Peinsznski, Paige

From: Lucki, Brenda
Sent: December 18, 2020 4:19 PM
To: McGillis, Sean; Duheme, Michael
Subject: FW: REPORT - PARL - Chong Motion - FINAL
Attachments: 20201218115410358.pdf; 20201218112832027.pdf

Importance: High

FYI

From: DMNS-CSMSN (PS/SP) <ps.dmns-csmsn.sp@canada.ca>
Sent: December 18, 2020 3:14 PM
To: Stewart, Rob (PS/SP) <rob.stewart@canada.ca>; 'jody.thomas@forces.gc.ca' <jody.thomas@forces.gc.ca>; Beauregard, Monik (PS/SP) <monik.beauregard@canada.ca>; Lucki, Brenda <brenda.lucki@rcmp-grc.gc.ca>; 'catrina.tapley@cic.gc.ca' <catrina.tapley@cic.gc.ca>; 'jonathan.vance@forces.gc.ca' <jonathan.vance@forces.gc.ca>; 'marta.morgan@international.gc.ca' <marta.morgan@international.gc.ca>; Keenan, Michael (Ext.) <michael.keenan@tc.gc.ca>; 'Nathalie.G.Drouin@justice.gc.ca' <Nathalie.G.Drouin@justice.gc.ca>; 'John.Ossowski@cbsa-asfc.gc.ca' <John.Ossowski@cbsa-asfc.gc.ca>; Rochon, Paul <paul.rochon@canada.ca>; Thompson, Paul (IC) <paul.thompson@canada.ca>; 'Shelly.bruce@cse-cst.gc.ca' <Shelly.bruce@cse-cst.gc.ca>; Mithani, Siddika (CFIA/ACIA) <siddika.mithani@canada.ca>; 'vigneaultd@smtp.gc.ca' <vigneaultd@smtp.gc.ca>; 'Vincent.Rigby@pco-bcp.gc.ca' <Vincent.Rigby@pco-bcp.gc.ca>; Rochon, Dominic (PS/SP) <dominic.rochon@canada.ca>; Yaskiel, Ava (FIN) <ava.yaskiel@canada.ca>; Stewart, Iain (PHAC/ASPC) <iain.stewart@canada.ca>; 'Sarah.Paquet@canafe-fintrac.gc.ca' <Sarah.Paquet@canafe-fintrac.gc.ca>; 'martin.green@pco-bcp.gc.ca' <martin.green@pco-bcp.gc.ca>; 'MARTIN.LANDREVILLE@forces.gc.ca' <MARTIN.LANDREVILLE@forces.gc.ca>; 'mike.macdonald@pco-bcp.gc.ca' <mike.macdonald@pco-bcp.gc.ca>; Duheme, Michael <Michael.Duheme@rcmp-grc.gc.ca>; Moreau, Ken (PS/SP) <ken.moreau@canada.ca>; Payer, Alexina (PS/SP) <alexina.payer@canada.ca>; Scapillati, Dominique (PS/SP) <dominique.scapillati@canada.ca>; 'CDSCalendar@forces.gc.ca' <CDSCalendar@forces.gc.ca>; 'RAQUEL.GARBERS@forces.gc.ca' <RAQUEL.GARBERS@forces.gc.ca>; Soper, Lesley (PS/SP) <lesley.soper@canada.ca>; Daigle, Francois (AssocDM/SMD) <Francois.Daigle@justice.gc.ca>; Christopher.MacLennan@international.gc.ca; Paquet, Sarah (FINTRAC/CANAFE) <Sarah.Paquet@fintrac-canafe.gc.ca>
Cc: ADAM.GREEN2@forces.gc.ca; Chan2, Justin (PS/SP) <justin.chan2@canada.ca>; CORI.ANDERSON@forces.gc.ca; DMNS-CSMSN (PS/SP) <ps.dmns-csmsn.sp@canada.ca>; Mayer, Matthew (PS/SP) <matthew.mayer@canada.ca>; RAQUEL.GARBERS@forces.gc.ca; Soper, Lesley (PS/SP) <lesley.soper@canada.ca>; SUE.STEFKO@forces.gc.ca; Geday, Emily (PS/SP) <Emily.Geday@canada.ca>; O'Malley, Tim (PS/SP) <tim.omalley@canada.ca>; Renaud, Élise (PS/SP) <Elise.Renaud@canada.ca>; Wong, Suki (PS/SP) <suki.wong@canada.ca>
Subject: REPORT - PARL - Chong Motion - FINAL
Importance: High

Colleagues,

Please find attached the English and French letters in response to the motion introduced in the House of Commons by Mr. Michael Chong (Wellington—Halton Hills) that was passed on November 18, 2020. The motion reads:

That, given that (i) the People's Republic of China, under the leadership of the Chinese Communist Party, is threatening Canada's national interest and our values, including Canadians of Chinese origin within Canada's borders, (ii) it is essential that Canada have a strong and principled foreign policy backed by action in concert with its allies, the House call upon the government to: (a) make a decision on Huawei's involvement in Canada's 5G network within 30 days of the adoption of this motion; and (b) develop a robust plan, as Australia has done, to combat China's growing foreign operations here in Canada and its increasing intimidation of Canadians living in Canada, and table it within 30 days of the adoption of this motion.

This open letter will be sent to all Members of Parliament, and will be formally tabled in January 2021.

We wish to thank your respective ministries for their support as we prepared this letter.

Wishing you a safe and happy holiday season.

DMNS Committee Secretariat | Secrétariat du Comité des SMSN

Pages 3 to / à 8

are not relevant

sont non pertinentes

Peinsznski, Paige

From: Lucki, Brenda
Sent: February 17, 2021 9:28 AM
To:
Subject: RE: Natural Sciences and Engineering Research Council of Canada

Thank you for your correspondence. I can assure you that the RCMP takes all matters that may affect Canada's national security seriously.

I have forwarded your message to the Deputy Commissioner responsible for Federal Policing for his attention and appropriate action.

Regards,

Commissioner/Commissaire
Brenda Lucki
Tel: 613-843-4590

Follow me on Twitter / Suivez-moi sur Twitter : @CommrRCMPGRC

From:
Sent: February 16, 2021 2:05 PM
To: Lucki, Brenda <brenda.lucki@rcmp-grc.gc.ca>
Subject: Natural Sciences and Engineering Research Council of Canada

Dear Commissioner Lucki,

I wrote today to the head of the NSERC to express my concern at the continuing pattern of technology and money transfer from that organization to China, and I write to you on the same issue as I believe it constitutes an offence under the Canadian Criminal Code of 1985:

C-46 (2) (b)

"Every one commits treason who, in Canada,

Without lawful authority, communicates or makes available to an agent of a state other than Canada, military or scientific information or any sketch, plan, model, article, note or document of a military or scientific character that he knows or ought to know may be used by that state for a purpose prejudicial to the safety or defence of Canada."

May I draw your attention to the phrase, "...or ought to know..." which in this instance appears particularily relevant given the common knowledge that your sister service CSIS has repeatedly warned the government of the dangers represented by the Chinese Communist Party and very specifically, Huawei.

I believe that there is here a case for investigation by the RCMP .

Yours most sincerely,

s.19(1)

Pages 11 to / à 13

are not relevant

sont non pertinentes

Pages 14 to / à 15

are duplicates

sont des duplicatas

Pages 16 to / à 24

are not relevant

sont non pertinentes

Pages 25 to / à 27

are duplicates

sont des duplicatas

Pages 28 to / à 37

are not relevant

sont non pertinentes

Pages 38 to / à 39

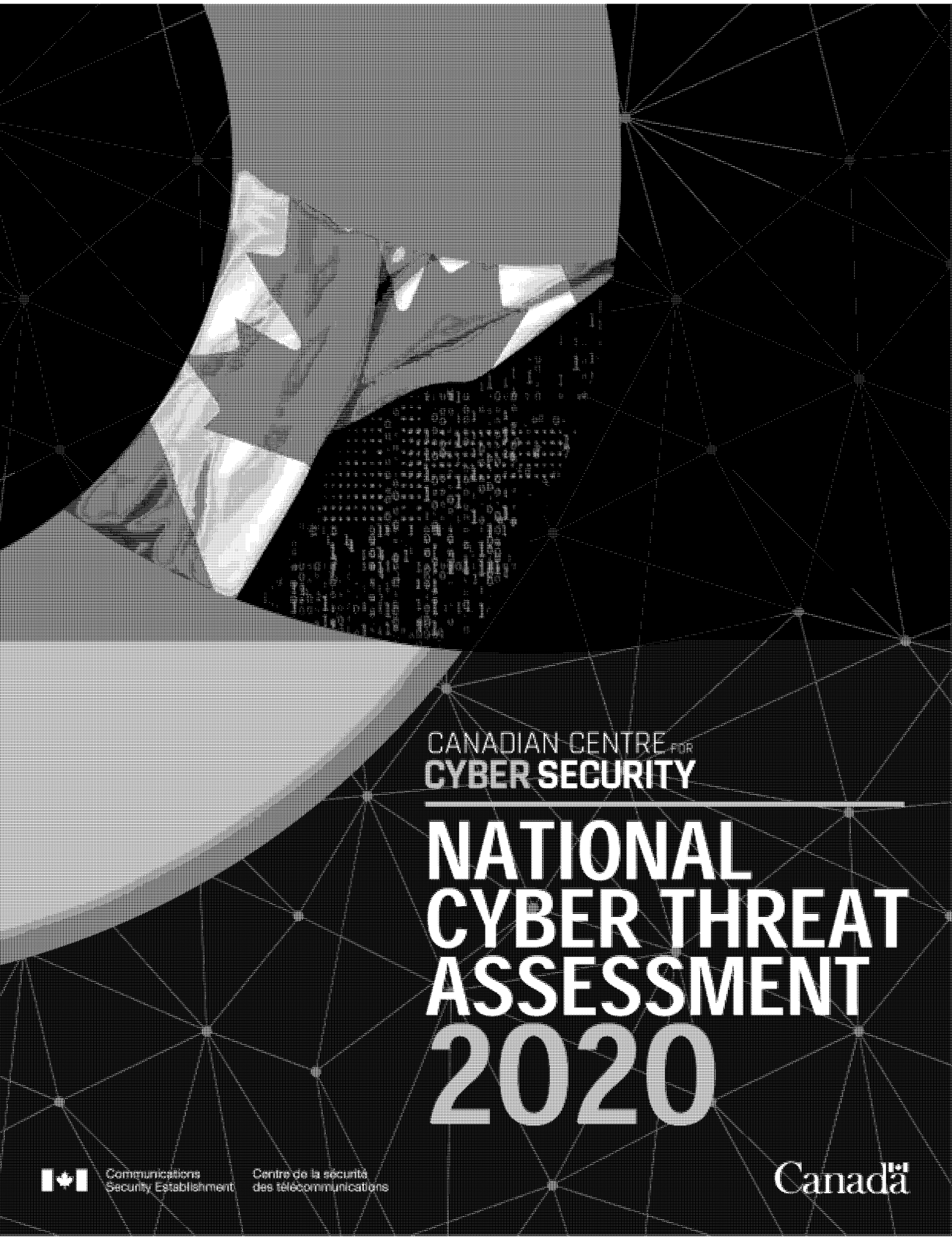
are duplicates

sont des duplicatas

Pages 40 to / à 100

are not relevant

sont non pertinentes



CANADIAN CENTRE FOR
CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2020

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

000101

ABOUT THE CYBER CENTRE

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. As part of the Communications Security Establishment (CSE), the Cyber Centre is a growing organization with a rich history. The Cyber Centre brought operational security experts from across the Government of Canada under one roof. In line with the National Cyber Security Strategy, the Cyber Centre represents a shift to a more unified approach to cyber security in Canada.

We are trusted experts in cyber security with a straightforward, focused mandate to collaborate with government, the private sector, and academia. We are builders, creators, developers, researchers, and scientists. We work to make Canada a safer place to be online.

WE HELP KEEP CANADA AND CANADIANS SAFE IN CYBERSPACE BY:

- Being a **clear, trusted source of relevant cyber security information** for Canadians, Canadian businesses, and critical infrastructure owners and operators;
- Providing **targeted cyber security advice and guidance** to protect the country's most important cyber systems;
- Working **side by side with provincial, territorial, and municipal governments, and private sector partners** to solve Canada's most complex cyber challenges;
- Developing and sharing our **specialized cyber defence technology and knowledge;**
- **Defending cyber systems**, including Government of Canada networks, by developing and deploying sophisticated cyber defence tools and technology;
- Leading the **Government's operational response during cyber events** by using our expertise and access to provide information immediately useful for managing incidents.

Cyber defence is a team sport. Our unique advantage helps make Canada more resistant to cyber threats and more resilient during and after cyber events.

LEARN MORE BY VISITING CYBER.GC.CA,
OR FOLLOW US ON TWITTER @CYBERCENTRE_CA

MINISTER'S FOREWORD

Cyber security is one of the most serious economic and national security challenges we face. Defending Canada and Canadians against cyber threats is a shared responsibility and a team effort. For anybody who thinks cyber security doesn't concern them, I would urge them to read this report.

I am grateful to the team at the Cyber Centre for this timely assessment. By sharing their insights, they are making sure policymakers, business leaders and individual Canadians have the right information to counter these threats effectively.

We know that Canadians are among the most connected populations, and the COVID-19 pandemic has only increased and reinforced our reliance on the internet. As we see almost daily in the headlines, cyber attackers are finding ever more sophisticated ways to exploit our connectivity.

Cyber threats are threats to the privacy, financial security, and even the personal safety of Canadians and the viability of Canadian businesses. "Cyber" just describes the delivery mechanism.

The Cyber Centre's unified approach to cyber security, which builds on Canada's already world-class cyber security expertise, can help Canadians rest assured that their government is prepared to meet the cyber security challenges of tomorrow, today.

The key findings of this report from the Cyber Centre are a timely reminder not to let our guard down.

We are seeing a proliferation of cyber threats, as sophisticated cybercriminals sell their tools and talent through illegal online markets.

Foreign state-sponsored cyber programs are probing our critical infrastructure for vulnerabilities.

Foreign efforts to influence public discourse through social media have become the "new normal".

More than that, the Internet is at a crossroads, with countries like China and Russia pushing to change the way it is governed, to turn it into a tool for censorship, surveillance, and state control.

By continuing to work with partners in government, business, and everyday Canadians, we can build a stronger, more cyber-resilient Canada.

Honourable Harjit Sajjan
Minister of National Defence

MESSAGE FROM THE HEAD OF THE CYBER CENTRE

It has been two years since the release of Canada's first National Cyber Threat Assessment 2018 (NCTA 2018), and during that time, much of what was predicted in 2018 has come to pass. The National Cyber Threat Assessment (NCTA 2020) comes at a time when Canadians and the Canadian economy have increasingly shifted their activities online, a shift that was made more rapid by the onset of COVID-19.

The COVID-19 pandemic has illustrated the extent to which the Canadian economy is reliant upon digital infrastructure. With a sudden increase in the number of Canadians working from home, the protection and security of cyber and telecommunications infrastructure, hardware and software, and the supply chains that support them, is critical to national security and economic prosperity. It is core to our daily lives and, in many cases, the digital infrastructure underpinning our society is out of view and hidden from most Canadians.

This document is not intended to review the NCTA 2018. Some predictions were accurate, others arrived at different speeds. It is said that hindsight is 20/20 and I challenged our assessment teams in 2018 and, again this year, in 2020, to be bold and make predictions. Only the future will tell if our predictions are accurate but they are informed by the full extent of CSE's expertise and knowledge of what is happening in the Canadian and worldwide cyber environment and leverage all sources of information both classified and available openly.

The NCTA is the foundation for many of the activities of the Canadian Centre for Cyber Security (Cyber Centre). The NCTA is intended to set our priorities. We work to address the threats outlined in this report and increase the overall cyber security baseline of Canada. But we don't do it alone. A good example of this approach is the partnership with the Canadian Internet Registration Authority (CIRA) and the launch of their Canadian Shield service. This service, made free to every Canadian by CIRA, can, if used, directly reduce the impact and reach of cybercrime, such as ransomware. Succinctly, it is a direct response to the statement in the NCTA 2018 that the threat most likely to impact Canadians is cybercrime.

But the last two years have also shown that doing the basics of cyber security matters. The vast majority of cyber incidents in Canada occurred because basic elements of cyber security weren't followed. For Canadians, you can rely upon GetCyberSafe.ca to provide simple, realistic, and achievable steps to make yourself more secure. If you are a Canadian not-for-profit, business of any size, or another level of government you can find information at cyber.gc.ca. We each need to do our part to make Canada more secure.

I hope you find NCTA 2020 informative and it spurs every Canadian to take even a single action to make themselves more secure. Each step contributes to our vision of a Secure Digital Canada.

Scott Jones
Head, Canadian Centre for Cyber Security

www.cyber.gc.ca

EXECUTIVE SUMMARY

Canadian individuals and organizations increasingly rely on the Internet for daily activities. In a COVID-19 context, this trend has accelerated to enable Canadians to work, shop, and socialize remotely in accordance with public health physical distancing guidelines. However, as devices, information, and activities move online, they are vulnerable to cyber threat actors.

Cyber threat actors pose a threat to the Canadian economy by exacting costs on individuals and organizations, notably through the theft of intellectual property and proprietary information. They threaten the privacy of Canadians through the theft of personal information, which facilitates additional criminal behaviour including identity theft and financial fraud. As physical infrastructure and processes continue to be connected to the Internet, cyber threat activity has followed, leading to increasing risk to the functioning of machinery and the safety of Canadians.

KEY JUDGEMENTS

- **The number of cyber threat actors is rising, and they are becoming more sophisticated.** The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity. Illegal online markets for cyber tools and services have also allowed cybercriminals to conduct more complex and sophisticated campaigns.
- **Cybercrime continues to be the cyber threat that is most likely to affect Canadians and Canadian organizations.** We assess that, almost certainly, over the next two years, Canadians and Canadian organizations will continue to face online fraud and attempts to steal personal, financial, and corporate information.
- **We judge that ransomware directed against Canada will almost certainly continue to target large enterprises and critical infrastructure providers.** These entities cannot tolerate sustained disruptions and are willing to pay up to millions of dollars to quickly restore their operations. Many Canadian victims will likely continue to give in to ransom demands due to the severe costs of losing business and rebuilding their networks and the potentially destructive consequences of refusing payment.
- **While cybercrime is the most likely threat, the state-sponsored programs of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.** State-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations.
- **State-sponsored actors are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals.** We judge that it is very unlikely, however, that cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for future activities, or as a form of intimidation.
- **State-sponsored actors will almost certainly continue to conduct commercial espionage against Canadian businesses, academia, and governments to steal Canadian intellectual property and proprietary information.** We assess that these threat actors will almost certainly continue attempting to steal intellectual property related to combatting COVID-19 to support their own domestic public health responses or to profit from its illegal reproduction by their own firms. The threat of cyber espionage is almost certainly higher for Canadian organizations that operate abroad or work directly with foreign state-owned enterprises.
- **Online foreign influence campaigns are almost certainly ongoing and not limited to key political events like elections.** Online foreign influence activities are a new normal, and adversaries seek to influence domestic events as well as impact international discourse related to current events. We assess that, relative to some other countries, Canadians are lower-priority targets for online foreign influence activity. However, Canada's media ecosystem is closely intertwined with that of the United States and other allies, which means that when their populations are targeted, Canadians become exposed to online influence as a type of collateral damage.

TABLE OF CONTENTS

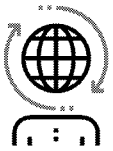
ABOUT THIS DOCUMENT

This document highlights the cyber threats facing individuals and organizations in Canada. It provides an update to the National Cyber Threat Assessment 2018 (NCTA 2018), with analysis of the interim years and forecasts until 2022. We recommend reading the NCTA 2020 along with the Introduction to the Cyber Threat Environment, which we have updated. This introduction provides a basic overview of cyber threat actors, their motivations, cyber tools, and an appendix of key cyber security tools and techniques referred to in this assessment.

As envisioned in the National Cyber Security Strategy, we prepared this document to help Canadians shape and sustain our nation's cyber resilience. It is only when we work together – government, the private sector, and the public – that we can build resilience to cyber threats in Canada.

LIMITATIONS

This assessment does not provide an exhaustive list of all cyber threat activity in Canada or mitigation advice. As a threat assessment, the purpose of this document is to describe and evaluate the threats facing Canada. We focus on understanding the current cyber threat environment and how threat activity can affect Canadians and Canadian organizations. General guidance can be found on the Cyber Centre's website in documents such as the Get Cyber Safe Campaign.



SOURCES

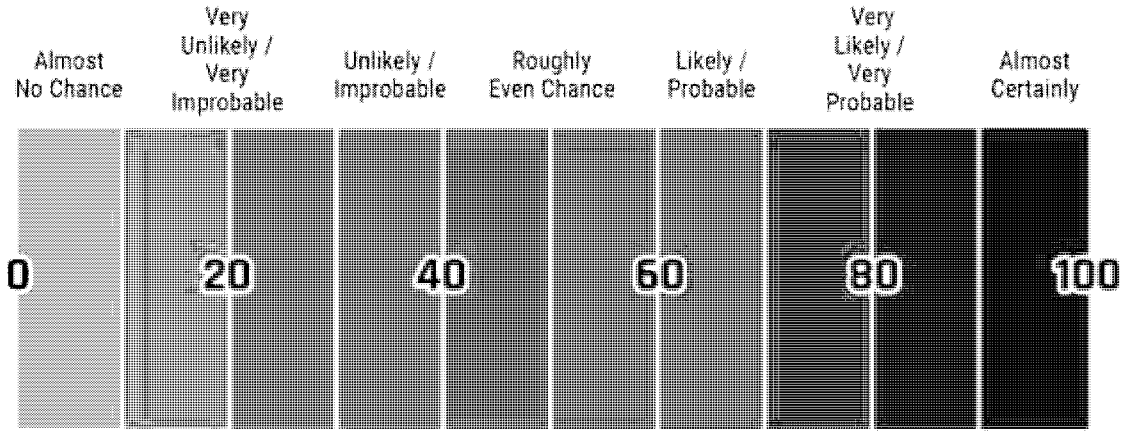
The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the Cyber Centre's knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessment. CSE's foreign intelligence mandate provides us with valuable insights into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

ASSESSMENT PROCESS

Our cyber threat assessments are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases, and using probabilistic language. We use the terms "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly," "likely," and "very likely" to convey probability.

This threat assessment is based on information available as of 20 October 2020.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



AN EVOLVING CYBER THREAT LANDSCAPE

The National Cyber Threat Assessment 2018 (NCTA 2018) outlined the cyber threats faced by Canadian individuals, businesses, and critical infrastructure providers and predicted how the threats would evolve over the following years. Many of these judgements remain relevant. Cybercrime is still the most likely cyber threat to impact Canadians, state-sponsored cyber threat actors continue to conduct cyber espionage against Canadian organizations, including both businesses and critical infrastructure, and cyber threat actors continue to adapt and adopt more advanced methods. However, the cyber threats faced by Canadians have also evolved, keeping pace with the changing ways Canadians use technology and the Internet.

The Internet is indispensable to people around the world and to Canadians. Shifts in March 2020 due to the COVID-19 pandemic have quickly changed the cyber landscape, as more Canadians work, shop, and socialize remotely. We foresee this trend continuing, bringing more facets of Canadian economic, social, and political life online and exposing them to cyber threats, which have also been evolving to take advantage of the growing importance of the Internet and related technologies.

As a scene-setter for the rest of the assessment, we identify in the following section five trends that will drive the evolution of the cyber threat landscape.

TECHNOLOGY IS CHANGING SOCIETY AND ALTERING THE THREAT LANDSCAPE

Technological Changes Spur Societal Changes

Canadians are increasingly reliant on the Internet. More and more important day-to-day activities, such as banking, government services, health services, commerce, and education, have moved online for convenience and efficiency. In today's COVID-19 context, this trend has accelerated to allow Canadians to work, shop, and socialize remotely in accordance with public health physical distancing guidelines. These changes are driven by emerging and maturing technologies, which continue to create new ways to use the Internet that improve standards of living and change how individuals and organizations interact.

Technologies like artificial intelligence (AI), the Internet of Things (IoT), the Industrial Internet of Things (IIoT), and cloud computing underpin a wide range of personal, commercial, and industrial activities. Advancements in the next two years in these and other information technologies, such as the roll out of 5G global wireless telecommunications, will change how Canadians do business, operate industrial plants, buy and obtain consumer goods, receive medical care, and more. In turn, Canadians will continue to see changes in other areas of their lives, including the design of cities and modes of transportation and the undertaking of elections and other democratic processes.

The Threat Landscape

As devices, information, and activities valued by Canadian individuals and organizations are moved online, they become susceptible to threat activity. Cyber threat actors—particularly cybercriminals and state-sponsored actors—continue to adapt their activities to find information that Canadians value and attempt to obtain it, hold it for ransom, or destroy it.

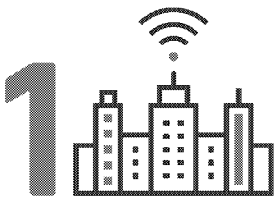
We judge that cybercriminals, who are motivated by financial gain, almost certainly represent the most pervasive cyber threat to Canadians. They conduct the most threat activities against Canadians, including ransomware attacks, theft of personal, financial, and confidential information, and distributed denial of service (DDoS) attacks. As discussed below, illegal markets for cyber products and services allow cybercriminals to access more sophisticated cyber tools.

However, the most sophisticated capabilities belong to state-sponsored cyber threat actors who are motivated by economic, ideological, and geopolitical goals. Their activities include cyber espionage, intellectual property theft, online influence operations, and disruptive cyber attacks.

