaps in the ability of CBSA and law enforcement to identify suspicious financing links to trade transactions. In response, the government established the Trade Fraud and Trade-Based Money Laundering Centre of Expertise at CBSA in April 2020 to identify, interdict and investigate complex trade fraud, and refer trade-based money laundering files to the RCMP.[151]

Major organized crime: Penetrating the legal marketplace

94. Organized crime groups are active in the legitimate economy to aid in the laundering process or to invest so-called clean money in the ongoing pursuit of profit. Beyond the various criminal activities noted above, organized crime groups maintain control of hundreds of businesses in many industries, including food services, transportation, construction and haulage, property management, financing and

---

[145] Transparency International Canada, *Opacity: Why Criminals Love Canadian Real Estate (And How to Fix It)*, 2019, https://static1.squarespace.com/static/5df7c3de2e4d3d3fce16c185/t/5e1e357c8460a6689db1c5f8/1579038078911/opacity.pdf.

[146] House of Commons Standing Committee on Finance, *24th Report: Confronting Money Laundering and Terrorist Financing: Moving Canada Forward*, 42nd Parliament, 1st Session, November 2018, www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-e.pdf.

[147] Financial Action Task Force, *Trade Based Money Laundering*, June 23, 2006.

[148] Financial Action Task Force, *Trade Based Money Laundering*, June 23, 2006.

[149] CBSA, *Trade-Based Money Laundering Overview*, ICAP_2020-JUNE-08, June 2020.

[150] CBSA, *Trade-Based Money Laundering Overview*, ICAP_2020-JUNE-08, June 2020.

[151] CBSA, *Trade-Based Money Laundering Overview*, ICAP_2020-JUNE-08, June 2020.

loans, real estate companies, and cash-only businesses.[152] The challenges associated with organized crime embedding itself in the legitimate economy are clearly described by France Charbonneau in her message for the final report of Quebec's [translation] *Commission of inquiry on the awarding and management of public contracts in the construction industry*:

> [translation] The repercussions from this illegal flow of money into the legal economy are devastating in the long run. Companies infiltrated by organized crime are often converted into empty shells, depriving society of the benefits associated with their activities as they are transformed into sterile investments used only for money-laundering purposes. The presence of organized crime in certain economic sectors also discourages investors. These criminal organizations launder their money by infiltrating the legal economy. They eventually become untouchable, even though they acquire their fortune illegally through the use of violence...[153]

COVID-19 pandemic

95. The pandemic has provided opportunities for organized crime groups. The RCMP notes that continued border restrictions could result in increased demand for licit and illicit goods that could be exploited by organized crime.[154] The RCMP also assesses that organized crime groups have increased their web presence, particularly to facilitate the illicit trafficking of pandemic-related goods (e.g., personal protective equipment, masks and medical equipment).[155] CBSA assesses that the pandemic has resulted in some adjustments to smuggling methods of organized crime groups, but that it is unlikely to result in significant drops in global trafficking of drugs to Canada over the next year. According to CBSA, the primary impact will likely be the absorption of smaller-scale organized crime groups into larger syndicates that are better able to adapt quickly to the shifting restrictions of the pandemic.[156]

Key conclusions

96. Major organized crime continues to pose an important national security threat. The proceeds of crime are estimated in the billions, which represents significant lost revenue for governments and a source of further criminality. Beyond these costs are the financial and societal ramifications of organized crime: it undermines the rule of law, threatens public safety, and erodes our financial, legal, political and social institutions.

---

[152] CISC, *Report on Serious and Organized Crime – Highlights*, December 2019, https://cisc-scrc.gc.ca/media/2019/2019-12-06-eng.htm.
[153] France Charbonneau, *Rapport de la Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction*, Mot de la présidente, November 24, 2015, https://www.ceic.gouv.qc.ca/fileadmin/Fichiers_client/fichiers/Rapport_final/Rapport_final_CEIC_MotPresidente.pdf.
[154] RCMP, *Impact of COVID-19 on Integrity, Organized Crime and Hostile State Activity*, March 19, 2020.
[155] RCMP, *Assessment of Federal Policing Priorities in the Age of COVID-19*, May 15, 2020.
[156] CBSA, *The Future Impact of COVID-19 on Drug Smuggling to Canada*, ICAP_2020-SEP-003, August 2020.