We assess that almost certainly the state-sponsored programs of China, Russia, Iran, and North Korea pose the greatest state-sponsored cyber threats to Canadian individuals and organizations. However, many other states are rapidly developing their own cyber programs, benefiting from various legal and illegal markets to purchase cyber products and services.

Activities by hacktivists or thrill-seekers almost certainly pose a less common and less sophisticated threat to Canadians. In general, activities by both hacktivists and thrill-seekers are less common than other types of activity, and these threat actors often have fewer resources to devote to their activities, limiting the sophistication of their operations. Hacktivists have conducted newsworthy cyber activities in 2020. One of these incidents primarily targeted US victims but also impacted entities in Canada, exposing data belonging to 38 Canadian police agencies.[3]

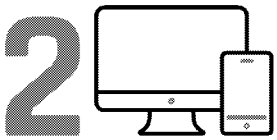
Below we identify five trends that will drive the evolution of the cyber landscape and threat activity.



MORE PHYSICAL SAFETY OF CANADIANS IS BEING PUT AT RISK

The safety of Canadians depends on critical infrastructure (e.g., energy, water), as well as consumer and medical goods (e.g., cars, home security systems, pacemakers, etc.), many of which are controlled by computers embedded within them. Increasingly, these computers are being connected to the Internet by their manufacturers, sometimes unbeknownst to consumers, to enable new features or provide data to a third party. However, once connected, these infrastructures and goods are susceptible to cyber threat activity, and maintaining their security requires investments over time from manufacturers and owners that can be difficult to sustain.

An important part of this trend is operational technology (OT), which is a broad term that refers to technology used to control physical processes such as dam openings, boiler activities, electricity conduction, and pipeline operations. In contrast with Information Technology (IT)—such as hardware and software found in most homes and organizations—OT has been relatively protected from cyber threat activity, because it was not originally designed to be connected to the Internet. However, manufacturers are now converging IT and OT. These changes are meant to increase efficiency and support long-term planning, but they also increase the risk of cyber threat activity reaching OT systems. A 2019 survey found that 68% of manufacturers plan to increase their investment in IT-OT convergence solutions for their organizations over the next two years.[2] We assess that, almost certainly, the most pressing threats to the physical safety of Canadians are to OT and critical infrastructure. However, in the future, targeting of smart cities and IoT devices such as personal medical devices and Internet-connected vehicles, may also put Canadians at risk.



MORE ECONOMIC VALUE IS BEING PUT AT RISK

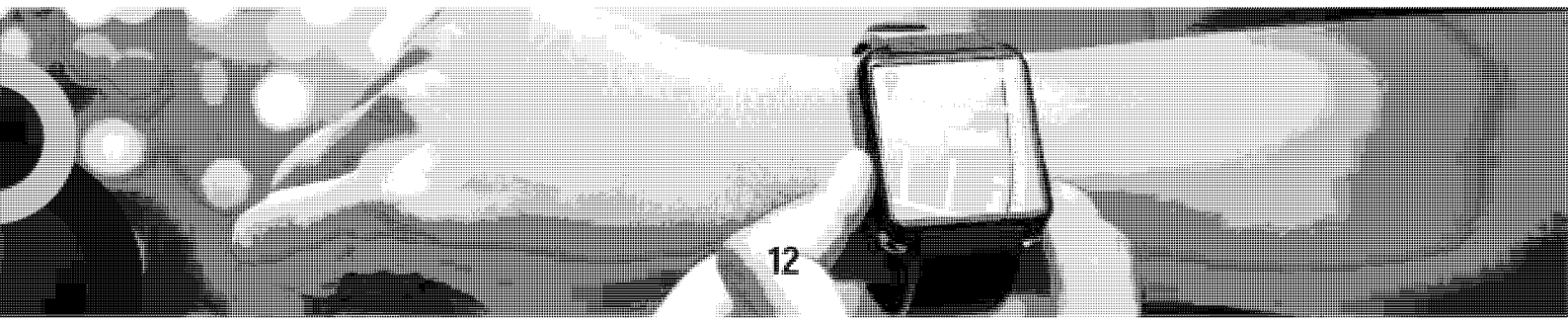
As we noted in NCTA 2018, state-sponsored cyber threat actors and cybercriminals continue to exact costs from Canadian individuals and businesses and damage the economy. Cybercriminals defraud individuals and companies and extort money from them through ransomware, and state-sponsored threat actors steal intellectual property and proprietary business information. Additionally, an increasing number of Canadians have moved their financial activity online, thereby increasing their susceptibility and attractiveness to cybercriminals. In 2019, 94% of Canadians had home Internet access (up from 79% in 2010) and 71% of Canadians banked online (up from 67% in 2010).[3]

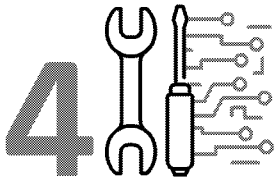
Due to restrictions related to the COVID-19 pandemic, Canadians have shifted quickly and significantly towards remote work arrangements. They are accessing intellectual property and other sensitive data using personal devices and home Wi-Fi networks that are often poorly secured in comparison to corporate IT infrastructure. The protection of intellectual property is crucial to the productivity and competitiveness of Canadian companies, and vital for Canada's economic growth and national defence. Certain countries continue to use advanced cyber espionage programs to obtain unfair advantages in the global marketplace and to improve their military technology. Commercial cyber espionage against Canadian companies is ongoing across a range of fields including aviation, technology and AI, energy, and biopharmaceuticals.[4]

MORE COLLECTED DATA INCREASES PRIVACY RISK

Canadians generate an incredible amount of data about their locations, shopping habits, patterns of life, and personal health when they use their phones and computers, bank and shop online, wear their smart watches and fitness trackers, arm their home security systems, or monitor their insulin levels with smart medical devices. As Canadians generate, store, and share more personal information online, this data becomes vulnerable to cyber threat actors via breaches or misuse by the companies or foreign governments that collect it. The growth in Internet-connected devices has also added to the amount of data collected on Canadians. The Office of the Privacy Commissioner of Canada (OPC) recorded 680 data breaches impacting 28 million Canadians in the year ending on 1 November 2019.[5]

Meanwhile, advances in data science make it more difficult to maintain data anonymity and privacy protections. These technological advances can allow information that was previously anonymous to be linked to other datasets and de-anonymized. Data privacy is an issue of importance for Canadians. A study commissioned by the OPC found that 92% of Canadians expressed concern about the protection of their privacy, with 37% stating that they were extremely concerned.[6]





ADVANCED CYBER TOOLS AND SKILLS ACCESSIBLE TO MORE THREAT ACTORS

An Increasing Commercial Market for Cyber Tools and Talent

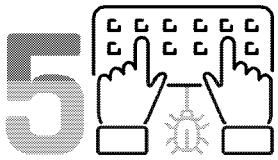
The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity, which increases the challenges inherent in identifying, attributing, and defending against cyber threat activity. Commercial markets for tools and talent have resulted in a shortening of the time it takes for a state to build a cyber program and an increase in the number of states with cyber programs. The Council on Foreign Relations maintains a growing list of countries suspected of sponsoring cyber operations since 2005. The current list stands at 33 countries.[7]

The global market for cyber products and services is projected to grow from approximately $204 billion CAD in 2018 to $334 billion CAD in 2023.[8] State-sponsored threat actors are recruiting skilled expatriates with lucrative salaries as a way to rapidly develop their national cyber programs. This is a significant change from when states had to develop their own cyber talent pipeline and build their own tools.

A Blossoming Cybercrime Ecosystem

In addition to a large legitimate commercial market, there is also an illegal market for cyber tools and services. Many online marketplaces allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrimes, including website defacement, espionage, DDoS attacks, and ransomware attacks. Purchasing tools and services greatly reduces the start-up time for cybercriminals and enables them to use better tools.

The development of cryptocurrency has facilitated the activities of cybercriminals and states as a means of exchanging and laundering money with greater anonymity. Without cryptocurrencies, many forms of cybercrime would be cost-prohibitive for cybercriminals. Anti-money laundering laws have been implemented in many countries to counter cybercrime. However, the success of cybercriminals is partially dependent upon jurisdictions in states around the world with lenient or non-existent laws and law enforcement related to cybercrime. For example, in Russia, China, and Iran, cybercriminals are very unlikely to be prosecuted for financially motivated cyber threat activity against targets outside of the country.[9]



INTERNET AT A CROSSROADS

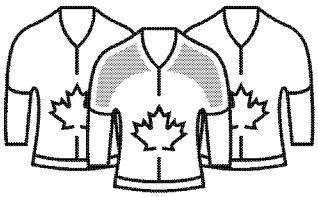
Internet Governance

Many states are pushing hard to change the accepted approach to Internet governance from the multi-stakeholder approach to one of state sovereignty. They view ideas and information primarily through the lenses of domestic stability and national security and want an Internet that will allow them to track their citizens and censor information. Some of these regimes use the Internet to quell protests, arrest dissidents, feed their citizens misinformation, and surveil them.[10] The leaders of the state-sovereignty governance model, China and Russia, continue to push their agenda in international forums such as the International Telecommunications Union (ITU) and other UN bodies, via policy proposals and technical standards proposals. Technical standards can have extraordinary real-world implications, as can be seen in the New Internet Protocol (NIP) proposal made by China and Chinese telecommunications companies, as the NIP would fundamentally transform the way the Internet works.[11] The NIP would provide certain cyber security advantages, but it would enable powerful censorship, surveillance, and state control.[12]

Historically, the dominant approach to Internet governance has been the multi-stakeholder approach championed by Canada and like-minded countries, that includes wide participation from governments, industry, civil society, and academia meeting across a range of bodies that establish technical and policy guidelines. This approach views the Internet as a global development tool that must balance universal access and interoperability with privacy and security.

Online Foreign Influence

As we noted in our Cyber Threats to Canada's Democratic Process Assessment, adversaries use online influence to further their core interests, which typically consist of national security, economic prosperity, and ideological goals. Online foreign influence activities have become a new normal, and adversaries seek to influence domestic events like elections as well as impact international discourse related to current events. Online democratic engagement requires a fair, open Internet, free from manipulation by foreign actors. An increasing number of states have developed cyber tools and are using them to carry out large-scale online influence activities. They exploit social media and legitimate advertising and information-sharing tools to reach a large audience and make their messaging more effective. Deepfake technology—allowing the creation of realistic-looking videos of events and public figures—adds another layer of uncertainty and confusion for the targets of disinformation campaigns. Deepfake technology has developed rapidly, with the industry expanding to include various face swapping applications, products that can produce a video of a full person from scratch[13], and audio deepfake software that is capable of cloning existing human voices.[14]



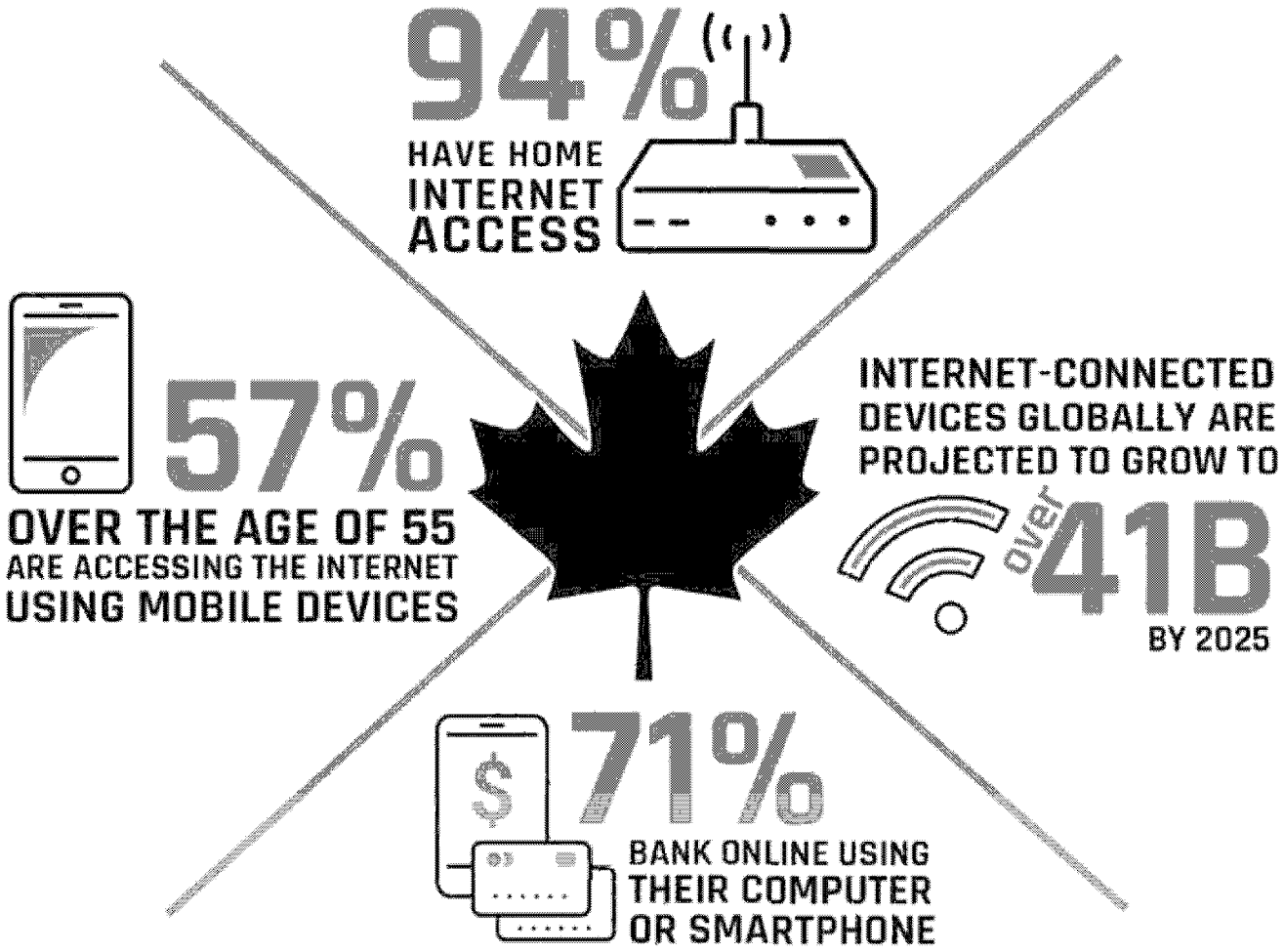
CYBER THREATS TO CANADIAN INDIVIDUALS

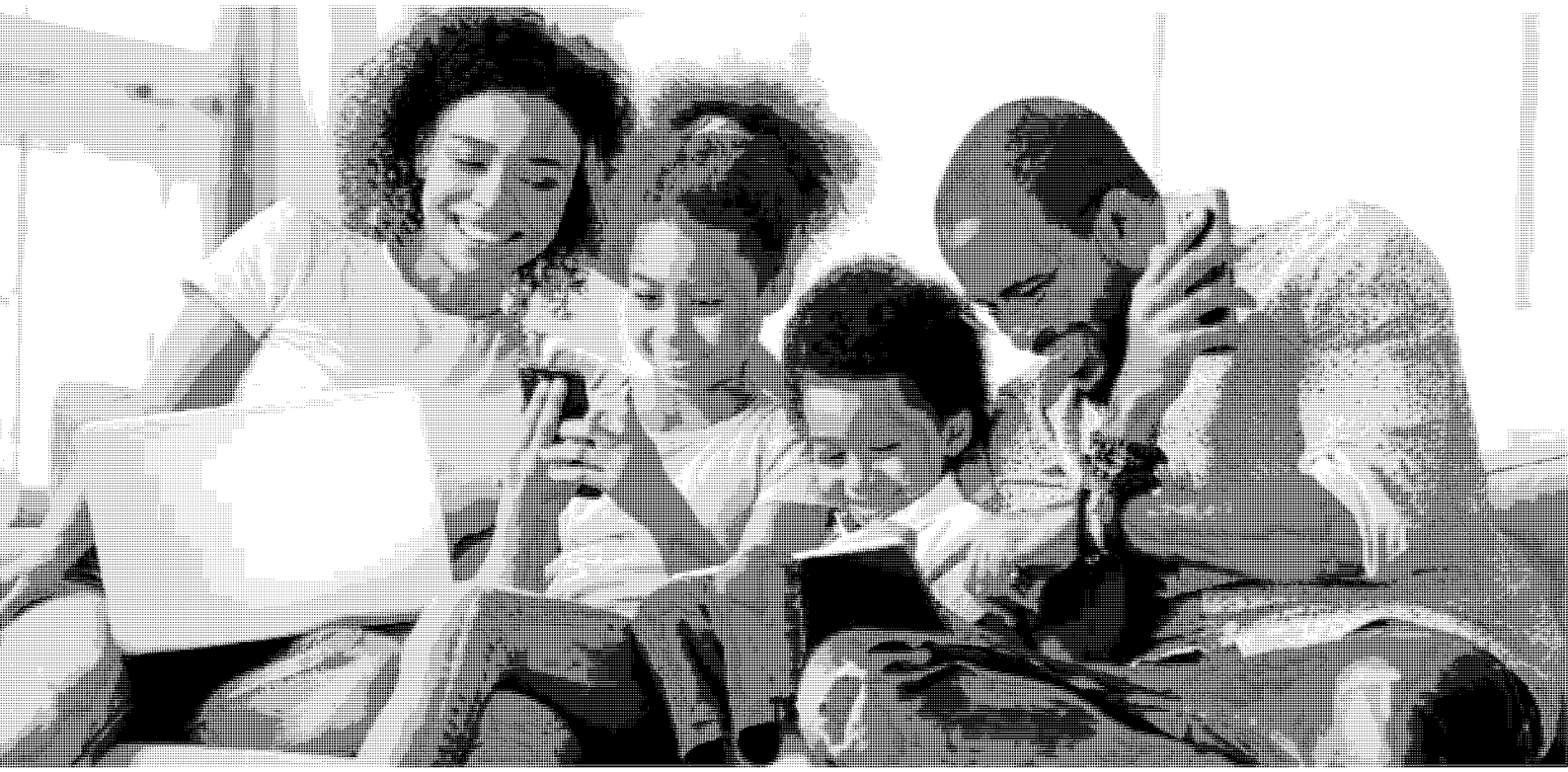
Canadians are putting more of their personal information online, and they increasingly depend on Internet-connected devices for communication, finances, entertainment, comfort, and safety. As technology and habits change, cyber threat actors adapt quickly to take advantage of new opportunities and keep pace with current events, including modifying cyber threat activity during the COVID-19 pandemic.

Canadians continue to fall victim to online fraud schemes. As mentioned in NCTA 2018, we assess that cybercrime will almost certainly continue to be the cyber threat that Canadians are most likely to encounter. Since NCTA 2018, cyber threat actors have improved their ability to keep scams relevant and appealing by associating their cyber fraud operations with current events. Elections, tax season, and trending news stories have all been used as a backdrop for cybercrime. For example, threat actors have leveraged the COVID-19 pandemic to trick victims into clicking on malicious links and attachments. Cyber threat actors also steal financial, medical, and other personal information to sell online or use in cybercrimes. Large corporate data breaches impact millions of customers and reveal personal information that can be used in follow-on crimes.

Canadians also continue to be subjected to online foreign influence operations that seek to influence Canadian public opinion and political discourse. Finally, evolving technologies like IoT medical devices, Internet-connected vehicles, and smart home security systems provide new targets for cyber threat actors to threaten the physical safety of Canadians.

Figure 1: Canadian Internet Usage, from 2018 Canadian Internet Use Survey by Statistics Canada[15], 2019 CIRA Internet Factbook [16], and forecasts of the International Data Corporation[17]





FRAUD AND EXTORTION

Individual Canadians lost over $43 million CAD to cybercrime fraud in 2019, according to statistics from the Canadian Anti-Fraud Centre.[18] This number only accounts for the reported cases of cybercrime fraud, and we assess that it is almost certain that actual amounts are higher. As predicted in NCTA 2018, over the last two years, we have observed increasingly sophisticated cyber fraud and extortion attempts directed at Canadians. We assess that this trend will almost certainly continue, facilitated by cybercrime marketplaces that enable threat actors to purchase cybercrime tools and services.

One way that cyber threat actors conduct fraud is by posing as legitimate organizations, such as government institutions, banks, or law firms to trick Canadians into clicking on malicious links or attachments which download malware onto their devices. For example, scammers create fake websites and online ads that offer cheap immigration services or may even guarantee high paying jobs for new immigrants. Many of the websites look like official government sites but require the victim to pay a fee to access "important forms".[19] Since March 2020, the Cyber Centre has worked with partners to take down over 3,500 websites, social media accounts, and email servers that were fraudulently representing the Government of Canada.

Cyber threat actors also extort money from victims by threatening cyber attacks or by stealing or claiming to have stolen incriminating information from victims. Threat actors also create fake profiles on social media and dating websites, which they use to lure victims into an online relationship that facilitates extortion and fraud. In some cases, they obtain intimate videos of their victim and then threaten to send the video to the victim's contacts unless they receive payment.[20]

THREAT ACTORS LEVERAGE A GLOBAL CRISIS – COVID-19

In 2020, we have observed cyber threat actors developing COVID-19-related content to trick victims into clicking on malicious links and attachments. Cyber threat actors know that people are anxious about the future and are less likely to act prudently when presented with emails, SMS messages, or advertisements related to COVID-19.

COVID-19 lures often attempt to replicate or imitate the branding and style of legitimate organizations, such as international organizations and public health agencies. Cyber threat actors can produce convincing copies of government websites and official correspondence. One SMS phishing campaign claimed to provide access to a Canadian Emergency Response Benefit payment, but only after the target divulged personal financial details. Another campaign impersonated the Public Health Agency of Canada's Medical Officer of Health to deliver malware through a fake COVID-19 update that appeared official and legitimate.

Figure 2: The Elements of Malicious Communication

THREATS TO PRIVACY

In NCTA 2018, we described how financial and personal information is attractive to cybercriminals and how they can exploit stolen information for financial gain. This remains true, but the threat has increased due to the growing quantity of information that is stored online as well as improvements in data science that enable new methods for exploiting stolen personal, financial, and even medical information.

In addition, cybercriminals are not the only cyber threat actors interested in this data: state-sponsored actors have also been observed compromising large databases to advance national priorities.

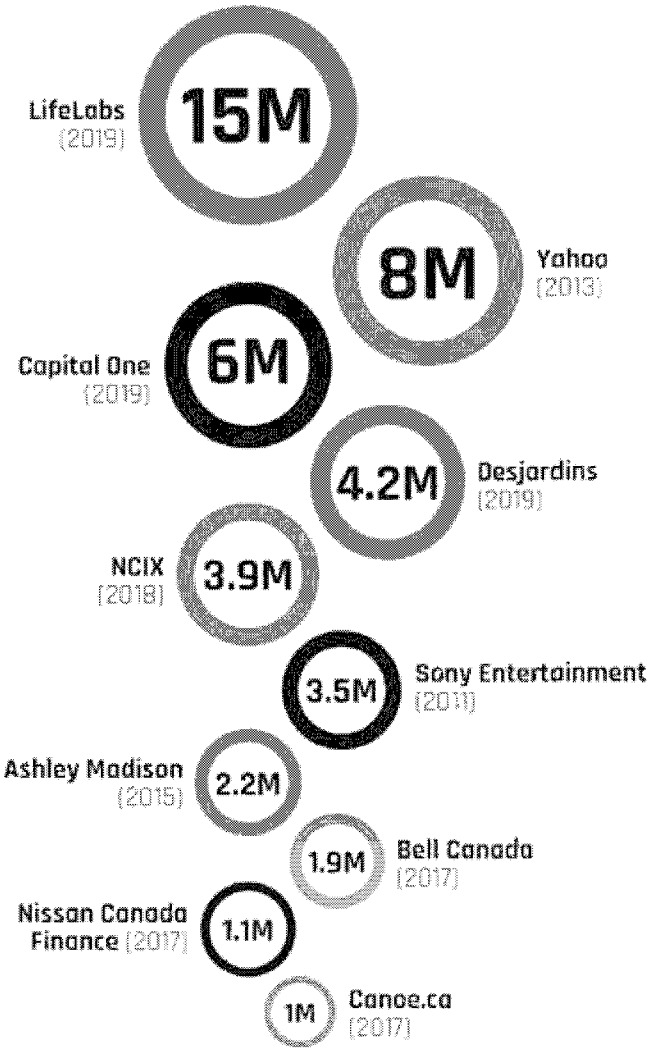
Financial Information

As more information is shared and stored online, the threat to individual privacy increases. Data breaches threaten the financial information of Canadians that is held by businesses which fall prey to cyber threat actors. Stealing personal and financial information from Canadians is profitable for cybercriminals, and we assess that it will likely increase in the next two years.

Cybercriminals profit by obtaining login credentials, credit card details, and other personal information and then using this information to steal money, commit fraud, or sell it on cybercrime marketplaces. In June 2019, the data breach of Canadian financial services company Desjardins affected the records of 4.2 million of its Canadian customers.[21] Personal information including names and birthdates, social insurance numbers, contact information, and banking details were compromised.