Weapons of Mass Destruction

Overview

97. The Committee identified weapons of mass destruction and the proliferation of dual-use materials and technologies as a national security threat in its 2018 annual report. These weapons have the potential to cause indiscriminate and mass casualties, and significant and long-term environmental and economic damage. These weapons and their proliferation have not posed an increased threat to Canada in the past two years. However, a number of trends, described below, may affect this assessment. These trends include: the global nuclear disarmament regime has weakened since 2018 and the continued used of chemical weapons by state and non-state actors has undermined international norms; and technological advancements have increased the accessibility of dual-use materials and facilitated the development and delivery of chemical and biological weapons. Moreover, Canada remains a target of illicit and covert procurement of dual-use technologies by several state actors. At the same time, the COVID-19 pandemic has revealed significant vulnerabilities in state economies, health sectors and response systems.

Description of the threat

98. The development, use and proliferation of weapons of mass destruction poses a threat to the security of Canada and its allies. These chemical, biological, radiological or nuclear weapons have the potential to cause indiscriminate and mass casualties, and significant and long-term environmental and economic damage.[157] The proliferation of materials and technology that could facilitate foreign states or non-state actors in the development and use of these weapons – notably delivery systems and dual-use items, including their associated intellectual property – is another issue of concern.[158]

99. The disarmament and non-proliferation of weapons of mass destruction has been a priority of the UN since its inception. An international treaty seeking to prevent the spread of nuclear weapons and eventually eliminate them, as well as conventions preventing the development, transfer or use of chemical and biological weapons, have received almost universal acceptance.[159]

---

[157] For more information, see: World Health Organization, "Biological Weapons," undated, www.who.int/health-topics/biological-weapons#tab=tab_1; Organization for the Prohibition of Chemical Weapons, "What is a Chemical Weapon," undated, www.opcw.org/work/what-chemical-weapon; and Nuclear Threat Initiative, "The Radiological Threat," December 30, 2015, www.nti.org/learn/radiological.

[158] Public Safety Canada, *Strengthening Canada's Counter-Proliferation Framework*, 2018, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-en.aspx.

[159] The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) came into force in 1970 and has 191 State parties (India, Israel, North Korea and Pakistan are not party to the NPT). The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BWC) came into force in 1975 and has 182 State parties. The Convention on the Prohibition of the Development, Stockpiling and Use of Chemical Weapons (CWC) came into force in 1997 and has 193 State parties. Nuclear Threat Initiative, "Get the Facts NPT," November 2019, https://media.nti.org/documents/npt_fact_sheet.pdf; Arms Control Association, "Biological Weapons Convention Signatories and States-Parties," September 2018, www.armscontrol.org/factsheets/bwcsig; and Arms Control Association "Chemical Weapons Convention Signatories and States-Parties," June 2018, www.armscontrol.org/factsheets/cwcsig.

100. Canada is an active participant in international disarmament fora and has developed an interdepartmental counter-proliferation framework to prevent the illicit acquisition, export or diversion of items of concern.[160] Canadian business and research institutions are active in nuclear energy, biotechnology and chemical sectors, rendering them targets for proliferators and other malicious actors.[161] The security and intelligence community works to address the proliferation threat through the administration of laws to prevent the export of dual-use technologies, reviews of investments that may be injurious to national security, and investigations of individuals or companies suspected of illicit activities in this area. The RCMP conducted *** investigation(s) related to this issue between July 2018 and September 2020.[162] In this same period, CSIS conducted warranted investigation(s) related to weapons of mass destruction against *** target(s) and *** organization(s).[163]