A similar event against another financial institution, Capital One, occurred in March 2019, exposing the personal information of 6 million Canadian customers. The stolen data included personal information in addition to credit scores, transaction data, and bank account numbers.[22]

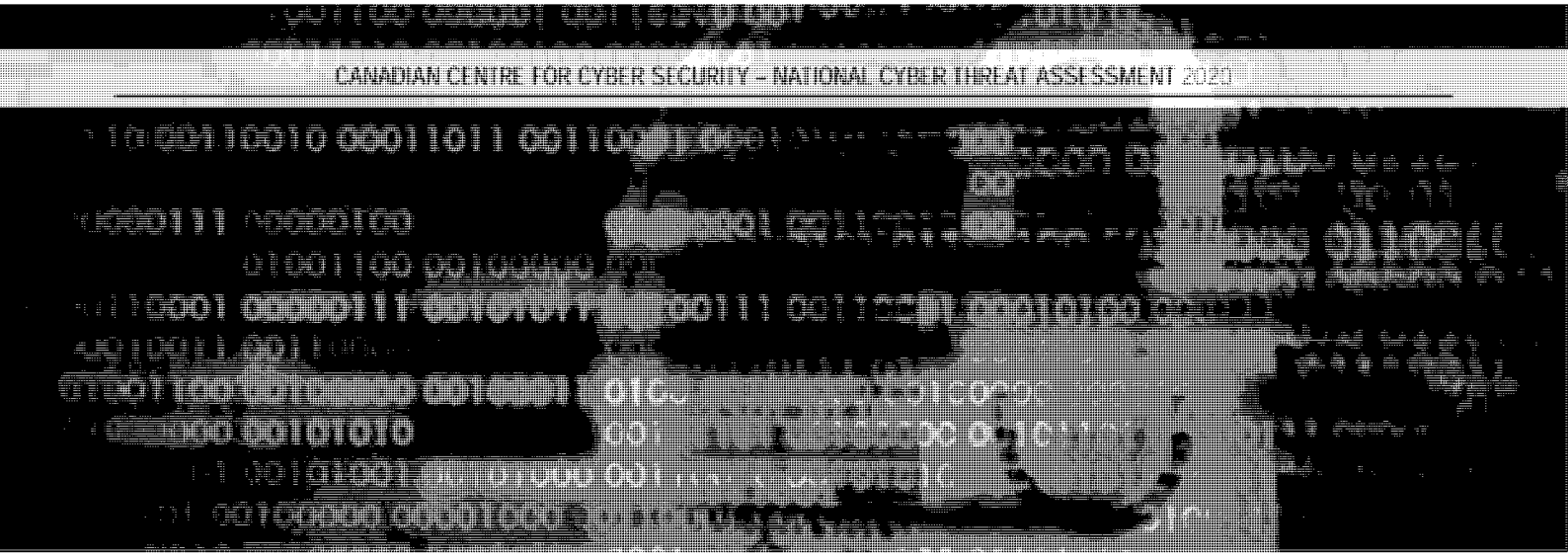
Figure 3: Ten of the Largest Data Breaches Impacting Canadians, 2011 to Present, by number of records



CRYPTOCURRENCY AND CRYPTOJACKING

Cybercriminals use malware to take unauthorized control of the processing power of computers to generate or "mine" cryptocurrency. This is called cryptojacking. Out-of-date or unpatched systems are particularly vulnerable to cryptojacking and some owners may be completely unaware that their device has been compromised, while others may experience slower performance or a rapidly drained battery.[23]

As we predicted in the 2018 NCTA, we have seen cybercriminals continue to develop and deploy malware in cryptojacking operations. We assess that this activity will very likely continue in the next two years, with activity levels linked to the fluctuations in cryptocurrency values.



Medical and Personal Data

In 2019, medical laboratory testing firm LifeLabs was the victim of a cyber breach that compromised the sensitive personal and medical information of 15 million Canadians before the lab paid a ransom to retrieve the information.[24] Threat actors, particularly state-sponsored cyber actors, are using data science to make better use of large datasets. They can identify, profile, and track individuals by combining and de-anonymizing data from multiple datasets.

Stolen personal data can be used by cyber threat actors for credential stuffing, where large numbers of compromised pairs of usernames and passwords are entered into websites in the hopes that one will match an existing account on the site. Stolen personal data can include credentials that allow this type of activity as well as access to the answers to personal security questions, rendering this protection ineffective. After collecting data from multiple breaches, cybercriminals may be able to combine the available personal information on an individual and more effectively target cyber threat activity.

CAPITAL ONE AND MARRIOTT BREACHES

The accumulation of data attracts both cybercriminals and state-sponsored cyber threat actors. In 2019, a cybercriminal stole customer data from US financial services firm Capital One. The breach affected 106 million individuals, including six million Canadians, and collected private data including social insurance/security numbers and bank account details.[25] In 2018, Marriott Hotels announced that its reservation system had been breached, and that private data on about 500 million guests was stolen. The attack was linked to state-sponsored hackers and allowed them to collect data including names, addresses, and passport numbers.[26]

ONLINE FOREIGN INFLUENCE

A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally. They try to delegitimize the concept of democracy and other values such as human rights and liberty, which may run contrary to their own ideological views. They also try to exacerbate existing friction in democratic societies around various divisive social, political, and economic issues. While online foreign influence activities tend to increase around elections, these ongoing campaigns have broadened in scope since 2018, expanding to react and adapt to current events, shifting their content strategies around trending news stories and popular political issues.

As predicted in NCTA 2018, Canadians have continued to be the subject of online foreign influence activity. For instance, we have observed recent campaigns focus their content around COVID-19 and government responses to the pandemic. Disinformation campaigns have also sought to discredit and criticize Canadian politicians to damage their reputations. However, we assess that relative to some other countries, Canadians are lower-priority targets for online foreign influence activity, though Canada's position on high-tension geopolitical issues could increase the threat. Crucially, Canada's media ecosystems are closely intertwined with those of the United States and other allies, which means that when their populations are targeted, Canadians become exposed to online influence as a type of collateral damage.

We assess that Canadians' exposure to online foreign influence is almost certainly going to continue for the next two years or more, though threat actors will be forced to adapt their activities to the changing policies of Internet companies such as Google, Facebook, and Twitter.

STATE-SPONSORED ACTORS SEEKING TO DIVIDE CANADIANS

Analysis of publicly released Twitter data revealed that Russian and Iranian online trolls used fraudulent Twitter accounts to highlight divisions among Canadians by amplifying inflammatory arguments surrounding divisive political issues such as terrorism, climate change, pipeline construction, and policies on immigration and refugees. Many of these tweets reacted to major news events such as the January 2017 Quebec City mosque shooting and the June 2019 approval of the Trans Mountain Pipeline expansion project.[27]

THREATS TO PHYSICAL SAFETY AND SECURITY

Personal Internet-connected devices, including IoT medical devices, Internet-connected vehicles, and smart home security systems are being integrated into day-to-day life and providing new targets for cyber threat actors. While other cyber threats, such as data breaches, are more common and have broader impacts, there is a risk that future cyber threat activity against these devices and systems can impact physical safety. For example, Internet-connected medical devices are increasingly common and are vulnerable to cyber threat actors who could target these devices and degrade or disrupt their performance.

As another example, stalkers and abusive partners are taking advantage of vulnerabilities in personal IoT devices to steal information collected by fitness trackers and smart home technologies to identify and locate their victims. They are also manipulating smart home devices to control a victim's surroundings and intimidate them. In one case, a man operated a smart vehicle application that allowed him to stop, start, and track his victim's vehicle from his phone.[28] An organization providing support for victims of domestic abuse reported that, as of January 2019, more than 2,500 of its clients had reported experiences of technology-facilitated abuse.[29]

INTERNET-CONNECTED PERSONAL MEDICAL DEVICES

In March 2020, Health Canada issued an alert that medical devices, such as pacemakers, blood glucose monitors, and insulin pumps with a particular Bluetooth chip were vulnerable to cyber attacks that could crash the device, unlock it, or bypass security to access functions that should only be available to an authorized individual.[30]

CYBER THREATS TO CANADIAN ORGANIZATIONS

As we predicted in NCTA 2018, cybercrime remains the most common threat faced by Canadian organizations of all sizes. However, other cyber threat activity, such as cyber espionage, can have a greater impact. Information stolen by cyber threat actors can be held for ransom, sold, or used to gain an unfair competitive advantage. Over the past two years, targeting of industrial processes and ransomware attacks have become regular occurrences resulting in major impacts, including reputational damage, productivity loss, legal repercussions, recovery expenses, and damage to infrastructure and operations. We assess that ransomware directed against Canada in the next two years will almost certainly continue to target large enterprises and critical infrastructure providers.

Cyber threat actors also put the information held by Canadian organizations at risk, including intellectual property as well as customer and client data. The theft of this information can have both short- and long-term financial consequences for the victims, including impacts to global competitiveness and reputational damage. During the COVID-19 pandemic, state-sponsored cyber threat actors have targeted Canadian intellectual property related to combatting COVID-19, and we assess that it is almost certain that state-sponsored actors will continue to do so in order to support their own domestic public health responses or to profit from its illegal reproduction by their own firms.

Cyber threat actors also exploit trusted business relationships between Canadian organizations, target both online and in-person payment systems, exploit supply chain vulnerabilities, and take advantage of the privileged access managed service providers maintain into the networks of their clients. These activities can be used to defraud organizations, conduct ransomware attacks, or steal proprietary information or customer and client data.

Canadian organizations of all sizes, such as small- and medium-sized enterprises, municipalities, universities, and critical infrastructure providers, face a growing number of cyber threats.[31]

These organizations control a range of assets that are of interest to cyber threat actors, including intellectual property, financial information and payment systems, data about customers, partners and suppliers, and industrial plants and machinery. As a general rule, the more Internet-connected assets an organization has, the greater the cyber threat it faces.

Figure 4: List of Assets Owned by Organizations that can Increase Cyber Security Risk

TARGETING THE SAFETY OF CANADIANS

Targeting Industrial Control Systems and Critical Infrastructure

The safety of Canadians is at risk when cyber threat actors target organizations responsible for the operation of utilities, delivery of healthcare, or provision of essential government services. However, as we judged in NCTA 2018, we assess that it remains very unlikely that cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for potential future activities, or as a form of intimidation. We judge that state-sponsored actors are very likely attempting to develop the additional cyber capabilities required to disrupt the supply of electricity in Canada.

Industrial control systems (ICS) are a type of OT that monitors and controls physical equipment in industrial or critical infrastructure processes. Especially in the electricity sector, ICS are targeted across the world, mostly by state-sponsored cyber threat actors. In 2019, Russia-associated actors probed the networks of electricity utilities in the US and Canada.[32] Iranian hacking groups have targeted ICS infrastructure in rival nations, including the US, Israel, and Saudi Arabia.[33] North Korean malware has been found in the IT networks of Indian power plants, and US utility employees have been targeted by Chinese state-sponsored cyber threat actors.[34]

In recent years, ransomware has increasingly impacted ICS. We assess that ransomware has almost certainly improved its ability to spread through corporate IT networks and threaten adjacent ICS environments. In some cases, victims have chosen to disable their industrial processes as a precautionary measure during a significant ransomware event. For example, in March 2019, a Norwegian aluminum company was impacted by a ransomware event that disrupted its logistical and production data so severely that it prompted the shutdown of ICS control and reversion to manual operations.[35] We assess that cybercriminals will very likely increase their targeting of ICS in the next two years in an attempt to place increased pressure on critical infrastructure and heavy industry victims to promptly accede to ransom demands.

ICS RANSOMWARE IN ACTION

Since January 2019, at least seven ransomware variants have contained instructions to terminate ICS processes.[36] The impact of these attacks on ICS varies according to the specific circumstances of the industrial process and the reaction of the site staff.[37] In June 2020, a car manufacturer halted production at most of its North American plants, including one in Canada, "to ensure safety" after very likely being hit by one of these ransomware variants.[38]

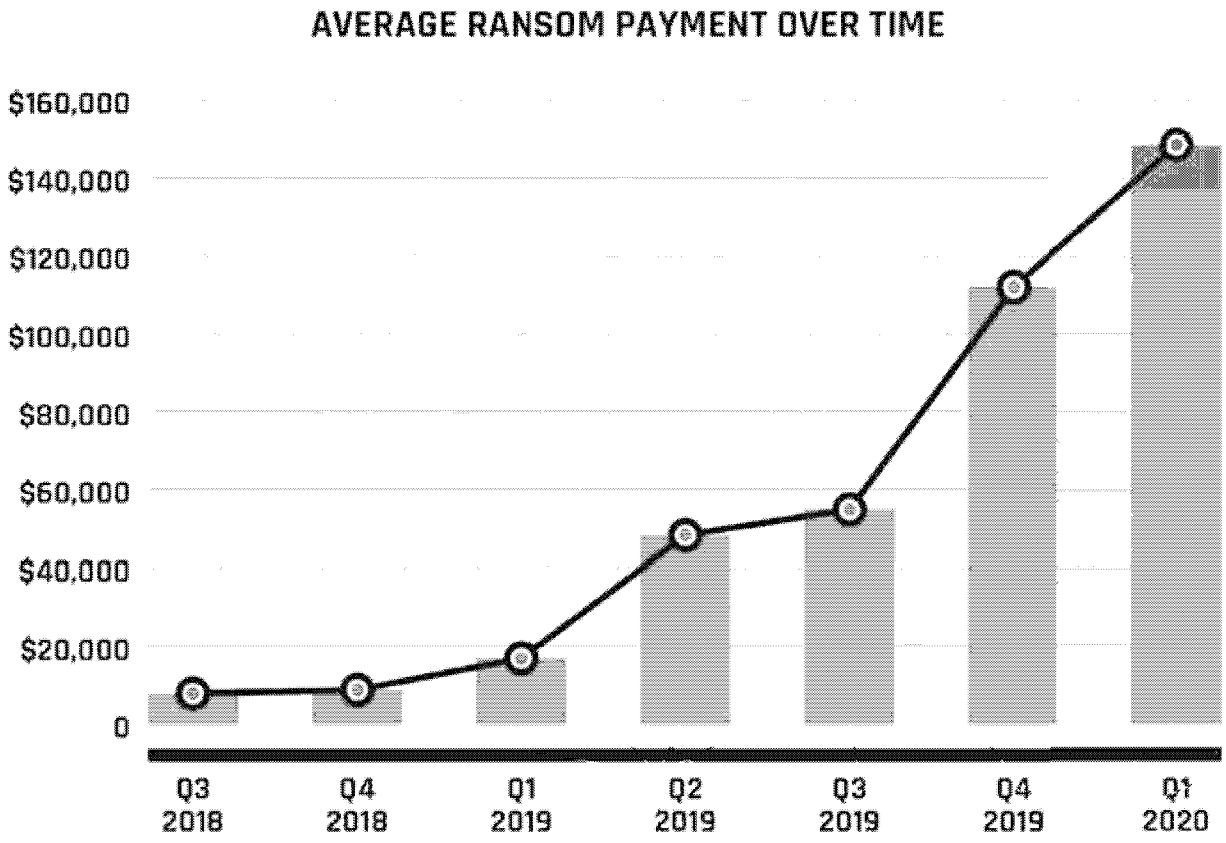
THREATS TO CANADIAN FINANCIAL AND ECONOMIC HEALTH

Cyber threat activity results in unwanted expenses for organizations, including the costs of ransoms or stolen funds, losses due to the disruption of operations, the price of securing and insuring networks, reputational damage and related loss of customers, and theft of intellectual property or confidential information.[39] These costs are a drain on organizations' finite resources and decrease their competitiveness against other companies. Taken together, they are also a drain on the Canadian economy.

Ransomware and Big Game Hunting

NCTA 2018 identified ransomware as the most common form of malware used for extortion against Canadian individuals. While it has remained prevalent, cybercriminals have shifted their tactics to allow them to increase their ransom demands and increase the likelihood of success. In recent years, cybercriminals have increasingly engaged in big game hunting (BGH), focusing their activities against large enterprises that will not tolerate sustained disruptions to their networks and are willing to pay large ransoms to quickly restore their operations.[40] As BGH ransomware campaigns have become more common, the value of ransom demands has increased. Ransomware researchers estimate that the average ransom demand increased by 33% since Q4 2019 to approximately $148,700 CAD in Q1 2020 due to the impact of targeted ransomware operations.[41] At the more extreme end of the spectrum are multi-million-dollar ransom events, which have become increasingly common. In October 2019, a Canadian insurance company paid $1.3 million CAD to recover 20 servers and 1,000 workstations.[42] In addition, we assess that it is likely that state-sponsored cyber threat actors will use ransomware to obfuscate the origins or intentions of their cyber operations. It is almost certain that the intelligence services of multiple countries maintain associations with cybercriminals that engage in ransomware schemes. In these mutually beneficial relationships, cybercriminals share stolen data with intelligence services while the intelligence service allows the cybercriminals to operate free from law enforcement.

Figure 5: Average Ransomware Payments, 2018 to 2020 (data from Coveware converted from USD to CAD)[43]



We expect that ransomware directed against Canada in the next two years will almost certainly continue to target large enterprises and critical infrastructure providers. Furthermore, many Canadian victims will likely continue to give in to ransom demands due to the severe economic and potentially destructive consequences of refusing payment. Since late 2019, multiple Canadian businesses and provincial governments have had their data publicly leaked by ransomware operators for refusing payment, including a construction company and a consortium of Canadian agricultural companies.[44]

RANSOMWARE FREQUENTLY TARGETS THE HEALTH SECTOR

In 2019 and 2020, many Canadian health organizations have been targeted in ransomware attacks. For example, three Ontario hospitals were the victims of ransomware attacks in October 2019, and a Canadian diagnostic and specialty testing company was compromised by ransomware in December 2019. In early 2020, ransomware also targeted a medical company in Saskatchewan.[45] During the COVID-19 pandemic, many health sector organizations globally have experienced ransomware attacks, including hospitals and healthcare centres in the Czech Republic, the US, Spain, and Germany.[46] Health sector organizations are popular ransomware targets because they have significant financial resources and network downtime can have life-threatening consequences for patients, increasing the likelihood that victims will pay the ransom.

Stealing Intellectual Property and Proprietary Information

In NCTA 2018, we described the threat posed to Canadian businesses by commercial cyber espionage, and this threat remains today, with state-sponsored cyber threat actors continuing to conduct cyber espionage against the networks of organizations in Canada and allied nations, seeking intellectual property, trade secrets, and other commercially sensitive information. In Canada, these threat actors have conducted espionage against a wide variety of Canadian organizations including businesses, academia, and governments, especially organizations in the health and biotechnology, energy, telecommunications, and defence sectors.[47]

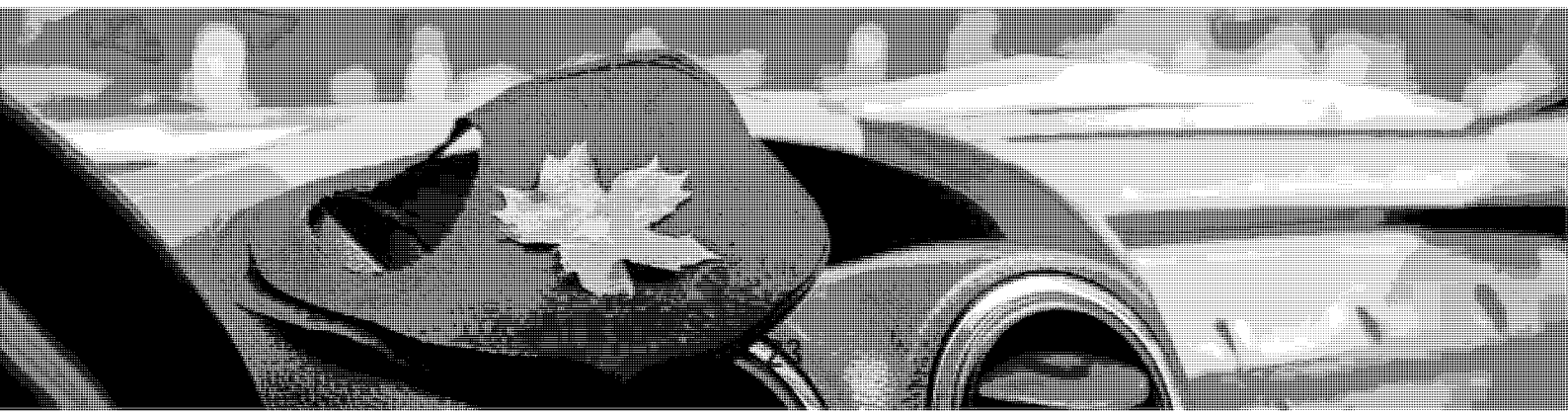
A long-running campaign by state-sponsored cyber threat actors used compromised managed service providers (MSPs) to target intellectual property and confidential business and technological information related to aviation, telecommunications, health and biotechnology, and other sectors. They targeted companies in Canada as well as at least 12 other countries since 2006.[48] In 2019, it was reported that one state-sponsored campaign targeted over two dozen universities in Canada, the US, and Southeast Asia in an attempt to acquire information related to military-use maritime technology and research.[49]

During the COVID-19 pandemic, large medical and biopharmaceutical companies in Canada and abroad have been targeted by state-sponsored cyber threat actors attempting to steal intellectual property related to COVID-19 tests, treatments, and vaccines. We assess that it is almost certain that state-sponsored actors will continue attempting to steal Canadian intellectual property related to combatting COVID-19 in order to support their own domestic public health response or to profit from its illegal reproduction by their own firms.[50]

Organizations with overseas activities and infrastructure face additional cyber threats. Their operations abroad may be governed by different, and sometimes weaker, intellectual property, privacy, or national security laws. Many countries have the legal authority and technical ability to covertly access data when it transits or resides in their country. This has implications for Canadian data and intellectual property that is sent abroad to offices in other states or that transits networks in other countries. Even data that is sent between two entities located in Canada may transit foreign networks as part of the path to their destinations. However, consistent with our judgement in NCTA 2018, we assess that the threat of cyber espionage is almost certainly higher for Canadian organizations that operate abroad or work directly with foreign state-owned enterprises.

RUSSIAN ACTORS TARGETING COVID-19 VACCINE RESEARCH

In July 2020, the Cyber Centre, the UK National Cyber Security Centre, and the US National Security Agency released a joint advisory reporting on the tactics, techniques, and procedures of a state-sponsored cyber threat actor targeting organizations involved in COVID-19 vaccine development in Canada, the US, and the UK.[51] We assess that the cyber threat actor responsible is almost certainly part of the Russian intelligence services and highly likely wishes to steal information and intellectual property relating to the development and testing of COVID-19 vaccines.



Stealing Customer and Client Data

As predicted in NCTA 2018, cyber threat actors continue to target large datasets held by organizations located in Canada and around the world. Large databases containing personal information such as names, addresses, phone numbers, employment information, credentials, and financial details are valuable to cyber threat actors. The aggregation of data collected from multiple breaches can provide cybercriminals with enough information to fraudulently apply for loans or credit cards, file false tax returns, transfer money illegally, extort victims, gain access to online accounts, or engineer persuasive phishing emails.[52] This data can also be used by state-sponsored cyber actors to pursue dissidents, minorities, or espionage targets within their country or abroad.

Data theft by cybercriminals tends to be opportunistic and financially motivated, while state-sponsored cyber threat actors look to acquire large quantities of sensitive information to support broader strategic goals, such as intelligence collection. We assess that over the next two years Canadian organizations will almost certainly continue to be attractive targets for cybercriminals and state-sponsored cyber threat actors interested in obtaining personally identifiable information and other sensitive data.

Cyber threat actors have also increased the sophistication of ransomware operations by threatening to reveal confidential client information unless a ransom is paid, creating additional incentives for victims to acquiesce to their demands.[53] However, even if a payment is made, cyber threat actors can decide to delete, modify, or release information, or use stolen data in a future scam.

THE LARGEST DATA BREACH IN CANADIAN HISTORY

In October 2019, Canadian medical testing company LifeLabs was compromised by cyber threat actors, exposing the sensitive personal information of about 15 million Canadians, representing the largest single breach of personal records in Canada. The information exposed included medical test results, health card numbers, names, dates of birth, home addresses, and email addresses. While the company made a payment to retrieve the data, there is no way to be sure that the threat actors did not keep a copy of the data to further exploit or sell to other criminals.[54]

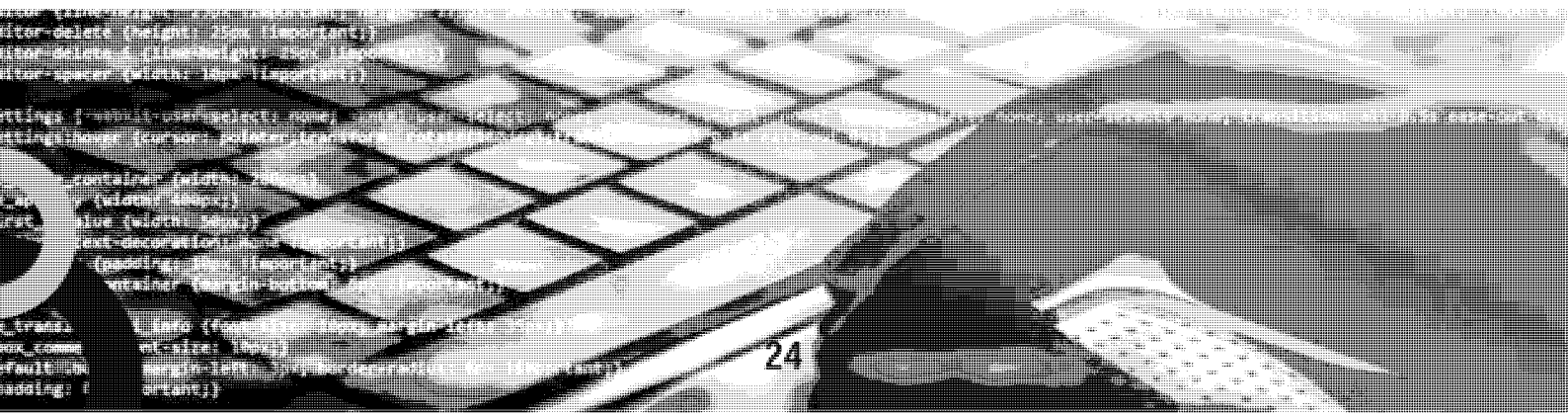
Exploiting Trusted Business Relationships

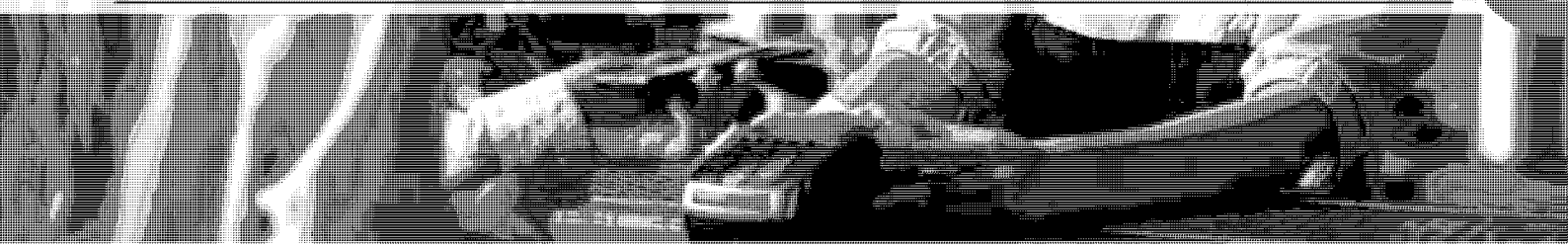
In NCTA 2018, we correctly predicted that cyber threat actors will continue to exploit the trusted relationships between businesses and their suppliers and service providers. Since 2018, financially motivated cyber threat actors have sharply increased their use of certain social engineering techniques to target organizations.[55] One of the most common and costly methods is known as business email compromise (BEC). This refers to an email designed to trick an employee in the target organization into directly transferring funds to cyber threat actors. Often, cyber threat actors impersonate high-level executives or trusted third parties. Cyber threat actors have recently been using the uncertainty surrounding the COVID-19 pandemic to target victims.