101. Disarmament and non-proliferation have been relatively effective since the arms control regime governing these weapons has been in place. Only four states have acquired nuclear weapons since the coming into force of the Treaty on the Non-Proliferation of Nuclear Weapons in 1970, the total inventories of nuclear warheads throughout the world has declined, and nuclear weapons have not been used in conflict since 1945.[164] Since relevant conventions came into force, there have been no significant large-scale biological weapons attacks and 96 percent of declared chemical weapons stockpiles have been eliminated.[165] However, developments over the past several years suggest these trends may be reversing. According to the Privy Council Office, the degradation of global arms control frameworks, the development of new weapons systems by several nuclear-armed states, and the continued targeting of Canada by state and non-state actors for dual-use technologies for new weapons development are cause for concern.[166]

Nuclear weapons

102. In January 2020, the *Bulletin of the Atomic Scientists* concluded that "the world is sleepwalking its way through a newly unstable nuclear landscape."[167] Two significant trends in the area of nuclear

---

[160] Public Safety Canada, *Strengthening Canada's Counter-Proliferation Framework*, 2018, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-en.aspx.
[161] Public Safety Canada, *Strengthening Canada's Counter-Proliferation Framework*, 2018, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-en.aspx.
[162] RCMP, *Tiered Project Activity Report*, November 27, 2020.
[163] CSIS, Email response to NSICOP Secretariat, December 10, 2020.
[164] According to the UN Office on Disarmament Affairs, nuclear weapons have been used in warfare only in the bombings of Hiroshima and Nagasaki by the United States in 1945. There are currently nine states that possess nuclear weapons. Five of them – China, France, the United Kingdom, the United States and Russia – possessed nuclear weapons when the NPT came into force. The Democratic People's Republic of Korea (North Korea), India, Israel and Pakistan acquired nuclear weapons after the NPT came into force, and they are not party to the treaty. UN Office on Disarmament Affairs, "Nuclear Weapons," undated, www.un.org/disarmament/wmd/nuclear; "World Nuclear Forces," *SIPRI Yearbook 2020*, 2020, www.sipri.org/yearbook/2020/10; and Tariq Rauf, "Is Past Prologue? Examining NPT Review Conference Commitments," UN Institute on Disarmament Research, undated, https://unidir.org/publication/past-prologue-examining-npt-review-conference-commitments.
[165] UN Office for Disarmament Affairs, *Securing Our Common Future: An Agenda for Disarmament*, 2018, www.un.org/disarmament/publications/more/securing-our-common-future.
[166] Privy Council Office, *National Security Environment in a Less Multilateral World*, October 17, 2019.
[167] John Mecklin, "Closer than ever: it is 100 seconds to midnight," *Bulletin of the Atomic Scientists*, January 23, 2020, https://thebulletin.org/doomsday-clock/current-time.

weapons have emerged in the past two years: the weakening of the nuclear disarmament regime, and the deterioration of the nuclear safety environment.

103. The nuclear disarmament regime is eroding for a number of reasons. First, long-standing bilateral arms control agreements between the two largest nuclear powers, the United States and Russia, are at risk. The United States withdrew from the Intermediate-range Nuclear Forces Treaty in 2019 after alleging that Russia was in violation of the treaty. The only remaining bilateral arms control agreement between the two countries, the New Strategic Arms Reduction Treaty (New START), expires in 2021 and its renewal is uncertain.[168] Second, disarmament negotiations with North Korea have stalled, and the unilateral U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA), a multilateral agreement to limit Iran's ability to develop a nuclear weapon, has prompted Iran to resume some previously restricted elements of its nuclear program.[169] Finally, progress on nuclear disarmament by nuclear weapon states is slow. While the total global inventory of nuclear warheads has declined, nuclear weapon states continue to modernize their weapons systems and have a poor record of implementing disarmament commitments agreed to during past review conferences on the Treaty on the Non-Proliferation of Nuclear Weapons.[170] This slow pace has led to growing frustration among non-nuclear weapons states and an increasing divide between the two groups, potentially undermining the global disarmament regime as a whole.[171]

104. The security and intelligence community has highlighted the continued modernization of missile systems. According to DND/CAF, China remains at the forefront of the testing and development of ballistic missiles, while North Korea, Iran and Russia have continued a steady pace of missile testing in the same period.[172]