BUSINESS EMAIL COMPROMISE TARGETS MORE THAN BUSINESSES

In May 2019, a municipal government in Ontario became the victim of a BEC scam. The threat actors posed as a known and trusted city vendor. In their fake email, they requested to change the banking information for the vendor, and when this was completed, $503,000 CAD was transferred to the new account, owned by the cybercriminal.[56]

Over the past two years, cyber threat actors have expanded the use of BEC beyond traditional business victims to target religious, educational, and not-for-profit organizations.[57] We assess that cyber threat actors will very likely continue to increase their use of BECs because of their simplicity and profitability.[58] By some estimates, between 2016 and 2019, there were more than 1,200 reported cases of BEC fraud in Canada, resulting in losses of more than $45 million CAD.[59] The average BEC loss involving wire transfers is approximately $47,000 CAD.[60]





Exploiting Retail Payment Systems

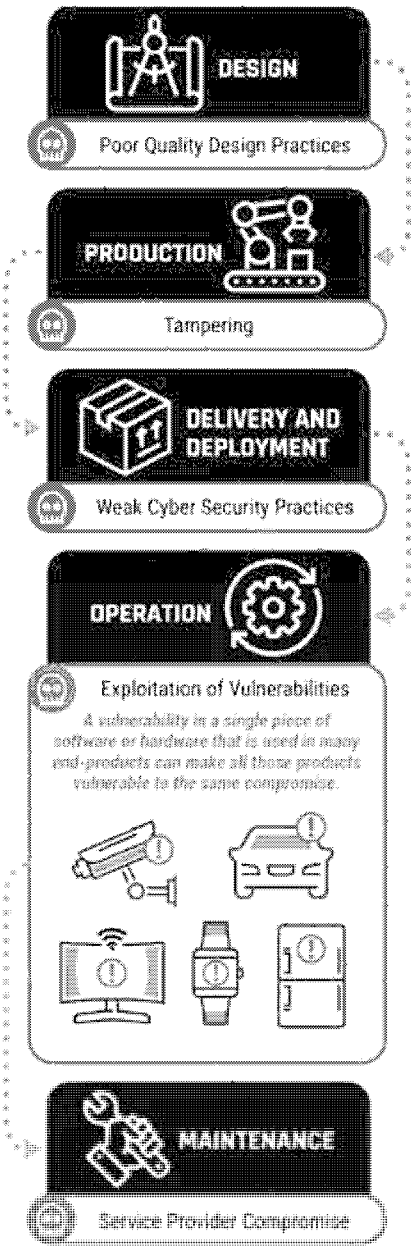
Cybercriminals target payment card data by stealing credit card details and other information that victims enter on e-commerce sites, which is called formjacking.[61] In 2018, approximately 4,800 websites were victims of formjacking each month.[62] Many large websites have been compromised using this technique, including airline companies, ticket sellers, and others.[63] In 2019, more than 200 campus stores at universities and colleges in Canada and the US were affected by formjacking.[64] We assess that this trend will likely increase over the next two years as Canadians are increasingly relying on e-commerce, in part due to the COVID-19 pandemic.[65]

Cyber threat actors also continue to target point-of-sale (POS) systems used by brick-and-mortar businesses, as discussed in NCTA 2018. They do so by installing malware that can steal customer information, interfere with business operations, make fraudulent purchases, manipulate pricing, and cause other forms of disruption. In late 2019, cybercriminals targeted the POS systems at some North American gas stations to steal financial data.[66] Magnetic strip records from credit cards harvested from infected POS terminals are sold on cybercrime marketplaces and allow criminals to recreate or clone cards.

Exploiting Supply Chains

Many organizations rely on a complex and often globally distributed supply chain for many aspects of their operations, including precursor manufacturing, IT infrastructure and support, and financial services.[67] Cyber threat actors target the networks of trusted vendors and then leverage the vendors to access the networks of their true targets. Supply chain compromises can occur before or after the delivery of a product or service, or during software updates or hardware upgrades. Cyber threat actors target these updates and upgrades because they know they will be downloaded and installed thousands or millions of times in any number of organizations, and therefore create many opportunities. As Figure 6 shows, every link in a global supply chain can pose a risk to cyber security. In 2018, we correctly predicted that cyber threat actors would increasingly try to exploit supply chain vulnerabilities. We assess that cyber threat actors will almost certainly continue to exploit these vulnerabilities over the next two years.

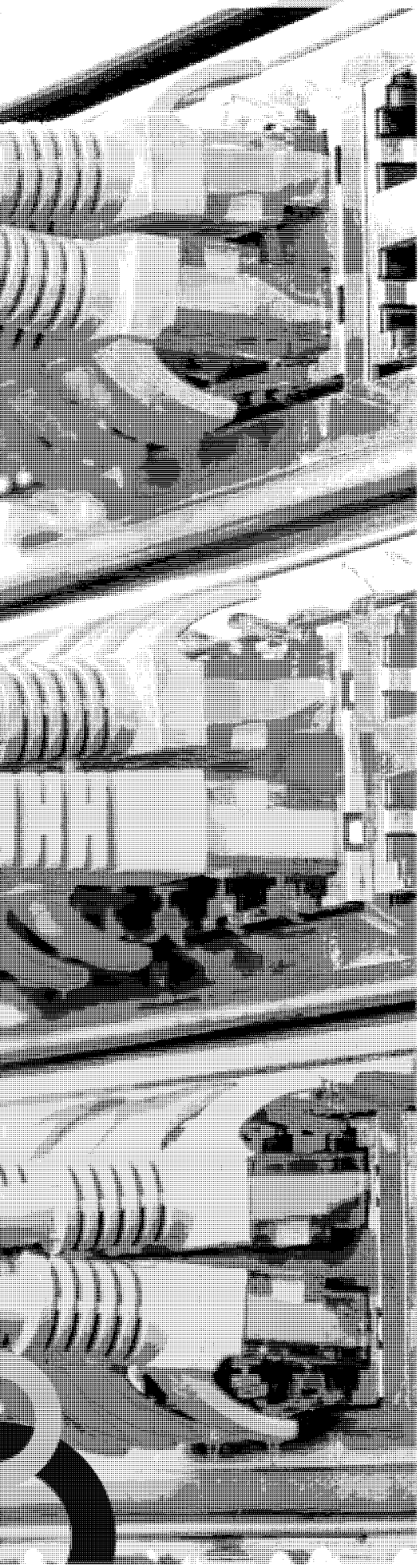
Figure 6: Supply Chain Vulnerabilities



EXPLOITING SUPPLY CHAIN VULNERABILITIES

Since the start of the COVID-19 pandemic, cyber threat actors have gained access to a large number of hospitals globally, compromising both IT networks and ICS components and imaging products used in the healthcare industry.[68] In 2018 the same actors targeted health sector organizations in at least 24 countries, including in Canada, as well as organizations in other sectors, such as manufacturing, IT, logistics, and agriculture.[69]

We judge that it is likely that this actor compromised its victims by using software updates from trusted vendors to spread its malware.[70] We assess that the responsible actors are likely state-sponsored and interested in acquiring sensitive or proprietary information to advance national priorities.

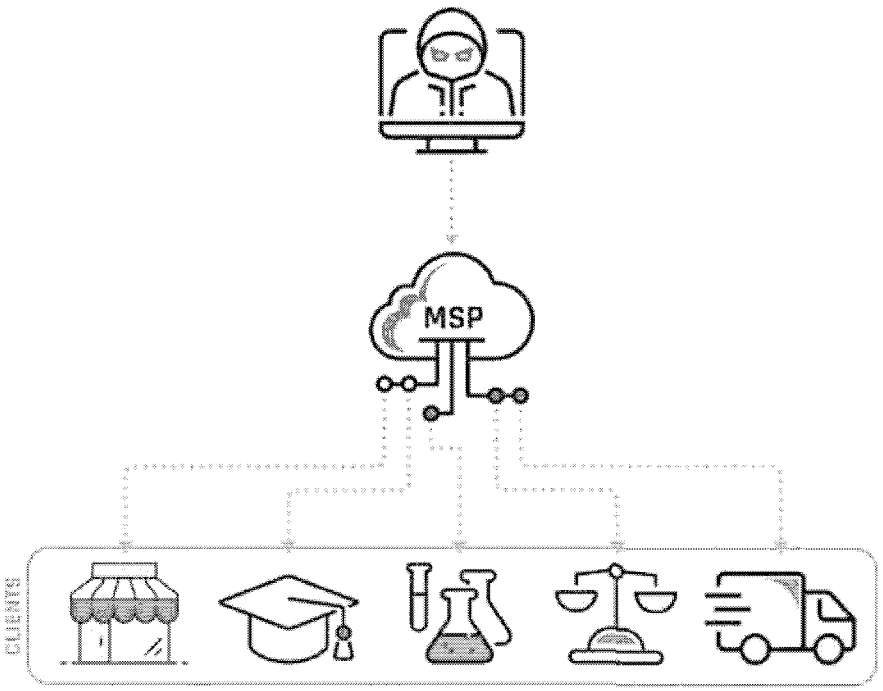


Exploiting Managed Service Providers

An MSP is a company used by organizations to provide IT services and reduce the cost of maintaining in-house IT infrastructure and personnel. When a corporate network is well-defended against direct attacks, cyber threat actors can target MSPs to obtain indirect access to client networks. In addition, threat actors who successfully compromise an MSP can reach a large number of victims: the MSP's clients.

NCTA 2018 correctly predicted that MSPs would remain attractive targets for advanced cyber threat actors. Throughout 2019, cybercriminals compromised MSPs for the purpose of abusing software used to remotely manage IT systems to automatically install ransomware on multiple client networks at once.[71] We expect that over the next two years ransomware campaigns will very likely increasingly target MSPs for the purpose of targeting their clients as a means of scaling targeted ransomware campaigns.

Figure 7: Exploitation of Managed Service Providers (MSP)



By targeting MSPs, threat actors can gain access to the MSP's clients (including businesses, universities, and other institutions) without having to compromise each client directly.

CONCLUSION

The cyber threat landscape in Canada is evolving and cyber threat actors continue to adapt their activities to keep up. In this National Cyber Threat Assessment, we identified trends within the threat landscape and the evolving cyber threat activities faced by Canadian individuals and organizations. Canadians' adoption of new technology and Internet-connected devices will usher in new threats.

As we wrote in 2018, many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats and influence operations continue to succeed today because they exploit deeply rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada against cyber threats and related influence operations requires addressing both the technical and social elements of cyber threat activity. Cyber security investments will allow Canadians to benefit from new technologies while ensuring that we do not unduly risk our safety, privacy, economic prosperity, and national security.

The Cyber Centre is dedicated to advancing cyber security and increasing the confidence of Canadians in the systems they rely on daily, offering support to critical infrastructure networks as well as other systems of importance to Canada.

We approach security through collaboration, combining expertise from government, industry, and academia. Working together, we can increase Canada's resilience against cyber threats.

USEFUL RESOURCES

- An Introduction to the Cyber Threat Environment
- Cyber Hygiene
- Get Cyber Safe Campaign
- Spotting Malicious Email Messages
- Don't Take the Bait: Recognize and Avoid Phishing Attacks
- CRA Guidance – Protect Yourself Against Fraud
- How to Use Online Banking Securely
- How to Shop Online Safely
- Using Your Mobile Device Securely
- How Updates Secure Your Device
- Password Best Practices
- Rethink Your Password Habits to Protect Your Accounts from Hackers
- Biometrics Security
- Implementing Multi-Factor Authentication
- Password Managers Security Tips
- Using Bluetooth Technology
- Artificial Intelligence
- Joint Report on Publicly Available Hacking Tools
- Protect Your Organization from Malware
- Ransomware: How to Prevent and Recover
- Protecting Your Organization from Denial of Service Attacks
- Cyber Security Considerations for Contracting with Managed Service Providers
- Employees and Social Media
- Using Virtual Desktop At-Home and In-Office
- Virtual Private Network
- Cyber Security Tips for Remote Work
- Security Tips for Organizations with Remote Workers
- IoT Security for Small and Medium Organizations
- Supply Chain Security for Small and Medium Organizations
- Security Considerations for Research and Development
- Cyber Security for Healthcare Organizations: Protecting Yourself from Common Cyber Attacks
- COVID-19 Malicious Websites
- Focused Cyber Security Advice and Guidance during COVID-19: List of Publications by Audience
- Cyber Security Advice and Guidance for Research and Development Organizations During COVID-19
- Canadian Shield – Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic

ENDNOTES

[1] BlueLeaks Data Breach Involved 38 Canadian Police Forces." *CBC News*. 22 September 2020. https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311.

[2] "IoT Makes Industrial Manufacturers "Smart"." *PwC*. Accessed 15 July 2020. https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov/manufacturing-iot-snapshot.html.

[3] Canada's Internet Factbook 2019." *Canadian Internet Registration Authority*. 2019. https://www.cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019. "Canadian Internet Use Survey." *Statistics Canada*. 10 May 2010. https://www150.statcan.gc.ca/n1/daily-quotidien/100510/dq100510a-eng.htm. "Canadian Internet Use Survey." *Statistics Canada* 26 November 2013. https://www150.statcan.gc.ca/n1/daily-quotidien/131126/dq131126d-eng.htm. "Canadian Internet Use Survey." *Statistics Canada*. 29 October 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm.

[4] David Vigneault. "Remarks at the Economic Club of Canada." *Government of Canada*. 04 December 2018. https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.

[5] "A full year of mandatory data breach reporting: What we've learned and what businesses need to know." Office of the Privacy Commissioner of Canada." 31 October 2019. https://www.priv.gc.ca/en/blog/20191031/.

[6] "2018-19 Survey of Canadians on Privacy." *Office of the Privacy Commissioner of Canada*. 11 March 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

[7] "Cyper Operations Tracker." *Council on Foreign Relations*. Accessed 15 September 2020. https://www.cfr.org/cyber-operations/.

[8] "Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023." *Markets and Markets*. September 2018. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html.

[9] "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware." *US Department of the Treasury*. 05 December 2019. https://home.treasury.gov/news/press-releases/sm845; Tim Maurer. "Why the Russian Government Turns a Blind Eye to Cybercriminals." *Slate*. 02 February 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html. "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." *United States Department of Justice*. 16 September 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East." *United States Department of Justice*. 16 September 2020. https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[10] "Canadian Internet Governance Forum Report 2019." *Canadian Internet Registration Authority*. 27 February 2019. https://canadianigf.ca/wp-content/uploads/2019/06/2019_CIGF_report_EN-1.pdf.

[11] Hascall Sharp and Oaf Kolkman. "Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T." *Internet Society*. 24 April 2020. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

[12] Jon Fingas. "China, Huawei propose internet protocol with a built-in killswitch." *Engadget*. 30 March 2020. https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

[13] Craig Silverman. "How to Spot a Deepfake Like the Barack Obama - Jordan Peele Video." *Buzzfeed News*. 17 April 2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed.

[14] "XR Belgium posts deepfake of Belgian premier linking COVID-19 with climate crisis." *The Brussels Times*. 14 April 2020. https://www.brusselstimes.com/all-news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/.

[15] "Canadian Internet Use Survey." *Statistics Canada*. 29 October 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm.

[16] Canada's Internet Factbook 2019." *Canadian Internet Registration Authority*. 2019. https://www.cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019.

[17] "The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast." *International Data Corporation*. 18 June 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[18] Sawyer Bogdan. "Canadians have lost $43 Million to Cybercrime in 2019: OPP." *Global News*. 24 October 2019. https://globalnews.ca/news/6077016/canadians-lost-43-million-cybercrime-2019/.

[19] "Scams by Medium." *Canadian Anti-Fraud Centre*. 13 February 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm.

[20] "Scams by Medium." *Canadian Anti-Fraud Centre*. 13 February 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm.

[21] John MacFarlane. "4.2 million Desjardins members affected by data breach, credit union now says." *CBC News*. 01 November 2019. https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[22] Aidan Wallace. "Major Data Breaches in 2019." *Toronto Sun*. 01 January 2020. https://torontosun.com/news/world/major-data-breaches-in-2019.

[23] Ken Hsu, Durgesh Sangvikar, Zhibin Zhang, and Chris Navarrete. "Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices." *Palo Alto Networks: Unit 42*. 24 June 2020. https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/.

[24] "LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario." *CBC News*. 17 December 2019. https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577.

[25] Maham Abedi. "Capital One data breach: here's what Canadians need to know." *Global News*. 30 July 2019. https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/.

[26] Josh Fruhlinger. "Marriott data breach FAQ: How did it happen and what was the impact?" *CSO Online*. 12 February 2020. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

[27] Roberto Rocha and Jeff Yates. "Twitter Trolls Stoked Debates About Immigrants and Pipelines in Canada, Data Shows." *CBC News*. 12 February 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[28] Reis Thebault. "A woman's stalker used an app that allowed him to stop, start, and track her car." *The Washington Post*. 06 November 2019. https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/.

[29] "Tech Abuse and Empowerment Service." *Refuge*. Accessed 15 July 2020. https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/.

[30] "Cybersecurity Vulnerabilities Associated with Devices with Bluetooth Low Energy Chips." *Health Canada*. 11 March 2020. https://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-eng.php.

[31] "Canada's Critical Infrastructure." *Public Safety Canada*. 19 May 2020. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx.

[32] Andy Greenberg. "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid." *Wired*. 14 June 2019. https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[33] Andy Greenberg. "A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems." *Wired*. 20 November 2019. https://www.wired.com/story/iran-apt33-industrial-control-systems/.

[34] "Top 2019 Cyber Attacks on ICS." *Waterfall Security*. 19 December 2019. https://waterfall-security.com/top-2019-attacks-on-ics/.

[35] Joe Tidy. "How a Ransomware Attack Cost One Firm £45m." *BBC News*. 25 June 2019. https://www.bbc.com/news/business-48661152.

[36] Andy Greenberg. "Mysterious New Ransomware Targets Industrial Control Systems." *Wired*. 03 February 2020. https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Nathan Brubaker, et. al. "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families". *FireEye Threat Research*. 15 July 2020. https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.

[37] "EKANS Ransomware and ICS Operations." *Dragos*. 03 February 2020. https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[38] Ben Dooley and Hsako Ueno. "Honda Hackers May Have Used Tools Favored by Countries." *New York Times*. 12 June 2020. https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html.

[39] James Lewis. "Economic Impact of Cybercrime—No Slowing Down." *Center for Strategic and International Studies and McAfee*. February 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

[40] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://www.bankinfosecurity.com/whitepapers/2019-internet-security-threat-report-w-5357.

[41] "Q1 2020 Ransomeware Marketplace Report." *Coveware*. 29 April 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[42] Ryan Flanagan. "Canadian Insurance Company Lost Nearly US$1M in Ransomware Attack." *CTV News*. 30 January 2020. https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490.

[43] Ransomware Payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020. *Coveware*. 29 April 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[44] Catharine Tunney. "Ransomware Attack on Construction Company Raises Questions About Federal Contracts." *CBC News*. 26 January 2020. https://www.cbc.ca/news/politics/ransowmare-bird-construction-1.5434308; "Time's Up for Agromart Group and their Data Got Leaked by REvil Ransomware Operators." *Cyble, Inc.* 2 June 2020. https://cybleinc.com/2020/06/02/times-up-for-agromart-group-and-their-data-got-leaked-by-revil-ransomware-operators/.

[45] David Burke. "Hospitals 'Overwhelmed' by Cyberattacks Fuelled by Booming Black Market." *CBC*. 02 June 2020. https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422.

[46] "Alert: Cyber Threats to Canadian Health Organizations." *Canadian Centre for Cyber Security*. 20 March 2020. https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations.

[47] Catharine Tunney. "CSIS chief calls commercial espionage 'the greatest threat to our prosperity'." *CBC News*. 04 December 2018. https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407/.

[48] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *US Department of Justice*. 20 December 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[49] Dustin Volz. "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets." *The Wall Street Journal*. 05 March 2019. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800.

[50] "Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity." *Canadian Centre for Cyber Security*. 27 April 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity/.

[51] "Advisory: APT29 targets COVID-19 vaccine development." *National Cyber Security Centre*. 16 July 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

[52] "What do Cybercriminals do with the Data They Steal?" *Sysnet Global Solutions*. Accessed 10 July 2020. https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/.

[53] Scott Ikeda. "Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit." *CPO Magazine*. 08 January 2020. https://www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/.

[54] Danny Palmer. "Ransomware warning: Now attacks are stealing data as well as encrypting it." *ZDNet*. 14 July 2020. https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[55] "2020 Data Breach Investigations Report." *Verizon*. 02 June 2020. https://enterprise.verizon.com/resources/reports/dbir/.

[56] Bruce Sussman. "BEC Scam Costs Canadian City $500k." *SecureWorld*. 18 June 2019. https://www.secureworldexpo.com/industry-news/canada-bec-scam-example.

[57] "The Sprawling Reach of Complex Threats: 2019 Annual Security Roundup." *Trend Micro*. 25 February 2020. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats.

[58] "2019 Internet Crime Report." *Federal Bureau of Investigation*. 11 February 2020. https://pdf.ic3.gov/2019_IC3Report.pdf.

[59] C. Steven Baker. "Is That Email Really From "The Boss"? The Explosion of Business Email Compromise (BEC) Scams." *The Better Business Bureau*. September 2019. https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-explosion-of-bec-scams.pdf

[60] "Behind the 'From' Lines: Email Fraud on a Global Scale." *Agari Cyber Intelligence Division*. Accessed 15 August 2020. https://www.agari.com/insights/whitepapers/behind-the-from-lines/.

[61] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[62] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[63] Jin Chen, Tao Yan, Taojie Wang, and Zhanglin He. "Anatomy of FormJacking Attacks." *Palo Alto Networks, Unit 42*. 27 April 2020. https://unit42.paloaltonetworks.com/anatomy-of-formjacking-attacks/.

[64] Joseph Chen. "Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada." *Trend Micro*. 03 May 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[65] Aanand Krishnan. "Web scammers are using the COVID-19 crisis to attack your customers with Magecart and other client-side exploits." *Tala Security*. 09 June 2020. https://blog.talasecurity.io/web-scammers-are-using-the-covid-19-crisis-to-attack-your-customers-with-magecart-and-other-client-side-exploits/.

[66] Merna Emara. "Cybercrime Attacks on the Rise at North American Gas Stations, Warns Card Giant Visa." *National Post*. 17 December 2019. https://nationalpost.com/news/world/cybercrime-attacks-on-the-rise-at-north-american-gas-stations-warns-card-giant-visa.