105. The threat to Canada from the use of nuclear weapons is limited to Russia and China, who would likely consider striking Canadian targets during a nuclear conflict with the United States. DND/CAF assesses that while both states continue to modernize their nuclear arsenals, their primary strategic

---

[168] John Mecklin, "Can the nuclear non-proliferation regime be saved when arms control is collapsing?" *Bulletin of the Atomic Scientists*, February 24, 2020, https://thebulletin.org/premium/2020-03/can-the-nuclear-nonproliferation-regime-be-saved-when-arms-control-is-collapsing.

[169] DND/CAF, *** November 16, 2020; Tongfi Kim, "The North Korean nuclear weapons programme and strategic stability in East Asia," *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su and Ian Anthony, *SIPRI*, June 2019, www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf; and John Mecklin, "Closer than ever: it is 100 seconds to midnight," *Bulletin of the Atomic Scientists*, January 23, 2020, https://thebulletin.org/doomsday-clock/current-time.

[170] Tariq Rauf, "Is Past Prologue? Examining NPT Review Conference Commitments," UN Institute on Disarmament Research, undated, https://unidir.org/publication/past-prologue-examining-npt-review-conference-commitments; UN Office for Disarmament Affairs, *Securing Our Common Future: An Agenda for Disarmament*, 2018, www.un.org/disarmament/publications/more/securing-our-common-future; and Cheryl Rofer, "Low-Yield Nukes are a Danger, Not a Deterrent," *Foreign Policy*, February 11, 2020, https://foreignpolicy.com/2020/02/11/deterrence-nuclear-war-low-yield-nukes-danger-not-deterrent.

[171] In July 2017, the UN Generally Assembly adopted the Treaty on the Prohibition of Nuclear Weapons. Nuclear weapons states have argued that this treaty undermines the NPT. Dr. Tytti Erasto and Dr. Tarja Cronberg, "Opposing Trends: the Renewed Salience of Nuclear Weapons and Nuclear Abolitionism," *SIPRI*, September 2018, https://www.sipri.org/publications/2018/sipri-insights-peace-and-security/opposing-trends-renewed-salience-nuclear-weapons-and-nuclear-abolitionism.

[172] DND/CAF, *** February 6, 2020.

objectives remain deterring a major conventional or nuclear attack.[173] North Korea's nuclear weapons and missile capabilities have increased since 2018 and it continues to develop capabilities to strike the United States. While concerns exist regarding Iran's nuclear-related activities, [*** This sentence was revised to remove injurious or privileged information. The sentence describes a DND/CAF assessment. ***][174]

106. The potential for terrorist groups to acquire nuclear weapons is not of significant concern for the security and intelligence community. CSIS assesses [*** Two sentences were revised to remove injurious or privileged information. The sentences describe a CSIS assessment. ***][175] ***[176] From a nuclear and radiological safety perspective, the International Atomic Energy Agency has recorded over 450 incidents of smuggling or unauthorized possession of nuclear materials (not weapons) and over 700 incidents involving theft or loss of such material since the 1990s.[177] The Nuclear Threat Initiative's 2020 Nuclear Security Index assesses that progress on global nuclear security has "slowed significantly" since 2018 and that remaining security gaps leave nuclear materials and facilities vulnerable to threat and sabotage.[178] Some experts have also raised concerns regarding the risk of cyber attacks against nuclear facilities.[179] In the Canadian context, however, the Canadian Nuclear Safety Commission notes that all operating nuclear facilities in Canada are compliant with strict cyber security regulations, and are regularly reviewed and inspected to ensure continued compliance.[180]

Chemical weapons

107. Another risk is weakened norms surrounding the use of chemical weapons. In the past decade, chemical weapons have been used repeatedly in conflicts and targeted assassinations. Over the course of Syria's civil war, the Organization for the Prohibition of Chemical Weapons-UN Joint Investigative Mission team found that chemical weapons were used on several occasions by both state and non-state actors since 2013.[181] DND/CAF assesses that the Syrian regime has used chemical weapons multiple times since the outbreak of the war and that Daesh has used chemical agents in *** Syria ***[182] The use of chemical weapons in targeted assassinations in the past three years, despite sanctions and

---

[173] DND/CAF, 2020 Strategic Threat Overview, Presentation to NSICOP Secretariat, October 13, 2020; and DND/CAF, *Global: Strike Threats Against North America*, July 15, 2018.
[174] DND/CAF, *Global: Strike Threats Against North America*, July 15, 2018; DND/CAF, "Excerpt from *** November 16, 2020.
[175] CSIS, *STIG2018 Joint Threat Assessment*, *** 2018.
[176] CSIS, *STIG2018 Joint Threat Assessment*, *** 2018.
[177] Global Affairs Canada, "Nuclear and radiological programming," 2017, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/weapons_mass_destruction-armes_destruction_massive.aspx?lang=eng.
[178] Nuclear Threat Initiative, "Losing Focus in a Disordered World," *2020 Nuclear Security Index*, July 2020, https://www.nti.org/analysis/reports/2020-nti-nuclear-security-index/.
[179] "Nuclear Threat Initiative, "Losing Focus in a Disordered World," 2020 Nuclear Security Index, July 2020, https://www.nti.org/analysis/reports/2020-nti-nuclear-security-index/.
[180] Eric Lemoine, "CNSC Cyber Security program for NPPS: The Present and the Future," Canadian Nuclear Safety Commission, March 2020.
[181] Arms Control Association, "Timeline of Syrian Chemical Weapons Activity, 2012-2020," March 2020, https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity; and Sadik Toprak, "Trends in recent CBRN incidents," *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su and Ian Anthony, SIPRI, June 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[182] DND/CAF, *Syria: Chemical Weapon Attack* *** April 16, 2018.

international condemnation, further undermines norms against the use of such weapons.[183] In February 2017, the North Korean government ordered the assassination of Kim Jong-nam, the brother of North Korean leader Kim Jong-un, with the VX nerve agent in Malaysia.[184] In March 2018, Russian intelligence agents poisoned former Russian spy Sergei Skripal and his daughter Yulia with a nerve agent in Salisbury, United Kingdom.[185] In August 2020, Russian intelligence agents poisoned Russian opposition leader Alexei Navalny with the same class of nerve agent in Russia.[186]

108. The proliferation of chemical weapons is an added concern. According to the Nuclear Threat Initiative, chemical weapons are "the most widely used and proliferated weapon of mass destruction."[187] Some of the agents used to develop these chemical weapons have legitimate uses and are highly regulated. However, technological developments in the past decade, including technologies and supply chains that can facilitate the delivery of these weapons and materials, may complicate non-proliferation efforts in the future.[188] CSIS suggests that recent incidents of chemical weapons use have increased public awareness and knowledge about these weapons, and could therefore change the chemical weapons threat environment.[189] Researchers have noted that terrorist groups such as al-Qaida have sought to obtain chemical weapons and the Organization for the Prohibition of Chemical Weapons-UN Joint Investigative Mission team identified instances of chemical weapons use by Daesh in Syria.[190] CSIS assesses [*** Two sentences were revised to remove injurious or privileged information. The sentences describe a CSIS assessment of risks associated with terrorists and proliferation. ***][191] ***[192]

Biological weapons

109. Similar concerns have been voiced about the proliferation of biological weapons and countries' capacity to respond to a large-scale biological attack.[193] In March 2020, the UN Secretary General warned that "scientific advances are reducing technical barriers which earlier limited the potential of