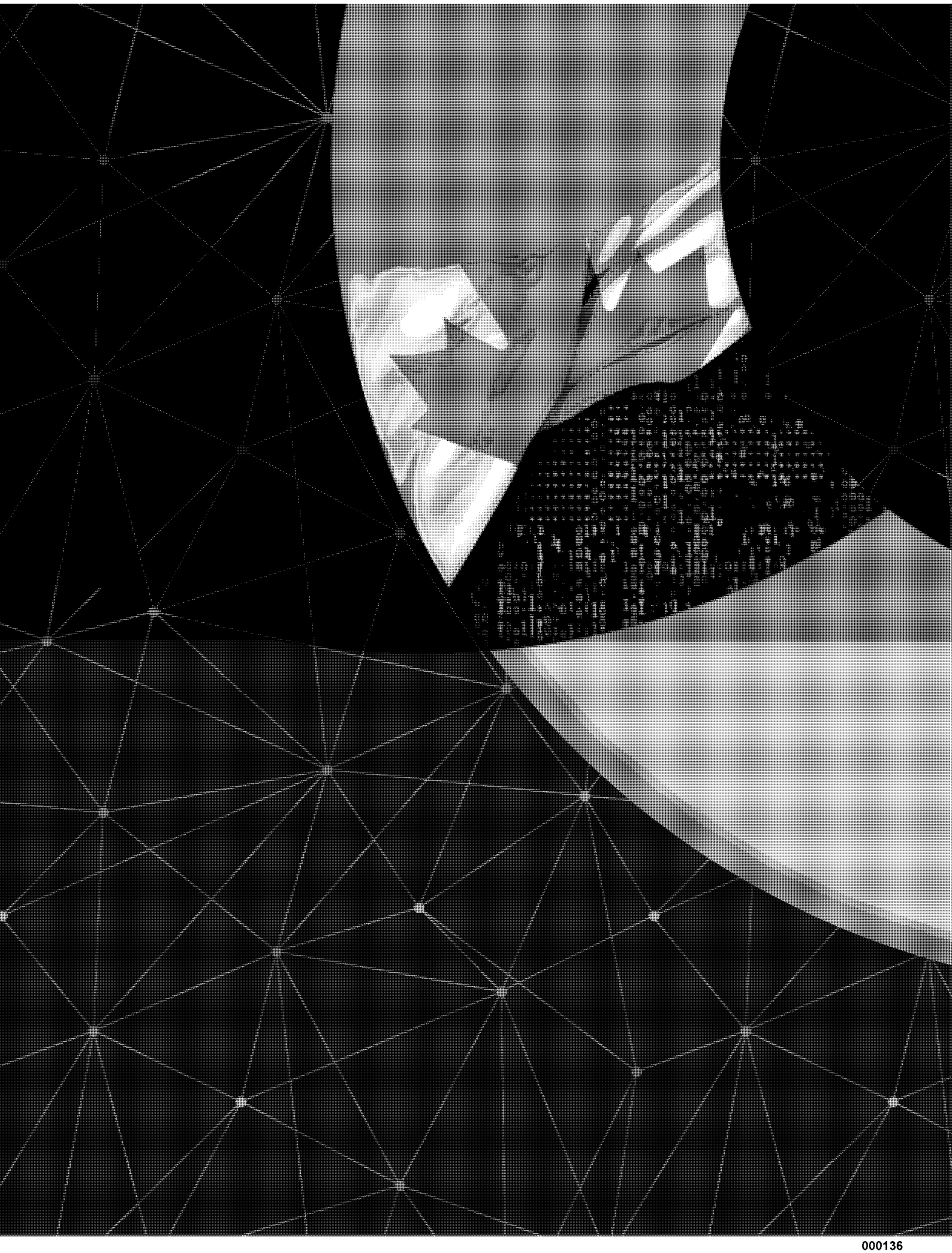
[67] A supply chain is defined as the system of organizations, people, technology, activities, information, and resources involved in moving a product or service from a supplier to a customer. See "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." *National Institute for Standards and Technology*. April 2015. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

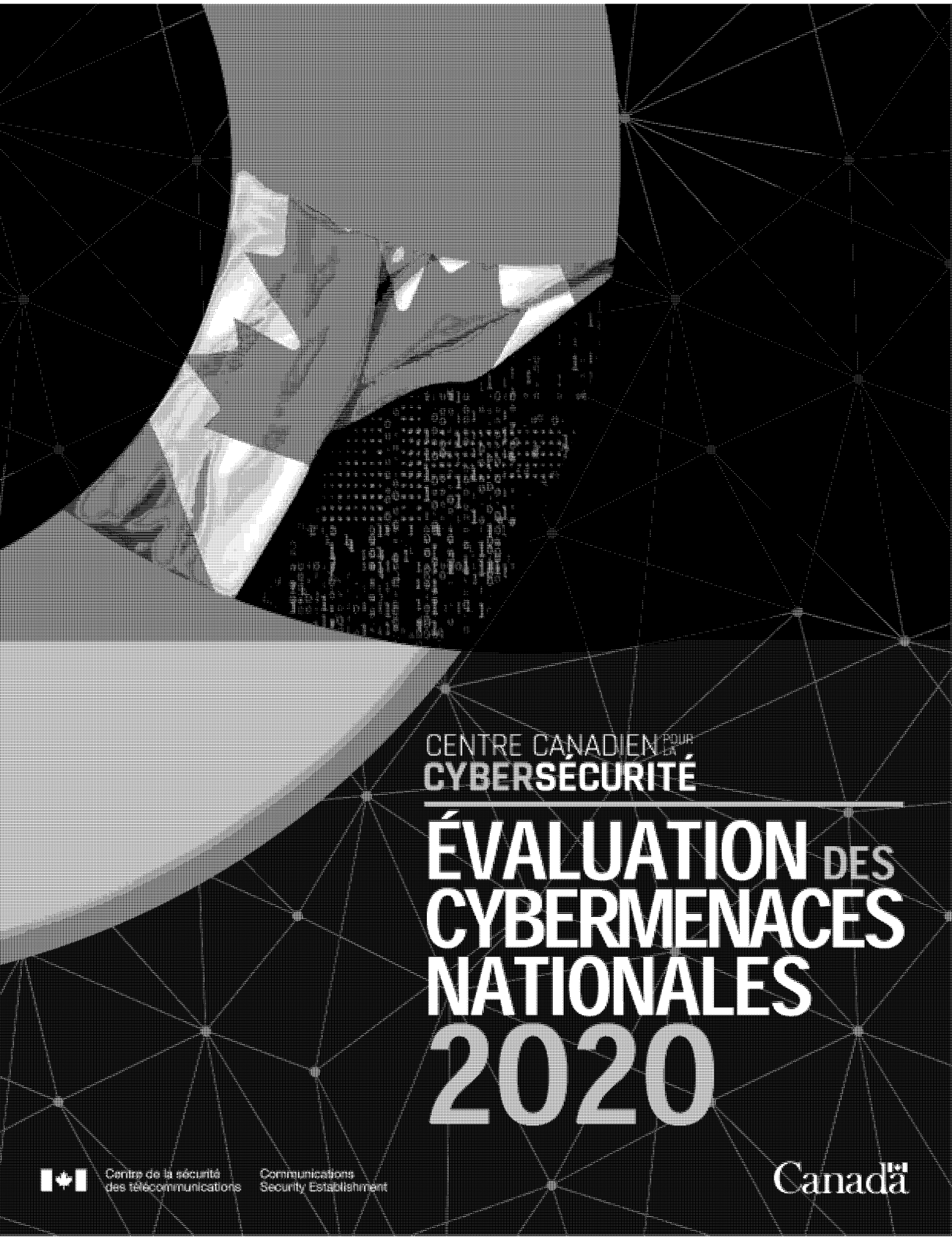
[68] Catalin Cimpanu. "FBI re-sends alert about supply chain attacks for the third time in three months." *ZDNet*. 31 March 2020. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/.

[69] Howard Solomon. "Canadian Organizations Among Victims of Global Attack on Healthcare-related Industries." *IT World*. 24 April 2018. https://www.itworldcanada.com/article/canadian-organizations-among-victims-of-global-attack-on-healthcare-related-industries/404475.

[70] Johannes B. Ullrich. "Kwampirs Targeted Attacks Involving Healthcare Sector." *SANS Internet Storm Center*. 31 March 2020. https://isc.sans.edu/forums/diary/Kwampirs+Targeted+Attacks+Involving+Healthcare+Sector/25968/?utm_medium=Social&utm_source=Twitter&utm_campaign=SANS+Central.

[71] Catalin Cimpanu. "GandCrab Ransomware Gang Infects Customers of Remote IT Support Firms." *ZDNet*. 14 February 2019. https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/; Catalin Cimpanu. "Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems." *ZDNet*. 20 June 2019. https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/; Catalin Cimpanu. "Ransomware Hits Hundreds of Dentist Offices in the US." *ZDNet*. 29 August 2019. https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.





CENTRE CANADIEN POUR CYBERSÉCURITÉ

ÉVALUATION DES CYBERMENACES NATIONALES 2020

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

À PROPOS DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (CCC) est l'autorité canadienne en matière de cybersécurité. Faisant partie du Centre de la sécurité des télécommunications (CST), le CCC est une organisation en plein essor qui jouit d'une riche histoire. Il regroupe sous un même toit des spécialistes en sécurité opérationnelle de l'ensemble du gouvernement du Canada. En phase avec la *Stratégie nationale de cybersécurité*, le CCC marque un tournant vers une approche plus unifiée à la cybersécurité au Canada.

Le CCC est formé d'une équipe d'experts en cybersécurité dignes de confiance, et son mandat clair et précis consiste à collaborer avec le gouvernement, le secteur privé et le milieu universitaire. Cette équipe, qui se compose de réalisateurs, de concepteurs, de développeurs, de chercheurs et de scientifiques, a pour rôle d'accroître la cybersécurité au Canada.

LE CCC CONTRIBUE À LA SÉCURITÉ DU CANADA ET DES CANADIENS DANS LE CYBERESPACE EN JOUANT LES RÔLES SUIVANTS :

- Il est une **source claire et fiable de renseignements pertinents sur la cybersécurité** pour les Canadiens, les entreprises canadiennes ainsi que les propriétaires et les exploitants d'infrastructures essentielles;
- Il offre des **avis et des conseils ciblés sur la cybersécurité** afin de protéger les plus importants cybersystèmes canadiens;
- Il travaille **en collaboration avec les gouvernements provinciaux et territoriaux, les administrations municipales et des partenaires du secteur privé** pour résoudre les défis les plus complexes du Canada en matière de cybermenace;
- Il développe et diffuse des **technologies et connaissances de cyberdéfense spécialisées**;
- Il **défend les cybersystèmes**, dont ceux du gouvernement du Canada, en élaborant et en déployant des outils et des technologies de cyberdéfense sophistiqués;
- Il agit à titre de **chef de file opérationnel du gouvernement lors d'incidents de cybersécurité** et tire parti de son expertise et de ses accès pour fournir de l'information opportune et utile à la gestion des incidents.

La cyberdéfense, c'est un sport d'équipe. L'avantage unique du CCC permet au Canada de résister plus efficacement aux cybermenaces et d'accroître sa résilience pendant et après des cyberincidents.

POUR EN SAVOIR PLUS À CE SUJET, VISITEZ LE CYBER.GC.CA OU SUIVEZ-NOUS SUR TWITTER @CENTRECYBER_CA

AVANT-PROPOS DU MINISTRE

La cybersécurité est l'un des enjeux les plus sérieux auxquels nous faisons face sur le plan de l'économie et de la sécurité nationale. Protéger le Canada et les Canadiens des cybermenaces est une responsabilité partagée et une affaire d'équipe. Je ne saurais trop insister sur l'importance de lire le présent rapport, tout particulièrement si vous pensez que la cybersécurité n'a rien à voir avec vous.

D'ailleurs, je tiens à remercier l'équipe du Centre pour la cybersécurité pour cette évaluation fort opportune. En partageant ses connaissances, elle s'assure que les décideurs politiques, les chefs d'entreprise et les citoyens canadiens ont l'information nécessaire pour contrer ces menaces.

Nous savons que les Canadiens sont parmi les peuples les plus connectés au monde et la pandémie de la COVID-19 n'a fait qu'accroître cette dépendance à Internet. Comme on peut le voir régulièrement dans l'actualité, les cyberattaquants trouvent sans cesse des moyens plus sophistiqués d'exploiter notre connectivité.

Les cybermenaces mettent à risque la vie privée, la stabilité financière et la sécurité personnelle des Canadiens, ainsi que la rentabilité des entreprises au pays. Le préfixe « cyber » ne reflète en fait que l'approche adoptée pour mener de telles activités.

Tirant avantage de l'expertise de pointe du Canada en la matière, l'approche unifiée du Centre pour la cybersécurité offre aux Canadiens l'assurance que le gouvernement est prêt à s'attaquer aux enjeux qui nous guettent sur le plan de la cybersécurité.

Les principales constatations soulevées dans le présent rapport du Centre pour la cybersécurité nous rappellent à quel point il est important de ne pas baisser notre garde.

On constate une recrudescence des cybermenaces, alors que les cybercriminels sophistiqués vendent leurs outils et leurs services en ligne par l'entremise de marchés illégaux.

Les cyberprogrammes parrainés par des États sondent nos infrastructures essentielles à la recherche de vulnérabilités.

Il est de plus en plus courant de voir les nations étrangères chercher à influencer les débats publics au moyen des médias sociaux.

De fait, Internet se trouve à la croisée des chemins, puisque des pays comme la Chine et la Russie s'efforcent de changer la façon dont nous régissons le cyberespace et d'en faire un outil susceptible de conférer à l'État un pouvoir de censure, de surveillance et de contrôle.

Nous continuerons de collaborer avec nos partenaires des secteurs privé et public, ainsi qu'avec les citoyens canadiens, en vue de créer un cyberespace fort et résilient dans l'ensemble du Canada.

L'honorable Harjit Sajjan
Ministre de la Défense nationale

MESSAGE DU DIRIGEANT PRINCIPAL DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Deux années se sont écoulées depuis la publication de la première Évaluation des cybermenaces nationales 2018 du Canada, et au cours de cette période, beaucoup de ce qui a été annoncé s'est concrétisé. L'*Évaluation des cybermenaces nationales 2020* arrive à un moment où les Canadiens et l'économie canadienne ont de plus en plus tendance à réorienter leurs activités vers les services en ligne. Cette transition s'est accélérée depuis l'arrivée de la COVID-19.

La pandémie de COVID-19 illustre bien jusqu'à quel point l'économie canadienne dépend de l'infrastructure numérique. Face à la hausse subite du nombre de Canadiens travaillant à la maison, il est essentiel de protéger les cyberinfrastructures, les infrastructures de télécommunications, le matériel, les logiciels et les chaînes d'approvisionnement qui les prennent en charge, pour assurer la sécurité nationale et la prospérité économique du Canada. Ces aspects sont au cœur de nos activités quotidiennes et, pour la majorité des Canadiens, l'infrastructure numérique à la base de notre société est souvent hors de vue ou cachée.

Le présent document ne se veut pas un examen de l'*Évaluation des cybermenaces nationales* de 2018. Certaines prévisions se sont révélées exactes, d'autres se sont réalisées à des rythmes différents. On dit qu'avec le recul, tout devient plus clair. En 2018, j'avais mis au défi les équipes d'évaluation, comme je l'ai fait encore cette année, de faire preuve d'audace et d'y aller de prévisions. Seul l'avenir nous dira si ces dernières sont exactes. Elles s'appuient sur toute l'expertise du CST et ses connaissances en matière de cybersécurité tant au Canada qu'ailleurs dans le monde, et mettent à profit toutes les sources d'information classifiée et librement disponible.

L'*Évaluation des cybermenaces nationales* est à la base d'un grand nombre des activités du Centre canadien pour la cybersécurité (CCC). Son objectif est d'établir nos priorités. Nous travaillons à atténuer les menaces décrites dans le présent rapport et à accroître la cybersécurité de base dans l'ensemble du Canada. Mais le CCC ne saurait faire cavalier seul. Un bon exemple de cet esprit de collaboration est le partenariat conclu avec l'Autorité canadienne pour les enregistrements Internet (ACEI) et le lancement du service Bouclier canadien. L'utilisation de ce service offert gratuitement par l'ACEI à tous les Canadiens permet de réduire directement l'incidence et la portée de la cybercriminalité qui seraient liées, par exemple, à un rançongiciel. En bref, il s'agit d'une réponse directe à l'énoncé que l'on retrouve dans l'évaluation de 2018 selon lequel la menace la plus susceptible d'avoir une incidence sur les Canadiens est la cybercriminalité.

Mais ces deux dernières années ont aussi démontré que ce qui compte réellement est de faire le nécessaire sur le plan de la cybersécurité. La grande majorité des cyberincidents qui se sont produits au Canada résultaient du non-respect des pratiques de base en matière de cybersécurité. Les Canadiens peuvent compter sur les étapes simples, réalistes et faciles à réaliser, qui sont proposées par la campagne du site Pensezcybersecurite.gc.ca pour accroître leur sécurité. Si vous êtes un organisme canadien à but non lucratif, une entreprise canadienne de toutes tailles ou un organisme faisant partie d'un autre ordre du gouvernement, vous trouverez de l'information sur le site cyber.gc.ca. Chacun doit faire sa part pour rendre le Canada plus sécuritaire.

J'espère que l'*Évaluation des cybermenaces nationales* de 2020 vous sera utile et qu'elle incitera chaque Canadien à entreprendre ne serait-ce qu'une initiative pour renforcer sa sécurité en ligne. Chaque étape franchie est un pas de plus vers notre objectif d'assurer la sécurité numérique du Canada.

Scott Jones
Dirigeant principal, Centre canadien pour la cybersécurité

www.cyber.gc.ca

RÉSUMÉ

Les Canadiens et les entreprises canadiennes dépendent de plus en plus d'Internet pour vaquer à leurs activités quotidiennes. Dans le contexte de la COVID-19, cette tendance s'est accélérée pour permettre aux Canadiens de travailler, de magasiner et de socialiser à distance conformément aux directives de distanciation physique émises par la santé publique. Cependant, alors que les dispositifs, l'information et les activités se tournent vers Internet, ils deviennent également vulnérables face aux auteurs de cybermenace.

Les auteurs de cybermenace représentent un risque pour l'économie canadienne en raison des coûts élevés que doivent subir les particuliers et les entreprises, notamment lors du vol de propriété intellectuelle et de renseignements exclusifs. Ils mettent en péril la vie privée des Canadiens en volant leurs renseignements personnels, ce qui favorise la criminalité, dont le vol d'identité et la fraude financière. Alors que les infrastructures matérielles et les processus restent liés à Internet, les cybermenaces présentent de plus en plus un danger sur le plan du fonctionnement de l'équipement et de la sécurité des Canadiens.

FAITS SAILLANTS

- **Le nombre d'auteurs de cybermenace est en hausse et ceux-ci deviennent de plus en plus sophistiqués.** La vente commerciale d'outils liés à la cybercriminalité, à laquelle s'ajoute un bassin mondial d'experts en la matière, a entraîné une hausse du nombre d'auteurs de cybermenace et donné lieu à des attaques plus sophistiquées. Les marchés en ligne servant à la vente d'outils et de services illicites ont également permis aux cybercriminels de mener des activités plus complexes et sophistiquées.

- **La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes.** Nous estimons qu'au cours des deux prochaines années, les Canadiens et les entreprises canadiennes devraient continuer d'être visés par la fraude en ligne et des tentatives de vol de données personnelles, financières et commerciales.

- **Nous considérons que les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles.** Comme ces derniers ne peuvent pas se permettre de subir des perturbations importantes, ils sont prêts à verser jusqu'à plusieurs millions de dollars pour rétablir leurs opérations. Il est probable que beaucoup de victimes canadiennes continueront de consentir à payer les rançons en raison des coûts élevés liés aux pertes commerciales et à la reconstruction de leurs réseaux, ainsi qu'aux conséquences potentiellement dévastatrices qui pourraient résulter advenant un refus.

- **Bien que la cybercriminalité représente la menace la plus importante, les programmes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent les plus graves menaces stratégiques pour le Canada.** Les cybermenaces parrainées par des États sont habituellement les menaces les plus sophistiquées auxquelles sont confrontés les Canadiens et les entreprises canadiennes.

- **Il est fort probable que des auteurs de cybermenace parrainés par des États cherchent à développer des moyens pour perturber les infrastructures essentielles du Canada, comme l'approvisionnement en électricité, pour atteindre leurs buts.** Nous croyons toutefois qu'il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Néanmoins, les auteurs de cybermenace pourraient cibler des entreprises canadiennes essentielles dans l'objectif de recueillir des données, de se prépositionner en vue d'activités ultérieures, ou de les intimider.

- **Les auteurs de cybermenace continueront probablement de mener des activités d'espionnage industriel contre les entreprises, le milieu universitaire et les gouvernements du Canada afin de voler la propriété intellectuelle et des renseignements canadiens de nature exclusive.** Nous estimons que ces auteurs malveillants continueront à tenter de voler la propriété intellectuelle portant sur la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés. La menace de cyberespionnage est certainement beaucoup plus grande pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

- **Les campagnes d'influence étrangère en ligne sont pratique courante et ne se limitent pas à des événements politiques importants, comme des élections.** Elles font maintenant partie de la nouvelle normalité, et les adversaires tentent non seulement d'influencer des événements à l'échelle nationale, mais ils veulent aussi avoir un impact sur les débats publics qui se tiennent sur la scène internationale. Nous estimons que, comparativement à d'autres pays, les Canadiens ne présentent pas une cible prioritaire en ce qui a trait à l'influence étrangère en ligne. Il faut toutefois noter qu'au Canada, l'écosystème des médias est étroitement lié à celui des États-Unis et d'autres alliés. Cela signifie que lorsque les populations de ces derniers sont ciblées, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne.

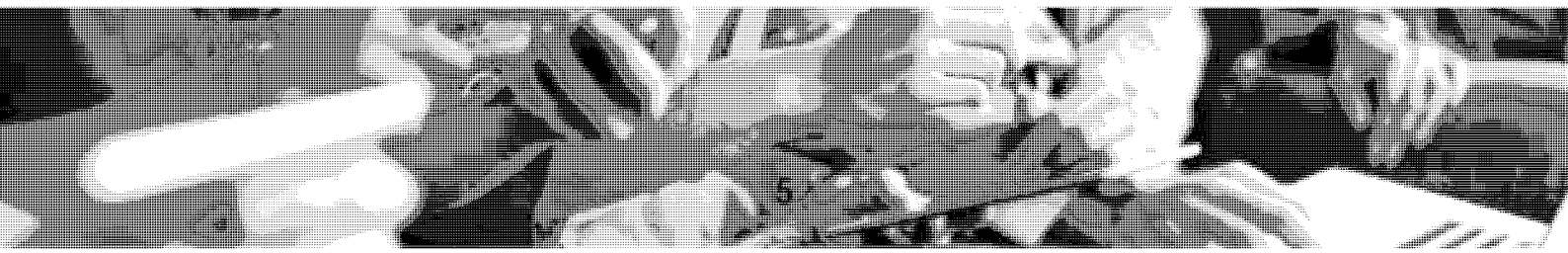


TABLE DES MATIÈRES

À PROPOS DU PRÉSENT DOCUMENT

Le présent document fait état des cybermenaces qui visent les citoyens et les entreprises du Canada. Il constitue une mise à jour de l'*Évaluation des cybermenaces nationales 2018*, ainsi qu'une analyse des années intermédiaires et des prévisions d'ici 2022. Nous vous recommandons de lire la présente évaluation et de consulter l'*Introduction à l'environnement de cybermenace*, qui a également été mise à jour. Cette introduction donne un aperçu général des auteurs de cybermenace, de leurs motivations et des outils à leur disposition. Elle comprend de plus une annexe indiquant les principales techniques et les principaux outils qui ont été mentionnés dans la présente.

Conformément à l'optique de la *Stratégie nationale de cybersécurité*, nous avons préparé ce document pour aider à façonner et à soutenir la résilience du Canada en matière de cybersécurité. Ce n'est qu'en travaillant ensemble (le gouvernement, le secteur privé et les particuliers) que nous pourrons assurer la résilience du Canada face aux cybermenaces.

RESTRICTIONS

L'objectif de la présente évaluation n'est pas de fournir une liste exhaustive des activités de cybermenace ciblant le Canada ou des conseils en matière d'atténuation. Elle a plutôt pour but de décrire et d'évaluer les menaces visant le Canada. Cette évaluation cherche à comprendre la nature et le contexte de cybermenace actuel, ainsi que la façon dont les activités de ce type peuvent toucher les citoyens et les organismes canadiens. Il est également possible de trouver des conseils généraux sur le site Web du Centre canadien pour la cybersécurité, notamment dans les documents liés à la campagne Pensez cybersécurité.

SOURCES

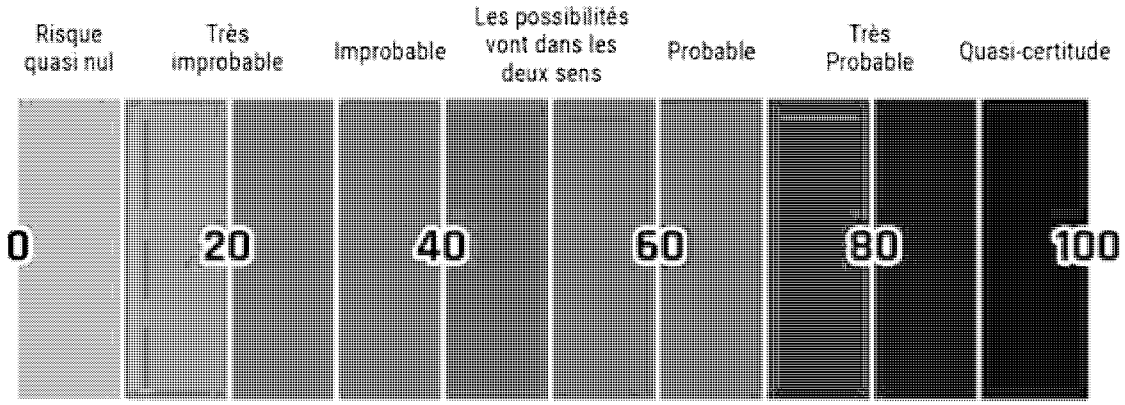
Les jugements formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du CCC en matière de cybersécurité. Le rôle que joue le CCC dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, ce qui a contribué à la présente évaluation. Le mandat de renseignement étranger du CST lui procure de précieuses informations sur le comportement des adversaires dans le cyberespace. Bien qu'il soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses jugements.

PROCESSUS D'ÉVALUATION

Les évaluations de cybermenace effectuées sont basées sur un processus d'analyse qui comprend l'évaluation de la qualité des renseignements disponibles, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes comme « on considère que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « susceptible », « probable » et « très probable » pour exprimer les probabilités.

La présente évaluation des menaces est basée sur des renseignements disponibles en date du 20 octobre 2020.

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



UN CONTEXTE DES CYBERMENACES EN ÉVOLUTION

L'*Évaluation des cybermenaces nationales 2018* décrivait les cybermenaces auxquelles ont fait face les citoyens, les entreprises et les fournisseurs d'infrastructures essentielles du Canada. Elle annonçait également comment ces menaces allaient évoluer au cours des prochaines années. Beaucoup de ces jugements demeurent pertinents. La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens. Il y a aussi les auteurs de cybermenace parrainés par des États qui continuent de se livrer au cyberespionnage contre des organismes canadiens, notamment les entreprises et les infrastructures essentielles; et il ne faut pas oublier les auteurs de cybermenace qui continuent d'adapter leurs techniques et d'adopter des méthodes plus avancées. Or, les menaces qui pèsent sur les Canadiens ont elles aussi évolué au même rythme que les façons dont ils utilisent la technologie et Internet.

Internet est un outil indispensable pour les gens à travers le monde et pour les Canadiens. Les changements qui ont dû être apportés en mars 2020 en raison de la pandémie de COVID-19 ont rapidement bouleversé le portrait de la cybersécurité alors que plus de Canadiens doivent travailler, magasiner et socialiser à distance. Nous prévoyons que cette tendance se poursuivra et que plus de facettes de la vie économique, sociale et politique des Canadiens passeront par Internet, ce qui les exposera à des cybermenaces qui ne cessent d'évoluer pour tirer avantage de l'importance accrue d'Internet et des technologies connexes.

Afin de bien comprendre le reste de l'évaluation, nous avons relevé dans la prochaine section cinq tendances qui guideront l'évolution du contexte des cybermenaces.

LA TECHNOLOGIE CHANGE LA SOCIÉTÉ ET MODIFIE LE CONTEXTE DES CYBERMENACES

Les changements technologiques amènent des changements sociaux

Les Canadiens dépendent de plus en plus d'Internet. Un nombre grandissant d'activités quotidiennes importantes se font maintenant en ligne pour des raisons de commodité et d'efficacité. On peut penser ici à tout ce qui touche les transactions bancaires, les services gouvernementaux, les services de santé, le commerce et l'éducation. Dans le contexte de la COVID-19, cette tendance s'est accélérée pour permettre aux Canadiens de travailler, de magasiner et de socialiser à distance conformément aux directives de distanciation physique émises par la santé publique. Ces changements sont engendrés par des technologies émergentes et arrivant à maturité, qui continuent de créer de nouveaux moyens pour utiliser Internet. Ces technologies permettent une meilleure qualité de vie et changent la façon dont les gens et les organismes interagissent.

Des technologies comme l'intelligence artificielle (IA), l'Internet des objets (IdO), l'Internet des objets industriel (IIoT pour *Industrial Internet of Things*) et l'infonuagique soutiennent une vaste gamme d'activités personnelles, commerciales et industrielles. Au cours des deux prochaines années, l'avancement de ces technologies et les progrès réalisés dans d'autres technologies de l'information, comme le déploiement du réseau 5G, changeront les pratiques commerciales des Canadiens, leurs façons d'exploiter des établissements industriels, d'acheter et d'obtenir des produits de consommation, de recevoir des soins médicaux, et plus encore. Les Canadiens seront en mesure de constater des changements apportés dans d'autres aspects de leur vie, notamment l'aménagement des villes et des moyens de transport, ainsi que le déroulement des élections et des processus démocratiques.

Le contexte des cybermenaces

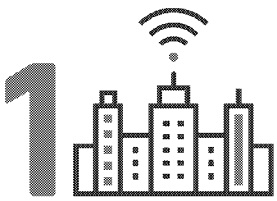
Alors que les dispositifs, l'information et les activités prisés par les Canadiens et les entreprises canadiennes se tournent vers Internet, ils s'exposent également aux cybermenaces. Les auteurs de cybermenace, plus particulièrement les cybercriminels et les auteurs parrainés par des États, continuent d'adapter leurs activités afin de trouver l'information importante pour les Canadiens. Leur objectif est de s'approprier de cette information, de la détenir en vue d'une demande de rançon ou de la détruire.

On considère que les cybercriminels, qui sont motivés par un gain financier, représentent presque assurément la plus grande cybermenace pour les Canadiens. Ils se livrent à la majorité des activités de cybermenace contre les Canadiens, dont les attaques par rançongiciel, le vol de données personnelles, financières et confidentielles, et les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*). Comme nous l'abordons un peu plus dans la présente, les marchés illégaux des produits et services liés à la cybercriminalité donnent aux cybercriminels accès à des outils plus sophistiqués.

Or, les moyens les plus sophistiqués appartiennent aux auteurs de cybermenace parrainés par des États qui sont motivés par des visées économiques, idéologiques et géopolitiques. Ils comptent parmi leurs activités le cyberespionnage, le vol de propriété intellectuelle, les campagnes d'influence en ligne et les cyberattaques perturbatrices. Nous sommes presque assurés que les programmes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent les plus graves cybermenaces pour les Canadiens et les entreprises canadiennes. Toutefois, beaucoup d'autres États développent rapidement leurs propres programmes et profitent de divers marchés légaux et illégaux pour se procurer des produits et services qu'ils pourront ensuite utiliser dans le cadre de leurs activités de cybermenace.

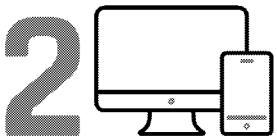
Les activités des hacktivistes ou des amateurs de sensations fortes posent une menace moins fréquente et moins sophistiquée pour les Canadiens. En règle générale, les activités des hacktivistes et des amateurs de sensations fortes sont moins répandues que les autres types d'activités. De plus, ces auteurs de cybermenace ont souvent moins de ressources à consacrer à leurs activités, ce qui limite la sophistication de leurs opérations. Les hacktivistes ont toutefois mené des cyberactivités d'importance majeure en 2020. Un des incidents les concernant ciblait principalement des victimes américaines, mais a quand même eu une incidence sur des organismes au Canada, alors que des données appartenant à 38 services de police canadiens ont été exposées.[1]

Nous présentons ci-dessous cinq tendances qui guideront l'évolution du contexte des cybermenaces et les activités de cybermenace.



1 LA SÉCURITÉ PHYSIQUE DES CANADIENS EST MENACÉE

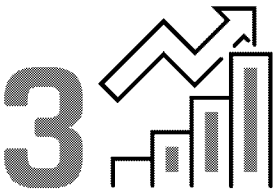
La sécurité des Canadiens dépend des infrastructures essentielles (comme l'énergie ou la gestion de l'eau), ainsi que de biens de consommation et de produits médicaux (voiture, système de sécurité à domicile, stimulateur cardiaque et autres) qui sont, dans plusieurs cas, contrôlés par des dispositifs informatiques implantés à même le corps. On remarque de plus en plus que ces dispositifs informatiques sont branchés à Internet par leurs fabricants, parfois à l'insu des consommateurs. Cette façon de procéder permet d'activer de nouvelles fonctions ou de fournir des données à des tiers. Une fois connectés, ces produits représentent toutefois une cybermenace. Assurer leur sécurité nécessite, au fil du temps, des investissements que les fabricants et les propriétaires pourraient avoir de la difficulté à maintenir. Un aspect important de cette tendance est la technologie opérationnelle (TO) qui, en termes génériques, fait référence à la technologie utilisée pour contrôler les processus physiques comme l'ouverture de barrage, le fonctionnement d'une chaudière, la transmission d'électricité et l'exploitation des pipelines. Contrairement à la technologie de l'information (TI) qui englobe le matériel et les logiciels que l'on trouve dans la plupart des maisons et des entreprises, la technologie opérationnelle a été relativement à l'abri des activités de cybermenace parce qu'elle n'a pas été initialement conçue pour être connectée à Internet. Or, les fabricants convergent maintenant vers la TI et la TO. Ces changements ont pour but d'accroître l'efficacité et de soutenir une planification à long terme, mais ils augmentent également le risque de voir les systèmes de TO être touchés par des activités de cybermenace. Une enquête effectuée en 2019 a démontré que 68 % des fabricants envisageaient d'accroître leurs investissements dans des solutions de convergence vers les TI et TO pour leurs organismes au cours des deux prochaines années.[2] Il est fort probable que les menaces les plus pressantes à la sécurité physique des Canadiens visent la TO et les infrastructures essentielles. Cependant, cibler des petites villes et des dispositifs de l'IdO, comme un dispositif médical personnel ou un véhicule connecté à Internet, pourrait éventuellement mettre les Canadiens en danger.



2 LA VALEUR ÉCONOMIQUE EST MENACÉE

Comme il est indiqué dans l'évaluation de 2018, les auteurs de cybermenace parrainés par des États et les cybercriminels continuent de soutirer des sommes importantes aux Canadiens et aux entreprises canadiennes et de mettre en péril l'économie. Les cybercriminels fraudent les citoyens et les entreprises et leur soutirent de l'argent au moyen de rançongiciels. Les auteurs de cybermenace parrainés par des États, quant à eux, volent plutôt la propriété intellectuelle et des renseignements de nature exclusive. En outre, de plus en plus de Canadiens effectuent leurs transactions financières en ligne, ce qui en fait des proies intéressantes pour les cybercriminels. En 2019, 94 % des Canadiens avaient un accès Internet à domicile (une hausse comparativement à 79 % en 2010), et 71 % des Canadiens utilisaient des services bancaires en ligne (le pourcentage atteignait 67 % en 2010).[3]

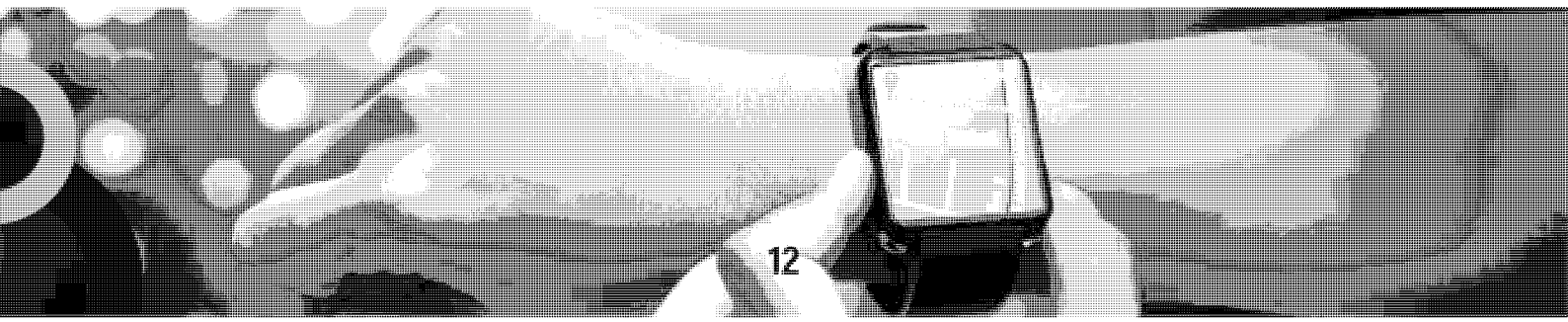
En raison des restrictions liées à la pandémie de COVID-19, les Canadiens se sont tournés rapidement et en grand nombre vers le télétravail. Ils accèdent à la propriété intellectuelle et à d'autres données sensibles en utilisant des dispositifs personnels et des réseaux Wi-Fi peu sécurisés comparativement à l'infrastructure de TI de leur entreprise. La protection de la propriété intellectuelle est cruciale pour la productivité et la compétitivité des entreprises canadiennes, et elle est vitale pour assurer la croissance économique du Canada ainsi que la défense nationale. Certains pays continuent d'avoir recours à des programmes avancés de cyberespionnage pour obtenir des avantages déloyaux sur les marchés mondiaux et améliorer leur technologie militaire. Le cyberespionnage industriel contre des entreprises est répandu dans de nombreux secteurs, dont ceux de l'aviation, de la technologie, de l'intelligence artificielle et de l'industrie biopharmaceutique.[4]

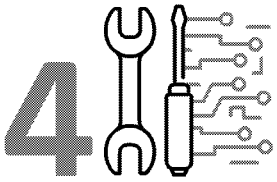


3 PLUS NOMBREUSES SONT LES DONNÉES RECUEILLIES PLUS GRAND EST LE RISQUE D'ENTRAVE À LA VIE PRIVÉE

Les Canadiens génèrent une incroyable quantité de données concernant les endroits où ils vont, leurs habitudes d'achat, leur mode de vie et leur santé lorsqu'ils utilisent leurs téléphones, ordinateurs ou services bancaires en ligne. C'est aussi le cas lorsqu'ils magasinent en ligne, portent des montres intelligentes et des moniteurs d'activité physique, arment leur système de sécurité à domicile ou contrôlent leur niveau d'insuline au moyen de dispositifs médicaux intelligents. Alors que les Canadiens génèrent, stockent et partagent de plus en plus de renseignements personnels en ligne, ces données sont plus susceptibles d'être la cible d'auteurs de cybermenace si les entreprises ou les gouvernements étrangers qui les recueillent sont victimes d'une atteinte à la sécurité ou les utilisent de façon abusive. Le nombre croissant de dispositifs connectés à Internet s'ajoute à la quantité de données recueillies sur les Canadiens. Le Commissariat à la protection de la vie privée du Canada (CPVP) a enregistré pas moins de 680 atteintes à la protection des données, qui ont touché 28 millions de Canadiens au cours de l'exercice s'étant terminé le 1er novembre 2019.[5]

Pendant ce temps, les progrès réalisés par la science des données font en sorte qu'il est plus difficile d'assurer l'anonymat et la confidentialité des données. Ces progrès technologiques permettent d'associer des renseignements qui étaient auparavant anonymes à d'autres ensembles de données et de les désanonymiser. La confidentialité des données est un enjeu important pour les Canadiens. Selon une étude commandée par le CPVP, 92 % des Canadiens ont soulevé des inquiétudes concernant la protection de leur vie privée, et 37 % se sont dits très préoccupés.[6]





DES COMPÉTENCES ET DES OUTILS AVANCÉS ACCESSIBLES À UN PLUS GRAND NOMBRE D'AUTEURS DE MENACE

La croissance du marché commercial des outils destinés aux activités de cybermenace et des services d'experts en la matière

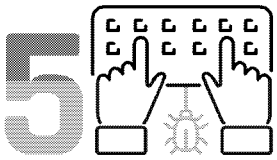
La vente commerciale d'outils liés à la cybercriminalité, à laquelle s'ajoute un bassin mondial d'experts en la matière, a entraîné une hausse du nombre d'auteurs de menace et donné lieu à une plus grande sophistication de leurs activités, ce qui complique le processus de reconnaissance, d'attribution et de défense contre les activités de cybermenace. On a remarqué sur ces marchés qu'il faut moins de temps à un État pour mettre en place un programme d'activités de cybermenace, et qu'un plus grand nombre d'États sont dotés de tels programmes. Depuis 2005, le Council on Foreign Relations tient une liste de plus en plus longue de pays soupçonnés de parrainer des activités malveillantes. La liste compte actuellement 33 pays.[7]

On s'attend à ce que la croissance du marché mondial des produits et services liés à la cybercriminalité passe d'environ 204 milliards $ CA en 2018 à 334 milliards $ CA en 2023.[8] Dans le but de développer rapidement leurs programmes nationaux, les auteurs de cybermenace parrainés par des États recrutent des expatriés qualifiés en leur offrant des salaires avantageux. Cela représente un changement important par rapport à l'époque où les États devaient développer leur propre bassin d'experts en la matière.

Un écosystème de cybercriminalité en plein essor

Au vaste marché commercial légitime s'ajoute un marché illégitime offrant des outils et des services liés à la cybercriminalité. De nombreux marchés en ligne autorisent la vente d'outils et de services spécialisés à des acheteurs qui s'en servent ensuite à des fins malveillantes, comme la défiguration de sites Web, l'espionnage, les attaques par DDoS et les attaques par rançongiciel. L'achat de ces outils et services permet aux cybercriminels de réduire considérablement leur temps de préparation et d'utiliser de meilleurs outils.

L'évolution de la cryptomonnaie a facilité les activités des cybercriminels et des États qui s'en servent pour échanger et blanchir de l'argent en préservant mieux leur anonymat. Si les cybercriminels n'avaient pas accès à la cryptomonnaie, les coûts associés à certains cybercrimes seraient prohibitifs. Des lois sur le blanchiment d'argent ont été adoptées dans beaucoup de pays pour contrer la cybercriminalité. Toutefois, le succès des cybercriminels est en partie attribuable aux lois trop clémentes ou inexistantes d'autorités gouvernementales partout dans le monde, ainsi qu'à l'application qui est faite de ces lois. Par exemple, en Russie, en Chine et en Iran, il est peu probable que des cybercriminels soient poursuivis pour avoir mené des activités de cybermenace motivées par un intérêt financier contre des cibles à l'extérieur du pays.[9]



INTERNET À LA CROISÉE DES CHEMINS

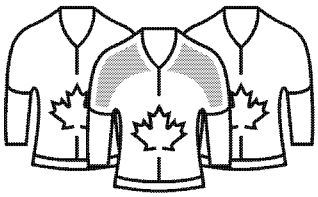
Gouvernance d'Internet

Beaucoup d'États exercent une forte pression pour changer l'approche reconnue à l'égard de la gouvernance d'Internet et suggèrent de passer d'une approche plurilatérale à une approche de souveraineté étatique. Ils considèrent les idées et l'information en termes de stabilité et de sécurité nationale, et ils veulent qu'Internet puisse leur permettre de surveiller leurs citoyens et de censurer l'information. Certains de ces régimes utilisent Internet pour réprimer les protestations, arrêter les dissidents, alimenter la désinformation et surveiller les citoyens.[10] La Chine et la Russie, qui sont des leaders du modèle de gouvernance fondée sur la souveraineté étatique, continuent de faire valoir leurs intérêts sur la scène internationale auprès d'agences comme l'Union internationale des télécommunications (UIT) et d'autres organisations des Nations Unies, en déposant des propositions politiques et relatives aux normes techniques. Ces dernières peuvent avoir des répercussions exceptionnelles et concrètes, comme le démontre la proposition du nouveau protocole Internet formulée par la Chine et les entreprises de télécommunications chinoises. Selon elles, le nouveau protocole pourrait transformer radicalement le fonctionnement d'Internet.[11] En plus d'offrir certains avantages sur le plan de la cybersécurité, ce nouveau protocole Internet conférerait à l'État un important pouvoir de censure, de surveillance et de contrôle.[12]

Historiquement, l'approche préconisée en ce qui a trait à la gouvernance d'Internet est l'approche plurilatérale adoptée par le Canada et d'autres pays aux vues similaires. Cette approche demande une grande participation de la part des gouvernements, des industries, de la société civile et du milieu universitaire, qui se réunissent pour établir des lignes directrices techniques et de politiques. Elle considère Internet comme un outil de développement global qui doit offrir un juste équilibre entre, d'une part, l'accès universel et l'interopérabilité et, d'autre part, la vie privée et la sécurité.

Influence étrangère en ligne

Comme nous l'avons indiqué dans notre *Évaluation des cybermenaces contre le processus démocratique du Canada*, les adversaires utilisent l'influence en ligne pour servir leurs intérêts fondamentaux, à savoir la sécurité nationale, la prospérité économique et leurs visées idéologiques. Les campagnes d'influence étrangère en ligne font maintenant partie de la nouvelle normalité et les adversaires tentent d'influencer des événements à l'échelle nationale (comme les élections) et d'avoir un impact sur les débats publics qui se tiennent sur la scène internationale. Un engagement démocratique en ligne fait appel à un Internet juste et transparent, à l'abri des manipulations des acteurs étrangers. De plus en plus d'États ont développé des cyberoutils qu'ils utilisent pour mener des activités d'influence en ligne à grande échelle. Ils profitent des médias sociaux, de publicités légitimes et d'outils d'échange d'information pour atteindre un large public et rendre leurs messages plus efficaces. La technologie d'hypertrucage, qui permet la création réaliste de vidéos et d'événements, ajoute un facteur d'incertitude et de confusion auprès des groupes ciblés par les campagnes de désinformation. Ce procédé de manipulation audiovisuelle s'est rapidement développé en raison de la forte augmentation de la demande pour diverses applications capables de changer les visages, des produits permettant de produire une vidéo d'une personne à partir de rien[13] et un logiciel d'hypertrucage audio capable de cloner des voix humaines.[14]



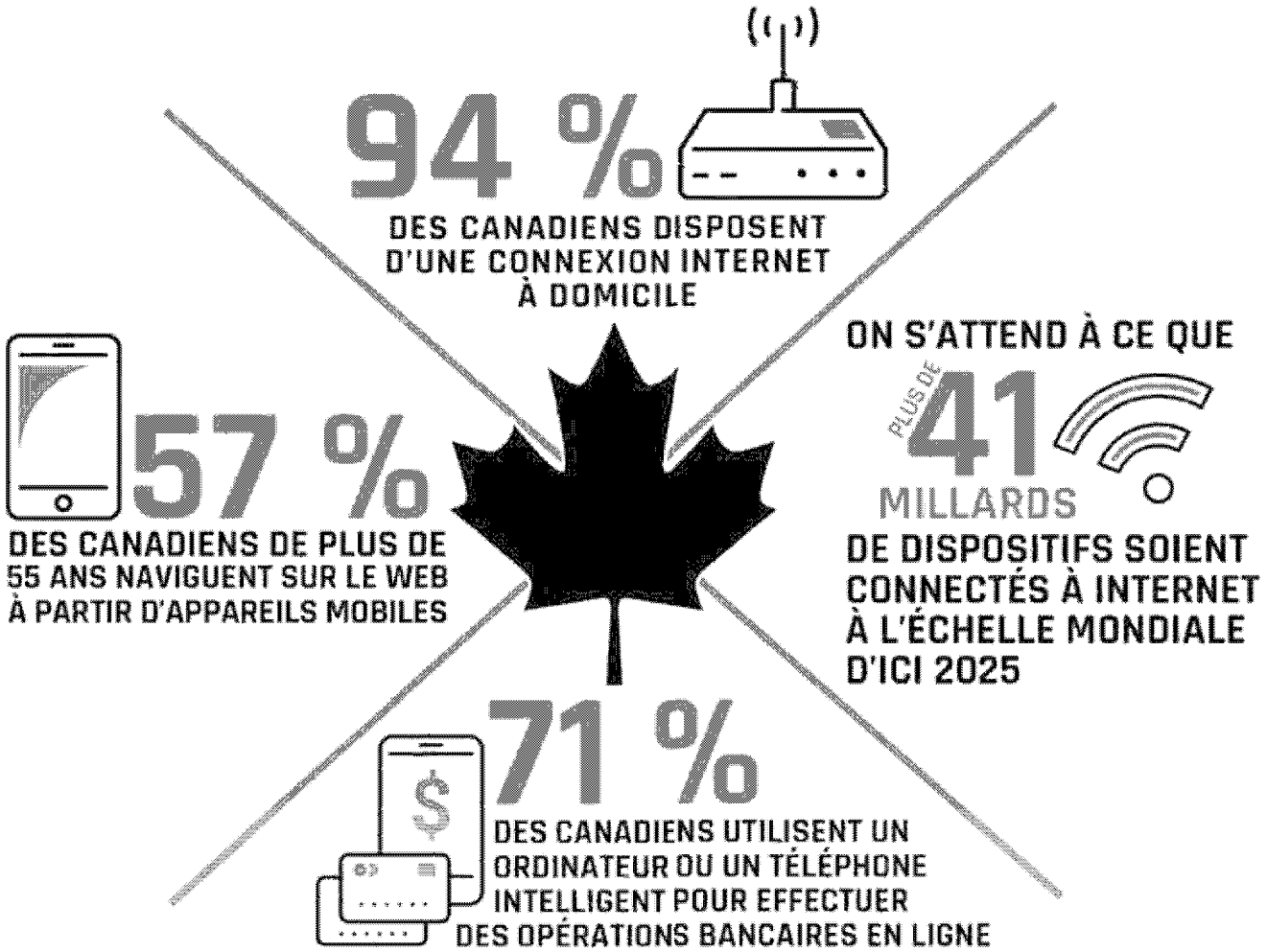
LES CYBERMENACES CONTRE LES CANADIENS

Les Canadiens mettent de plus en plus de renseignements personnels sur Internet, et ils dépendent aussi davantage de dispositifs connectés à Internet pour les communications, les finances, le divertissement, le confort et la sécurité. À mesure qu'évolue la technologie et que les habitudes changent, les auteurs de cybermenace s'adaptent rapidement pour tirer profit de nouvelles occasions et suivre les événements actuels. Ils vont par exemple modifier leur activité de cybermenace pendant la pandémie de COVID-19.

Les Canadiens continuent d'être victimes de fraudes en ligne. Comme prévu dans l'évaluation de 2018, il est fort probable que la cybercriminalité demeure la cybermenace la plus répandue auprès des Canadiens. Depuis la publication de l'évaluation de 2018, les auteurs de cybermenace ont amélioré leur façon de procéder de manière à rendre les arnaques pertinentes et attrayantes en associant leurs cyberfraudes à des événements d'actualité. Les élections, la période des impôts et les nouvelles qui font l'actualité ont toutes servi de toile de fond à la cybercriminalité. Par exemple, les auteurs de menace ont profité de la pandémie de COVID-19 pour inciter les victimes à cliquer sur des liens malveillants. Ces auteurs volent également des renseignements financiers et médicaux, ainsi que d'autres renseignements personnels qu'ils vendent en ligne ou utilisent dans le cadre de cybercrimes. Les importantes atteintes à la protection des données qui touchent les entreprises ont de sérieuses répercussions sur leurs clients. Ces atteintes révèlent des renseignements personnels pouvant servir à d'éventuels crimes.