---

[183] Sadik Toprak, "Trends in recent CBRN incidents," *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su and Ian Anthony, SIPRI, June 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[184] Hannah Ellis Peterson and Benjamin Haas, "How North Korea got away with the assassination of Kim Jong-nam," *The Guardian*, April 1, 2019, https://www.theguardian.com/world/2019/apr/01/how-north-korea-got-away-with-the-assassination-of-kim-jong-nam.
[185] BBC News, "Russian spy poisoning: what we know so far," *BBC*, October 8, 2018, https://bbc.com/news/uk-43315636.
[186] Dan Sabbagh and Luke Harding, "Kremlin meant to kill Navalny, western security agencies believe," *The Guardian*, November 16, 2020, https://www.theguardian.com/world/2020/nov/16/kremlin-alexei-navalny-western-security-agencies-novichok.
[187] Nuclear Threat Initiative, "The Chemical Threat,"30 December 2015, https://www.nti.org/learn/chemical/.
[188] Elena Dinu, "Reassessing CBRN terrorism threats," *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su and Ian Anthony, SIPRI, June 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[189] CSIS, *STIG2018 Joint Threat Assessment*, *** 2018.
[190] Elena Dinu, "Reassessing CBRN terrorism threats," *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su and Ian Anthony, SIPRI, June 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[191] CSIS, *STIG2018 Joint Threat Assessment*, *** 2018.
[192] CSIS, *STIG2018 Joint Threat Assessment*, *** 2018.
[193] Since the Biological Weapons Convention came into force in 1975, the only known instances of biological weapons attacks have been perpetrated by non-state actors. John P. Caves, Jr. and W. Seth Carus, "The Future of Weapons of Mass Destruction: Their Nature and Role in 2030," *National Defence University Centre for the Study of Weapons of Mass Destruction*, Occasional Paper No. 10, June 2014, https://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper-10.pdf.

biological weapons."[194] The Bulletin of the Atomic Scientists echoed this concern, noting that "genetic engineering and synthetic biology technologies are now increasingly affordable, readily available and spreading rapidly."[195] While these technologies have legitimate uses, they can also be used in the deployment of biological weapons. The Biological Weapons Convention has no formal verification mechanism. While no country admits to having a biological warfare program, DND/CAF assesses that specific countries maintain such programs ***[196] The UN Secretary General has highlighted the importance of building state capacity to respond to a biological attack if prevention fails.[197] The challenges many countries are facing in responding to the global COVID-19 pandemic suggest that capabilities to respond to a large-scale biological attack may be limited.

Dual-use technologies

110. According to CSIS, Canada remains a target of illegal and covert procurement and technology transfer by ***[198] [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes CSIS assessments of a state's methods and objectives, and concerns arising from new technologies. ***][199] ***[200] ***[201]

COVID-19 pandemic

111. The COVID-19 pandemic has not had a significant impact on the threat posed by weapons of mass destruction. At the same time, the COVID-19 pandemic has revealed significant weaknesses in state health sectors and response systems.

Key conclusions

112. The security environment surrounding weapons of mass destruction has not improved since 2018. The nuclear arms control regime has seen important setbacks in the past two years. Long-standing international norms against chemical weapons have been effectively undermined by the use of these weapons by state and non-state actors in conflicts and targeted assassinations. The use of biological weapons remains rare, but the verification regime is weak and the challenges of the COVID-19 pandemic suggest that states' capacity to respond may be limited. The relative accessibility of chemical and biological materials, and the proliferation of dual-use technologies, is of particular concern for Canada.

---

[194] United Nations Secretary General, "Secretary-General's message on the forty-fifth anniversary of the entry into force of the Biological Weapons Convention," March 26, 2020, https://www.un.org/sg/en/content/sg/statement/2020-03-26/secretary-generals-message-the-forty-fifth-anniversary-of-the-entry-force-of-the-biological-weapons-convention.

[195] John Mecklin, "Closer than ever: it is 100 seconds to midnight," *Bulletin of the Atomic Scientists*, 23 January 2020, https://thebulletin.org/doomsday-clock/current-time.

[196] DND/CAF, *** June 6, 2013; United Nations Office for Disarmament Affairs, *Securing our Common Future: An Agenda for Disarmament*, 2018, https://www.un.org/disarmament/publications/more/securing-our-common-future/.

[197] United Nations Office for Disarmament Affairs, *Securing our Common Future: An Agenda for Disarmament*, 2018, https://www.un.org/disarmament/publications/more/securing-our-common-future/.

[198] CSIS, *2018-2019 Annual Report to the Minister on Operational Activities*, December 19, 2019.

[199] CSIS, *** 2020.

[200] CSIS, *** 2019.

[201] CSIS, *** 2019.

Conclusion

113. This year has been difficult for all Canadians. With its changed membership since the 2019 election, the Committee had barely begun its work when measures to control the spread of COVID-19 were introduced. Those measures forced the Committee to adapt its work plan and to find ways of conducting its business while respecting requirements for both health and security. The Committee acknowledges the assistance of the Canadian Security Intelligence Service in providing the Committee with a secure means of holding meetings in the fulfillment of its mandate. It also recognizes the efforts of the security and intelligence organizations to provide documentation in response to Committee requests despite grappling with their own pandemic-related challenges.

114. These efforts reinforce for the Committee the importance of ensuring accountability even in the most trying of circumstances. As the Committee's overview of threats to national security shows, risks to Canada's security continue to evolve, including during a global crisis. Terrorist threats have changed in important ways; states conducted opportunistic attacks to interfere with our politics and steal hard-won research and proprietary data; and organized crime groups exploited legislative and enforcement weaknesses to launder money and traffic increasingly lethal drugs. Canadian security and intelligence organizations have not been complacent, as they continue to identify and mitigate threats while they adapt their own operations to new realities.

115. The same must be true for the organizations responsible for reviewing Canada's security and intelligence framework and activities. The Committee recognizes the pressures security and intelligence organizations face in meeting their operational responsibilities. It adjusted its own demands on departments in response, extending deadlines and reducing requests for briefings. Nevertheless, the Committee and its counterpart organization, the National Security and Intelligence Review Agency, continue to fulfill the roles assigned to them in statute. In the coming year, the Committee intends to provide two reviews to the Prime Minister – the framework for the government's cyber defence activities and the national security and intelligence activities of Global Affairs Canada – which will explore important issues of accountability, governance and effectiveness. This intention reflects the Committee's belief that for security and intelligence, operations and their review are both critical to protecting Canadians' security, rights and freedoms, and that the resumption of both must proceed hand in glove.

Annex A: Overview and Key Conclusions

Terrorism

Overview

116. In its 2018 annual report, the Committee noted that the national security and intelligence community identified terrorism as the primary threat to national security. The government also stated that individuals or groups inspired by Salafi-jihadi ideology posed the greatest terrorist threat to Canada. This assessment has evolved based on a number of trends and events. These include the liberation of Daesh-controlled territory in Iraq and Syria, the subsequent detention of Canadian extremist travellers (also known as foreign fighters) in Syria, attacks against Canadians by extremist individuals and organizations, and the rise of ideologically motivated violent extremism.

Key conclusions

117. Individuals or groups inspired by *Salafi-jihadi* ideology, such as Daesh and al-Qaida, posed the greatest terrorist threat to Canada in 2018. While Daesh and al-Qaida have been relatively weakened in the past two years, they continue to pose a threat to Canada and Canadian interests domestically and abroad. At the same time, CSIS has uncovered extensive ideologically motivated violent extremism activities (notably right-wing extremist groups), in the past two years, as demonstrated through online activity and physical attacks. The sizable increase in this activity throughout 2020 suggests the terrorist threat landscape is shifting. The primary physical threat to Canada remains low-sophistication attacks on unsecured public spaces. These trends mirror those experienced by Canada's closest allies.

Espionage and foreign interference

Overview

118. In 2018, the Committee identified espionage and foreign interference as growing threats that will likely require a more significant response in the years ahead. Espionage and foreign interference threaten Canada's sovereignty, prosperity and national interests. These threats target communities, governments, businesses, universities and technology. In 2019, the Committee reviewed the government's response to foreign interference and found that foreign interference activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. In 2020, CSIS stated that hostile state actors pose the greatest danger to Canada's national security. Media reports, speeches from officials and information on criminal cases all demonstrate that the threat continues to grow not just in Canada, but among its allies as well.