Les Canadiens sont toujours victimes des opérations d'influence étrangère en ligne. L'objectif de celles-ci est d'influencer l'opinion publique et le discours politique au Canada. Et pour terminer, il importe de souligner que l'évolution des technologies comme les dispositifs médicaux de l'IdO, les véhicules connectés à Internet et les systèmes de sécurité à domicile procure aux auteurs de cybermenace de nouvelles cibles pour mettre en péril la sécurité physique des Canadiens.

Figure 1 : Utilisation d'Internet par les Canadiens; données tirées de l'Enquête canadienne sur l'utilisation de l'Internet 2018 de Statistique Canada[15], du Dossier documentaire sur Internet au Canada 2019 de l'ACEI[16] et des prévisions de l'International Data Corporation[17]



FRAUDE ET EXTORSION

Selon les statistiques obtenues du Centre antifraude du Canada, en 2019, les Canadiens ont perdu plus de 43 millions $ CA à la suite de fraudes liées à la cybercriminalité.[18] Ce chiffre ne tient compte que des cas rapportés de fraudes. On considère que le chiffre réel est fort probablement plus élevé. Comme prévu dans l'évaluation de 2018 et selon nos observations, au cours des deux dernières années, les types de tentatives de cyberfraude et d'extorsion visant les Canadiens ont gagné en sophistication. Cette tendance risque de se poursuivre, facilitée par les marchés de la cybercriminalité qui permettent aux auteurs de menace d'acheter des outils et services qu'ils utiliseront ensuite dans le cadre d'activités de cybermenace.

Les auteurs de cybermenace commettent des fraudes en se faisant passer pour des organismes légitimes, tels que des institutions gouvernementales, des établissements financiers ou des cabinets d'avocats, afin d'inciter les Canadiens à télécharger des maliciels sur leurs dispositifs en cliquant sur des pièces jointes ou des liens malveillants. Par exemple, certains fraudeurs créent de faux sites Web et de fausses publicités en ligne offrant des services d'immigration bon marché, ou garantissant des emplois bien rémunérés aux nouveaux immigrants. Beaucoup de ces faux sites Web ressemblent à des sites officiels du gouvernement, mais exigent que les victimes paient des frais pour avoir accès à des « formulaires importants ».[19] Depuis mars 2020, le CCC a travaillé avec ses partenaires pour fermer plus de 3 500 sites Web, comptes de médias sociaux et serveurs de courrier électronique qui représentaient frauduleusement le gouvernement du Canada.

Les auteurs de cybermenace peuvent également soutirer de l'argent à leurs victimes en les menaçant de cyberattaques ou en volant ou prétendant leur avoir volé des renseignements incriminants. Ces arnaqueurs créent également de faux profils sur les médias sociaux et les sites de rencontre afin d'inciter leurs victimes à s'engager dans une relation sur Internet qui facilite l'extorsion et la fraude. Dans certains cas, ils obtiennent des vidéos intimes de leur victime et menacent d'envoyer la vidéo aux contacts de celle-ci si la rançon n'est pas versée.[20]

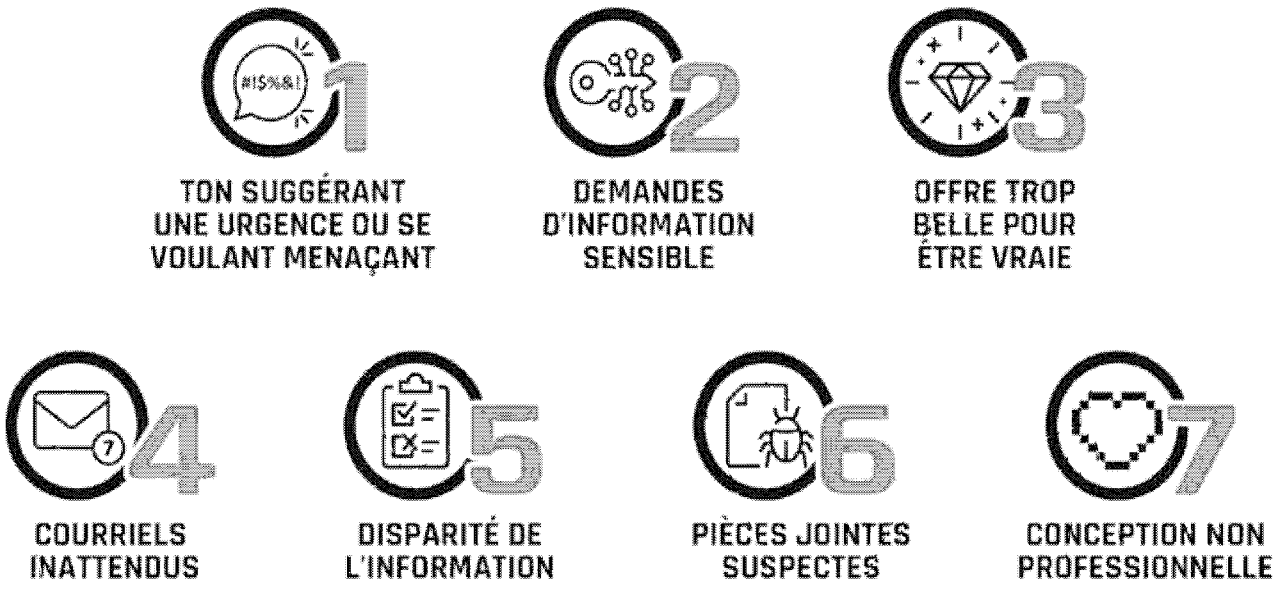
Depuis la publication de l'évaluation de 2018, nous avons remarqué que les auteurs de cybermenace se sont adaptés aux événements actuels en associant davantage leur façon de procéder à des événements d'actualité. Les élections, la période des impôts et les nouvelles qui font l'actualité ont toutes servi de toile de fond à la cybercriminalité pour inciter les victimes à cliquer sur des pièces jointes et des liens malveillants.

LES AUTEURS DE MENACE INFLUENCENT UNE CRISE MONDIALE : LA COVID-19

En 2020, nous avons observé les auteurs de cybermenace développer du contenu lié à la COVID 19 pour inciter les victimes à cliquer sur des pièces jointes et des liens malveillants. Les auteurs de cybermenace savent à quel point les gens sont inquiets quant à l'avenir et comptent sur le fait que leurs potentielles victimes sont moins portées à agir avec prudence lorsqu'elles reçoivent des courriels, des textos ou de la publicité concernant la COVID 19.

Les leurres liés à la COVID-19 impliquent souvent la reproduction ou l'imitation d'une marque ou d'un style propre à des organismes légitimes, comme des organismes internationaux et des services de santé publique. Les auteurs de cybermenace peuvent produire des copies convaincantes de sites Web du gouvernement et de correspondances officielles. Une campagne utilisant des courriels d'hameçonnage par SMS prétendait donner accès au paiement de la Prestation canadienne d'urgence, mais seulement après que la victime ait divulgué ses renseignements financiers personnels. Les auteurs d'une autre campagne se faisaient passer pour un médecin-conseil en santé de l'Agence de la santé publique du Canada pour implanter un maliciel au moyen d'une fausse mise à jour sur la COVID-19 qui semblait officielle et légitime.

Figure 2 : Éléments d'une communication malveillante



MENACES D'INGÉRENCE DANS LA VIE PRIVÉE

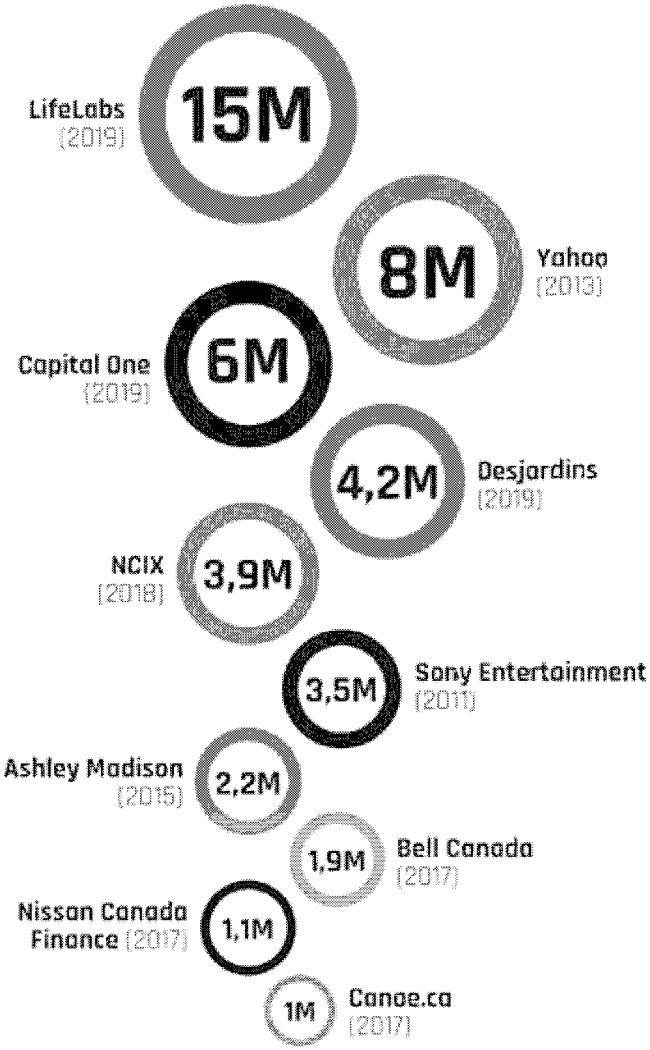
Dans l'évaluation de 2018, nous décrivons l'attrait des renseignements financiers et personnels pour les cybercriminels et voyons comment ces derniers profitent des renseignements volés pour obtenir un gain financier. La menace s'est maintenant intensifiée en raison de l'augmentation de la quantité de renseignements qui sont stockés en ligne, et dans la foulée des améliorations apportées à la science des données qui favorisent de nouvelles méthodes pour ce qui est d'exploiter les renseignements personnels, financiers et même médicaux. En outre, les cybercriminels ne sont pas les seuls auteurs de cybermenace intéressés à ces données. Il y a aussi les auteurs de cybermenace parrainés par des États qui compromettent d'importantes bases de données pour faire avancer les priorités nationales.

Renseignements financiers

La progression de la menace visant la vie privée des citoyens s'accroît avec le nombre de données échangées et stockées en ligne. Les atteintes à la protection des données menacent les renseignements financiers des Canadiens que détiennent les sociétés, et ces renseignements deviennent la proie des auteurs de cybermenace. Le vol des renseignements personnels et financiers des Canadiens est payant pour les cybercriminels, et on considère que ce type de fraude devrait augmenter au cours des deux prochaines années. Les cybercriminels font des profits au détriment des victimes en volant leurs justificatifs d'ouverture de session, les détails relatifs à leurs cartes de crédit et d'autres renseignements personnels. Ils peuvent ensuite décider de se servir de ces renseignements pour voler de l'argent ou commettre une fraude, ou tout simplement de les vendre sur les marchés de la cybercriminalité. En juin 2019, les données de 4,2 millions de membres canadiens de Desjardins ont été compromises.[21]

Cette fuite de données touchait, entre autres, les noms et les dates de naissance, les numéros d'assurance sociale, les coordonnées et les renseignements bancaires des victimes. Tout comme dans le cas de Desjardins, 6 millions de clients canadiens de la Capital One ont appris qu'ils avaient été victimes du vol de leurs renseignements personnels en mars 2019. Parmi les données volées, on retrouvait des renseignements personnels et des cotes de crédit, des données sur les opérations et des numéros de compte bancaire.[22]

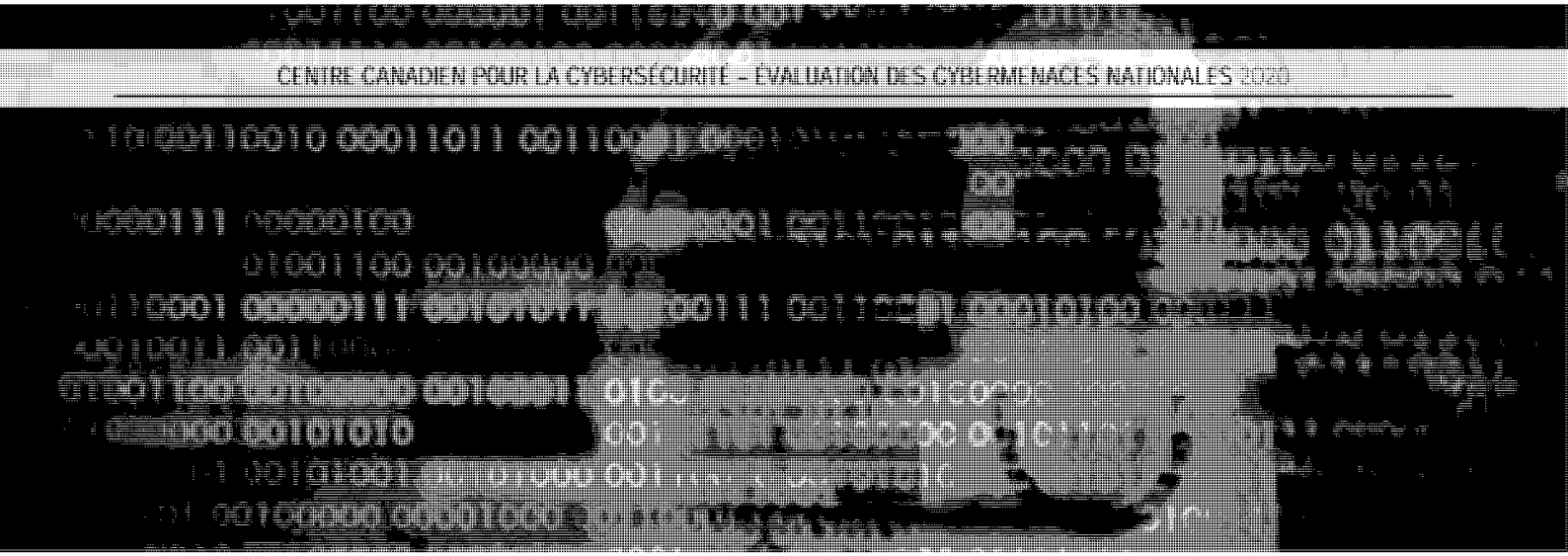
Figure 3 : Dix des plus importantes atteintes à la protection des données ayant eu une incidence sur les Canadiens de 2011 à aujourd'hui, par nombre de dossiers



CRYPTOMONNAIE ET CRYPTOMINAGE PIRATE

Les cybercriminels ont recours à des maliciels pour prendre le contrôle d'ordinateurs et utiliser leur puissance de calcul pour générer ou « miner » de la cryptomonnaie sans autorisation. C'est ce que l'on appelle le cryptominage. Les systèmes informatiques désuets ou non corrigés sont particulièrement vulnérables à cette cybermenace, et certains utilisateurs touchés peuvent ne rien voir d'inhabituel avec leur dispositif, tandis que d'autres constatent des problèmes de ralentissement ou une décharge rapide de la pile.[23]

Comme prévu dans l'évaluation de 2018, les cybercriminels ont continué de développer des maliciels en vue de les déployer dans le cadre d'opérations de cryptominage pirate. Selon nos observations, cette activité devrait fort probablement continuer au cours des deux prochaines années dans la mesure où les niveaux d'activité sont liés aux fluctuations de la valeur de la cryptomonnaie.



Données médicales et personnelles

En 2019, l'entreprise de laboratoire médical LifeLabs a été victime d'une cyberattaque qui a compromis les données personnelles et médicales de 15 millions de Canadiens avant que l'entreprise paie la rançon demandée pour récupérer les données.[24] Les auteurs de menace, et tout particulièrement les auteurs de cybermenace parrainés par des États, ont recours à la science des données pour mieux utiliser les grands ensembles de données. Ils peuvent ainsi identifier, profiler et suivre les citoyens en combinant et en désanonymisant les données provenant de plusieurs ensembles de données.

Les auteurs de cybermenace peuvent utiliser les renseignements personnels volés en se servant d'une technique appelée « attaque de bourrage de justificatifs » par laquelle un grand nombre de combinaisons de noms d'utilisateur et de mots de passe compromis sont entrées dans des sites Web dans l'espoir qu'une de celles-ci corresponde à un compte existant. Les renseignements personnels volés peuvent comprendre des justificatifs d'identité qui faciliteront ce type d'activité de même qu'un accès aux réponses aux questions de sécurité, rendant ainsi inefficace cette protection. Après avoir recueilli des données lors de multiples atteintes à la sécurité, les cybercriminels sont en mesure de combiner les renseignements personnels d'une personne et de cibler plus efficacement leurs activités de cybermenace.

ATTEINTE À LA PROTECTION DE DONNÉES DE LA CAPITAL ONE ET DES HÔTELS MARRIOTT

Une accumulation de données attire les cybercriminels et les auteurs de cybermenace parrainés par des États. En 2019, un cybercriminel a volé les données des clients de la Capital One, une société de services financiers américaine. Cette atteinte à la sécurité a touché 106 millions de clients, dont six millions de Canadiens. Parmi les renseignements privés recueillis se trouvaient des numéros d'assurance sociale et de sécurité sociale ainsi que des renseignements bancaires.[25] En 2018, la chaîne hôtelière Marriott a annoncé que sa base de données de réservation avait été compromise, et que les renseignements personnels d'environ 500 millions d'invités avaient été volés. Cette attaque a été liée à des pirates informatiques parrainés par des États. Ils ont pu mettre la main sur de nombreux renseignements, dont des noms, des adresses et des numéros de passeport.[26]

INFLUENCE ÉTRANGÈRE EN LIGNE

Un nombre croissant d'États ont élaboré et déployé des programmes visant à mener une activité d'influence en ligne dans le cadre de leurs pratiques quotidiennes. Des adversaires ont recours à des campagnes d'influence pour tenter de changer le discours public, les choix des décideurs politiques, les relations gouvernementales et la réputation des politiciens et des pays, tant à l'échelle nationale qu'internationale. Ils tentent de délégitimiser le concept de la démocratie ainsi que d'autres valeurs, comme les droits de la personne et ceux touchant aux libertés, qui peuvent aller à l'encontre de leurs propres positions idéologiques. Ils cherchent également à aggraver la friction actuelle dans les sociétés démocratiques en ce qui concerne diverses questions controversées d'ordre social, politique et économique. Bien que les activités d'influence en ligne aient tendance à augmenter en périodes électorales, la portée de ces campagnes continues s'est élargie depuis 2018, de façon à réagir et à s'adapter aux événements actuels, et à changer les stratégies en fonction des nouvelles qui font l'actualité et des enjeux politiques populaires.

Comme prévu dans l'évaluation de 2018, les Canadiens continuent d'être la cible d'activités d'influence en ligne. Par exemple, nous avons noté que l'attention des récentes campagnes s'est tournée sur la COVID-19 et les mesures prises par les gouvernements face à la pandémie. Les campagnes de désinformation ont également cherché à discréditer et à critiquer les politiciens canadiens dans le but de nuire à leur réputation. Nous estimons néanmoins que, comparativement à d'autres pays, les Canadiens ne présentent pas une cible prioritaire en ce qui a trait aux campagnes d'influence étrangère en ligne, mais les positions prises par le Canada sur des enjeux prioritaires d'ordre géopolitique pourraient faire augmenter la menace. Il faut toutefois noter qu'au Canada, les écosystèmes des médias sont étroitement liés à ceux des États-Unis et d'autres alliés. Conséquemment, lorsque les populations de ces pays sont ciblées, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne.

On considère que l'exposition à l'influence étrangère en ligne se poursuivra certainement pendant au moins les deux prochaines années pour autant que les auteurs de cybermenace adaptent leurs activités à l'évolution des politiques des sociétés Internet comme Google, Facebook et Twitter.

LES AUTEURS DE CYBERMENACE TENTENT DE DIVISER LES CANADIENS

Une analyse des données Tweeter a révélé que des trolls d'Internet russes et iraniens ont utilisé des comptes de façon frauduleuse pour mettre en évidence les divisions entre les Canadiens en amplifiant des propos incendiaires sur des questions politiques qui attisent la discorde, comme le terrorisme, les changements climatiques, la construction de pipelines, ainsi que les politiques sur l'immigration et à l'égard des réfugiés. Bon nombre de ces gazouillis réagissaient à des événements importants, comme ce fut le cas en janvier 2017 à la suite de la tuerie de la mosquée de Québec, ou en juin 2019 après l'approbation de l'expansion du pipeline Trans Mountain.[27]

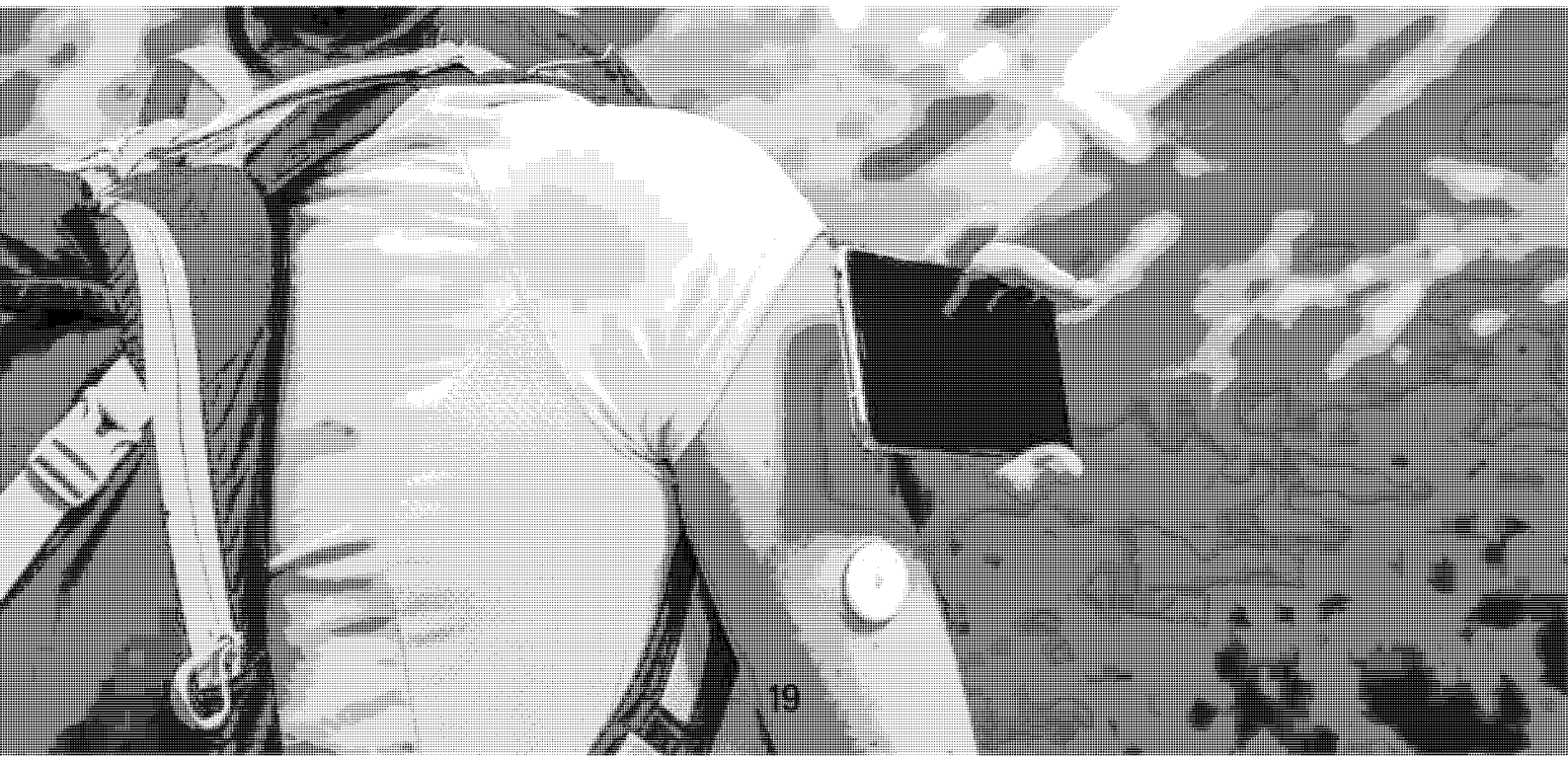
MENACES À LA SÉCURITÉ PHYSIQUE

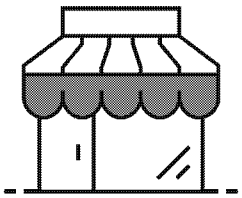
Les dispositifs personnels connectés à Internet, notamment les dispositifs médicaux de l'IdO, les véhicules connectés à Internet et les systèmes de sécurité à domicile, font partie du quotidien et constituent de nouvelles cibles pour les auteurs de cybermenace. Cela dit, bien que d'autres cybermenaces, comme les atteintes à la protection des données, soient plus répandues et aient des répercussions plus larges, les utilisateurs courent quand même le risque que leurs dispositifs et systèmes soient éventuellement ciblés par des activités de cybermenace pouvant avoir une incidence sur leur sécurité physique. Par exemple, les dispositifs médicaux connectés à Internet sont de plus en plus courants et susceptibles d'être la cible d'auteurs de cybermenace qui chercheront à en altérer ou en perturber le fonctionnement.