Key conclusions

119. The threat from espionage and foreign interference is significant and continues to grow. Several states are responsible for conducting such activities in Canada, but intelligence shows that China and Russia remain the primary culprits. Though the effects of espionage and foreign interference are not as readily apparent as those of terrorism, they are the most significant long-term threats to Canada's sovereignty and prosperity. The pandemic, meanwhile, has provided a new impetus for foreign states to conduct espionage activities against the Canadian health sector and Canadian organizations working in science and technology.

Malicious cyber activities

Overview

120. In its 2018 overview, the Committee characterized malicious cyber activities as a significant risk to national security and specifically pointed to the threat China and Russia pose to government networks. Cyber threats are pervasive. They affect government systems, critical infrastructure providers, the private sector and Canadians. Cyber threat actors range from low-sophistication cyber criminals to highly capable state-sponsored actors. Their motivations also vary, and include the theft of personal information for fraud-related purposes or of intellectual property and confidential business information for industrial espionage, and the interruption of critical services. In 2020, cyber threats continue to be a national security concern for Canada, and Russia and China continue to be the most sophisticated state-sponsored actors targeting Canadian government systems. Over the past year, cyber threat actors have also taken advantage of the global health crisis caused by the COVID-19 pandemic to further their objectives. Malicious state and non-state actors have targeted the health sector and government services, and conducted online disinformation campaigns aimed at manipulating public opinion and undermining confidence in the functioning of key public health systems.

Key conclusions

121. Cyber threats present a serious and growing risk to Canada's national security. State actors, China and Russia in particular, continue to target government networks, public institutions and private companies for cyber espionage. These actors continue to build their capability to target critical infrastructure, conduct online influence campaigns and monitor dissidents abroad. The pandemic put these threats into stark relief, in particular the threats posed to Canada's health sector. The Committee will deliver its review of the government's defensive cyber capabilities to the Prime Minister in 2021.

Major organized crime

Overview

122. In its 2018 annual report, the Committee stated that the impact of organized crime was significant and insidious. Organized crime groups pursue traditional criminal activities such as the illegal

trafficking of drugs, weapons, illicit goods and people, and financial crimes, such as fraud, illegal gaming and market manipulation. The illegal activities of major organized crime groups continue to carry significant costs for society and pose substantial risks to Canada. Over the past two decades, these activities have grown in complexity and sophistication. The nature of the threat has not markedly changed since 2018.

Key conclusions

123. Major organized crime continues to pose an important national security threat. The proceeds of crime are estimated in the billions, which represents significant lost revenue for governments and a source of further criminality. Beyond these costs are the financial and societal ramifications of organized crime: it undermines the rule of law, threatens public safety, and erodes our financial, legal, political and social institutions.

Weapons of mass destruction

Overview

124. The Committee identified weapons of mass destruction and the proliferation of dual-use materials and technologies as a national security threat in its 2018 annual report. These weapons have the potential to cause indiscriminate and mass casualties, and significant and long-term environmental and economic damage. These weapons and their proliferation have not posed an increased threat to Canada in the past two years. However, a number of trends, described below, may affect this assessment. These trends include: the global nuclear disarmament regime has weakened since 2018 and the continued used of chemical weapons by state and non-state actors has undermined international norms; and technological advancements have increased the accessibility of dual-use materials and facilitated the development and delivery of chemical and biological weapons. Moreover, Canada remains a target of illicit and covert procurement of dual-use technologies by several state actors. At the same time, the COVID-19 pandemic has revealed significant vulnerabilities in state economies, health sectors and response systems.

Key conclusions

125. The security environment surrounding weapons of mass destruction has not improved since 2018. The nuclear arms control regime has seen important setbacks in the past two years. Long-standing international norms against chemical weapons have been effectively undermined by the use of these weapons by state and non-state actors in conflicts and targeted assassinations. The use of biological weapons remains rare, but the verification regime is weak and the challenges of the COVID-19 pandemic suggest that states' capacity to respond may be limited. The relative accessibility of chemical and biological materials, and the proliferation of dual-use technologies, is of particular concern for Canada.