Un autre exemple démontre que des harceleurs et des partenaires violents tirent avantage des vulnérabilités des dispositifs personnels de l'IdO pour voler les renseignements recueillis par les montres intelligentes et les moniteurs d'activité physique dans le but d'identifier et de localiser leurs victimes. Ils sont également en mesure de manipuler les systèmes de maison intelligente afin de contrôler l'environnement de leurs victimes et de les intimider. Dans un cas en particulier, un homme s'est servi d'une application de véhicule intelligent pour démarrer, éteindre et suivre le véhicule de sa victime à partir de son téléphone.[28] Un organisme offrant du soutien aux victimes de violence conjugale a indiqué qu'en date de janvier 2019, plus de 2 500 femmes qui y trouvent refuge ont déclaré avoir été victimes d'abus facilités par la technologie.[29]

DISPOSITIFS MÉDICAUX PERSONNELS CONNECTÉS À INTERNET

En mars 2020, Santé Canada a publié une alerte informant les Canadiens de vulnérabilités de cybersécurité touchant des dispositifs médicaux, comme les simulateurs cardiaques, les glucomètres et les pompes à insuline, dotés d'un certain type de puce Bluetooth. Des auteurs de menace pourraient exploiter ces vulnérabilités pour provoquer une panne du dispositif, le déverrouiller ou contourner les mesures de sécurité afin d'accéder à des fonctionnalités qui sont réservées à un utilisateur autorisé.[30]





LES CYBERMENACES CONTRE LES ORGANISMES CANADIENS

Comme prévu dans l'évaluation de 2018, la cybercriminalité demeure la menace la plus répandue à laquelle font face les entreprises canadiennes de toutes tailles. Toutefois, d'autres activités de cybermenace, comme le cyberespionnage, peuvent avoir une incidence plus grande. L'information volée fait souvent l'objet d'une demande de rançon. Elle peut aussi être vendue et utilisée afin de tirer un avantage concurrentiel. Depuis les deux dernières années, cibler des procédés industriels et mener des attaques par rançongiciel sont pratique courante. Les incidences de ces cyberincidents peuvent être majeures, notamment porter atteinte à la réputation, entraîner une perte de productivité, avoir des répercussions juridiques, exiger des dépenses relatives à la reprise et entraîner des dommages à l'infrastructure et aux opérations. On considère que les activités malveillantes dirigées contre le Canada continueront probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles au cours des deux prochaines années.

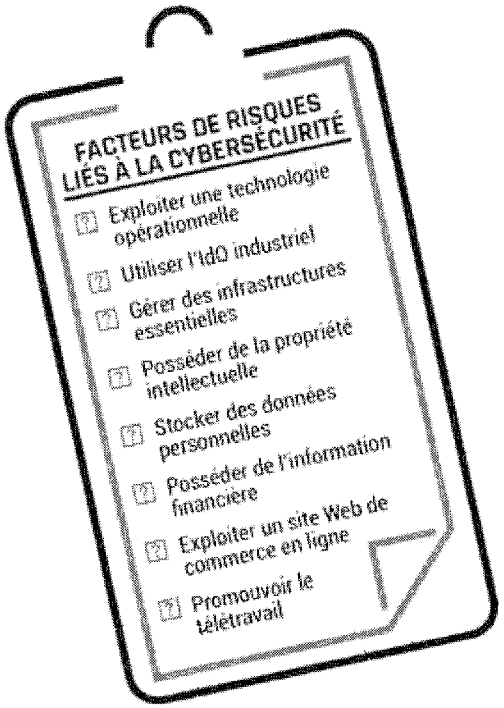
Les auteurs de cybermenace mettent également en danger l'information que détiennent les organisations canadiennes ainsi que les données des clients. Le vol de cette information peut avoir des conséquences financières à court et à long termes pour les victimes, notamment des impacts sur leur compétitivité à l'échelle internationale et sur leur réputation. Pendant la pandémie de COVID-19, des auteurs de cybermenace parrainés par des États ont ciblé la propriété intellectuelle canadienne liée à la lutte contre la COVID-19, et on estime que ces auteurs continueront probablement à le faire afin d'appuyer leurs programmes de santé publique nationaux ou de tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés.

Les auteurs de cybermenace ciblent les systèmes de paiement en ligne et en personne, profitent des vulnérabilités des chaînes d'approvisionnement et tirent parti de l'accès privilégié que maintiennent les fournisseurs de services gérés aux réseaux de leurs clients. Ces activités peuvent servir à frauder des organisations, à se livrer à des attaques par rançongiciel ou à voler des renseignements exclusifs ou les données des clients.

Les organisations canadiennes de toutes tailles, comme les petites et moyennes entreprises, les municipalités, les universités et les fournisseurs d'infrastructures essentielles, sont confrontées à un nombre croissant de cybermenaces.[31]

Ces organisations contrôlent un vaste éventail d'actifs pouvant intéresser les auteurs de cybermenace, dont la propriété intellectuelle, les données financières, les systèmes de paiement, les données des clients, les partenaires et les fournisseurs, ainsi que les installations industrielles et leur machinerie. En règle générale, plus une organisation possède d'actifs connectés à Internet, plus elle court le risque de faire face à une cybermenace.

Figure 4 : Liste des actifs appartenant à des organisations qui augmentent le risque pour la cybersécurité



CIBLER LA SÉCURITÉ DES CANADIENS

Cibler les systèmes de contrôle industriels et les infrastructures essentielles

La sécurité des Canadiens est menacée lorsque les auteurs de cybermenace ciblent des organisations responsables de l'exploitation des services publics ou de la prestation de soins de santé ou de services gouvernementaux essentiels. Or, à en juger par l'évaluation de 2018, il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Ils pourraient néanmoins cibler des entreprises canadiennes essentielles dans le but de recueillir des données, de se prépositionner en vue d'activités ultérieures ou de les intimider. Il est fort probable que des auteurs de cybermenace parrainés par des États cherchent à développer les moyens nécessaires pour perturber l'approvisionnement en électricité au Canada.

Les systèmes de contrôle industriels (SCI) appartiennent à un type de technologie opérationnelle qui permet d'assurer la surveillance et le contrôle de l'équipement matériel utilisé dans le cadre des procédés industriels ou des processus liés aux infrastructures essentielles. Les SCI, et plus particulièrement ceux du secteur de l'électricité, sont ciblés dans le monde entier. Les auteurs de cybermenace parrainés par des États sont souvent à l'origine de ces attaques. En 2019, des pirates associés à la Russie ont accédé aux réseaux de fournisseurs d'électricité aux États-Unis et au Canada.[32] Des groupes de pirates informatiques iraniens ont ciblé des infrastructures dans des nations rivales, notamment les États-Unis, Israël et l'Arabie saoudite.[33] Un maliciel nord-coréen a été trouvé dans les réseaux informatiques d'une centrale électrique indienne, et des employés des services publics américains ont été visés par des auteurs de cybermenace parrainés par la Chine.[34]

Depuis les dernières années, les rançongiciels ont de plus en plus d'incidences sur les SCI. On estime que les programmes des rançongiciels peuvent maintenant s'infiltrer plus efficacement dans les réseaux informatiques et devenir une menace pour les environnements SCI connexes. Dans certains cas, les victimes choisissent de désactiver leurs procédés industriels par mesure de précaution lorsque l'entreprise fait l'objet d'une attaque par rançongiciel. Par exemple, en mars 2019, une aluminerie norvégienne a été paralysée par un rançongiciel qui a attaqué ses données logistiques et de production, ce qui l'a forcée à arrêter les SCI et à passer à la production en mode manuel.[35] Les cybercriminels devraient cibler davantage les SCI au cours des deux prochaines années afin d'accroître la pression sur les infrastructures essentielles et ainsi inciter les victimes de l'industrie à consentir rapidement au paiement de la rançon demandée.

EXEMPLE DE RANÇONGICIEL VISANT LES SCI

Depuis janvier 2019, au moins sept variantes de rançongiciel contenaient des instructions visant à interrompre les procédés liés aux SCI.[36] L'impact de ces attaques sur les SCI varie en fonction des circonstances particulières du procédé industriel et de la réaction du personnel en place.[37] En juin 2020, un constructeur automobile a suspendu la production dans la majorité de ses usines en Amérique du Nord, dont une au Canada, pour « assurer la sécurité de ses activités » après avoir été la cible d'une attaque faisant appel à une de ces variantes de rançongiciel.[38]

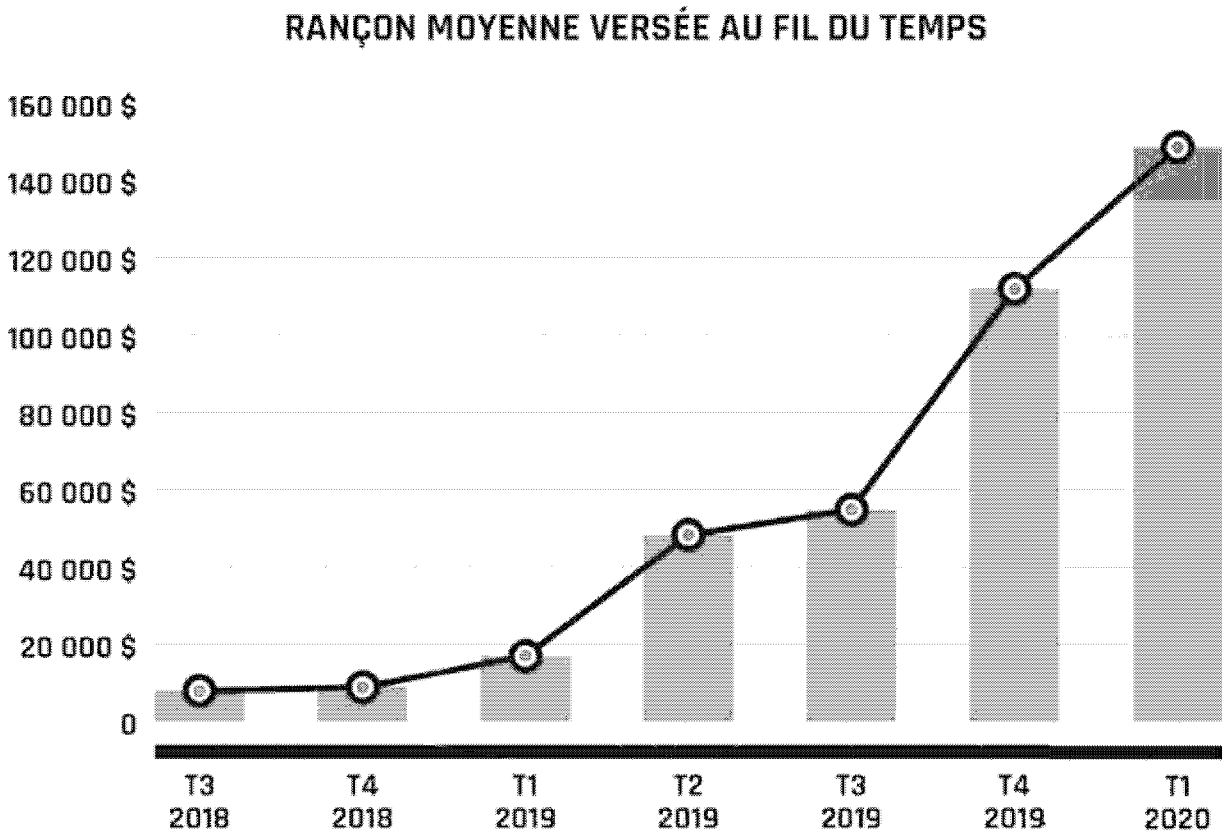
MENACES À LA SANTÉ FINANCIÈRE ET ÉCONOMIQUE DES CANADIENS

Les activités de cybermenace entraînent des dépenses imprévues pour les organisations. Il peut s'agir des rançons versées ou de fonds volés, des pertes occasionnées par l'interruption des opérations, des coûts nécessaires pour assurer la sécurité des réseaux, d'une atteinte à la réputation et de la perte de clients qui en découle, et sans oublier du vol de propriété intellectuelle et de renseignements confidentiels.[39] Ces coûts siphonnent les ressources limitées des organisations et diminuent la compétitivité de ces dernières face à d'autres entreprises. Combinés, ils représentent en fait un fardeau sur l'ensemble de l'économie canadienne.

Rançongiciel et chasse au gros gibier

Selon l'évaluation de 2018, le rançongiciel a été identifié comme étant la forme la plus répandue de maliciel utilisé pour extorquer de l'argent aux Canadiens. Les cybercriminels ont toutefois changé leurs tactiques pour leur permettre d'augmenter le montant des rançons demandées et d'accroître leur probabilité de réussite. Au cours des dernières années, les cybercriminels chassent de plus en plus le gros gibier et concentrent leurs activités sur de grandes entreprises qui doivent éviter que leurs réseaux soient perturbés, et qui sont prêtes à payer de lourdes rançons pour rétablir rapidement leurs opérations.[40] Avec la recrudescence de ce type de campagne de rançongiciel, le montant des rançons demandées a aussi augmenté. Les chercheurs en rançongiciel estiment que la moyenne des demandes de rançon a augmenté de 33 % depuis le T4 de 2019 pour atteindre environ 148 700 $ CA au cours du T1 de 2020 en raison de l'impact de ce type de cybermenace sur les opérations visées par des rançongiciels.[41] À l'extrémité du spectre se trouvent les demandes de rançon de plusieurs millions de dollars, qui sont devenues de plus en plus courantes. En octobre 2019, une compagnie d'assurance canadienne a payé 1,3 million $ CA pour récupérer 20 serveurs et 1 000 postes de travail.[42] De plus, nous croyons que les auteurs de cybermenace parrainés par des États pourraient utiliser un rançongiciel afin de masquer l'origine de leurs activités et leurs intentions. Il est presque assuré que les services de renseignement de nombreux pays collaborent avec des cybercriminels qui se livrent à des stratagèmes par rançongiciel. Dans cette collaboration avec bénéfices mutuels, les cybercriminels échangent des données avec les services de renseignement et ces derniers leur permettent de poursuivre leurs opérations sans avoir à respecter les lois.

Figure 5 : Rançon moyenne versée lors d'attaques par rançongiciel entre 2018 et 2020 (données de Coveware[43] avec conversion de $ US à $ CA)



Nous croyons que les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles. En outre, il est probable que bon nombre de victimes canadiennes continueront de consentir à payer les rançons pour éviter les conséquences économiques graves et potentiellement dévastatrices qui pourraient survenir advenant un refus. Depuis la fin de 2019, de nombreuses entreprises canadiennes et plusieurs gouvernements provinciaux ont vu leurs données divulguées par des opérateurs de rançongiciels après avoir refusé de verser la rançon demandée. Ce fut entre autres le cas pour une entreprise de construction et un consortium d'entreprises agricoles canadiennes.[44]

LE SECTEUR DE LA SANTÉ FRÉQUEMMENT CIBLÉ PAR LES RANÇONGICIELS

En 2019 et 2020, de nombreux organismes canadiens du secteur de la santé ont été ciblés dans le cadre d'attaques par rançongiciel. Par exemple, en octobre 2019, trois hôpitaux de l'Ontario ont été victimes de telles attaques, et un centre de diagnostic et de tests spécialisés a vu ses données compromises par un rançongiciel en décembre 2019. Au début de 2020, une attaque par rançongiciel a aussi ciblé une société médicale de la Saskatchewan.[45] Beaucoup d'organismes mondiaux du secteur de la santé ont dû faire face à des attaques par rançongiciel pendant la pandémie de COVID-19, notamment des hôpitaux et des centres de soins de santé en République tchèque, aux États-Unis, en Espagne et en Allemagne.[46] Ces organismes sont des cibles populaires parmi les opérateurs de rançongiciels en raison de leurs importantes ressources financières et du fait qu'ils sont plus susceptibles de payer la rançon, puisqu'une panne de réseau peut mettre en danger la vie de patients.

Vol de propriété intellectuelle et de renseignements exclusifs

Dans l'évaluation de 2018, il a été question de la menace qui pèse sur les entreprises canadiennes en raison du cyberespionnage industriel. La menace est toujours présente aujourd'hui, puisque des auteurs de cybermenace parrainés par des États continuent de mener des activités d'espionnage contre les réseaux d'organismes au Canada et dans des nations alliées dans le but de voler la propriété intellectuelle, des secrets commerciaux et d'autres renseignements commerciaux de nature exclusive. Au Canada, ces auteurs de cybermenace ont mené des activités d'espionnage contre une grande diversité d'organismes canadiens, dont ceux du secteur privé, du milieu universitaire et du gouvernement. Ils ciblent plus particulièrement les organismes du secteur de la santé et de la biotechnologie, de l'énergie, des télécommunications et de la défense.[47]

Une campagne de longue date menée par des auteurs de cybermenace parrainés par des États a compromis des fournisseurs de services gérés (FSG) dans le but de mettre la main sur la propriété intellectuelle et des renseignements commerciaux et technologiques confidentiels liés à l'aviation, à la santé, à la biotechnologie, aux télécommunications, ainsi qu'à d'autres secteurs. Ils ont ciblé des entreprises tant au Canada que dans pas moins de 12 pays depuis 2006.[48] On a signalé en 2019 qu'une campagne parrainée par des États avait ciblé plus de deux douzaines d'universités au Canada, aux États-Unis et en Asie du Sud-Est pour tenter d'obtenir de l'information liée à la technologie et à la recherche maritimes à des fins militaires.[49]

Durant la pandémie de COVID-19, plusieurs grandes entreprises des industries médicale et biopharmaceutique du Canada et de l'étranger ont été la cible d'auteurs de cybermenace parrainés par des États qui tentaient de voler la propriété intellectuelle liée aux essais, aux traitements et aux vaccins contre la COVID-19. Selon nos observations, il est probable que ces auteurs de cybermenace continuent à tenter de voler la propriété intellectuelle canadienne touchant la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés.[50]

Les organisations ayant des activités et des infrastructures à l'étranger sont exposées à des cybermenaces supplémentaires. Leurs opérations à l'étranger peuvent être régies par des lois sur la propriété intellectuelle, la protection de la vie privée ou la sécurité nationale, qui sont différentes et parfois plus laxistes. De nombreux pays disposent d'un pouvoir juridique et ont la compétence technique nécessaire pour accéder secrètement aux données qui passent par leur pays ou y sont conservées. Cela a de sérieuses conséquences sur les données et la propriété intellectuelle canadiennes envoyées dans des bureaux à l'étranger ou sur celles qui transitent par des réseaux qui se trouvent dans d'autres pays. Même les données qui sont échangées entre deux organismes au Canada peuvent transiter par des réseaux étrangers avant d'arriver à destination. Toutefois, conformément aux jugements formulés dans l'évaluation de 2018, on considère que la menace de cyberespionnage est certainement beaucoup plus grande pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

CYBERATTAQUES RUSSES CIBLANT LA RECHERCHE DE VACCIN CONTRE LA COVID-19

En juillet 2020, dans un communiqué conjoint, le Centre canadien pour la cybersécurité, le National Cyber Security Centre du Royaume Uni et la National Security Agency des États-Unis ont dressé un rapport des tactiques, des techniques et des procédures utilisées par un auteur de cybermenace parrainé un État qui ciblait des organisations impliquées dans le développement de vaccins contre la COVID-19 au Canada, aux États-Unis et au Royaume-Uni.[51] On considère que l'auteur de cette attaque pourrait fort probablement faire partie des services de renseignement russes et que son objectif est vraisemblablement de voler l'information et la propriété intellectuelle liées au développement et aux essais de vaccins contre la COVID-19.

Vol de données des clients

Comme prévu dans l'évaluation de 2018, les auteurs de cybermenace continuent de cibler les grands ensembles de données détenus par des entreprises au Canada et à travers le monde. Les bases de données volumineuses qui contiennent des renseignements personnels, tels que des noms, des adresses, des numéros de téléphone, de l'information relative à l'emploi, des références et des données financières ont pour eux une valeur inestimable. L'agrégation des données obtenues lors de multiples compromissions permet aux cybercriminels d'obtenir suffisamment d'information pour demander frauduleusement des prêts ou des cartes de crédit, produire une fausse déclaration d'impôt, transférer de l'argent illégalement, extorquer de l'argent à des victimes, avoir accès à des comptes en ligne ou concevoir des courriels d'hameçonnage persuasifs.[52] Les auteurs de cybermenaces parrainés par des États peuvent également se servir de ces données pour traquer des dissidents, des minorités ou des cibles d'espionnage dans leur pays ou à l'étranger.

Les cybercriminels qui s'adonnent au vol de données sont généralement des opportunistes motivés par l'appât du gain, alors que les auteurs de cybermenace parrainés par des États cherchent à obtenir de grandes quantités d'informations sensibles pour soutenir des objectifs stratégiques plus larges, comme la collecte de renseignements. Selon la présente évaluation, il est fort probable qu'au cours des deux prochaines années, les organisations canadiennes demeurent une cible de choix pour les cybercriminels et les auteurs de cybermenace parrainés par des États qui cherchent à obtenir de l'information nominative et d'autres données sensibles.

Les attaques par rançongiciel menées par les auteurs de cybermenace ont également gagné en sophistication. Ces derniers menacent les entreprises de divulguer l'information confidentielle de leurs clients à moins qu'une rançon soit versée, incitant ainsi les victimes à acquiescer à leurs demandes.[53] Toutefois, même si un paiement est effectué, les auteurs de cybermenace peuvent décider de supprimer, de modifier ou de divulguer l'information, ou encore utiliser les données volées lors d'une fraude ultérieure.

LA PLUS IMPORTANTE ATTEINTE À LA PROTECTION DES DONNÉES DE L'HISTOIRE CANADIENNE

En octobre 2019, une cyberattaque menée par des pirates informatiques a compromis les données de l'entreprise canadienne de laboratoire médical LifeLabs. Les renseignements personnels et confidentiels d'environ 15 millions de Canadiens ont été exposés, ce qui représente la fuite la plus massive de données personnelles jamais enregistrée au Canada. Les voleurs se sont emparés de résultats d'examen, de numéros de carte d'assurance maladie, de noms, de dates de naissance, d'adresses privées et d'adresses de courriel. Bien que LifeLabs ait payé la rançon pour récupérer les données, on ne peut garantir que les voleurs n'ont pas fait une copie des données pour profiter de ces renseignements ou les vendre à d'autres criminels.[54]

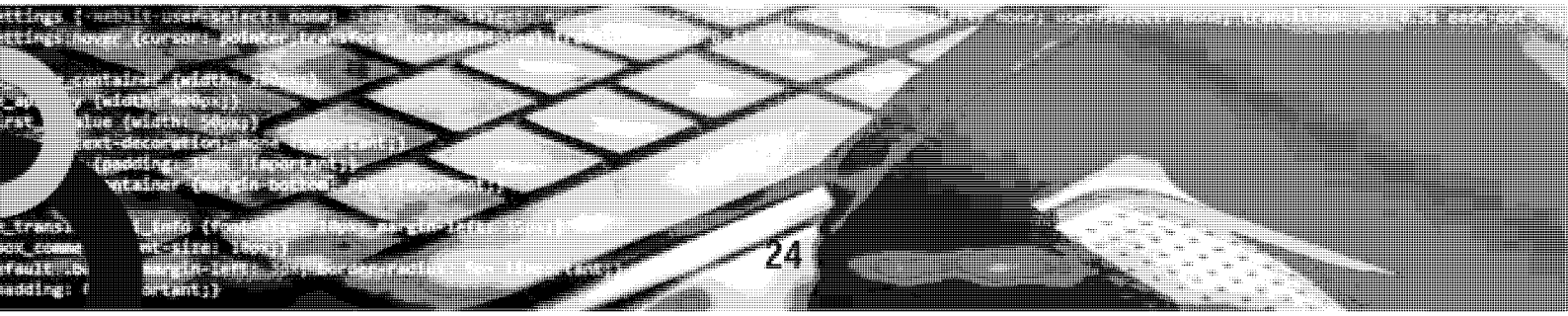
Exploitation des relations de confiance

Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les auteurs de cybermenace continueraient probablement de tirer parti des relations de confiance entre les entreprises et leurs fournisseurs de services. Depuis 2018, les auteurs de cybermenace motivés par un intérêt financier ont nettement accentué le recours à certaines techniques de piratage psychologique pour cibler des organisations.[55] Une des techniques les plus répandues et parmi les plus coûteuses est appelée la « compromission de courriel d'affaires » ou la « fraude du faux PDG ». Ce type de fraude consiste à envoyer un courriel à un employé d'une entreprise pour le convaincre de transférer directement des fonds à l'expéditeur malveillant. Souvent, les auteurs de cybermenace se font passer pour des cadres supérieurs ou des tiers de confiance. En raison des incertitudes entourant la pandémie de COVID-19, les auteurs de cybermenace se servent de la situation pour cibler des victimes.

LA FRAUDE UTILISANT LA COMPROMISSION DE COURRIEL D'AFFAIRES NE TOUCHE PAS QUE LES ENTREPRISES

En mai 2019, une municipalité de l'Ontario a été victime d'une fraude par compromission de courriel d'affaires. L'auteur de menace s'est fait passer pour un fournisseur de confiance de la ville. Dans son faux courriel, il a demandé de changer l'information bancaire du fournisseur et une fois les changements effectués, 503 000 $ CA avaient été virés sur le nouveau compte appartenant au cybercriminel.[56]

Au cours des deux dernières années, les auteurs de cybermenace ont étendu leur utilisation de la compromission de courriel d'affaires pour cibler des organisations religieuses, à vocation éducative et à but non lucratif.[57] Les cybercriminels devraient en principe continuer à utiliser de plus en plus la compromission par courriel d'affaires en raison de la simplicité et de la rentabilité de cette technique.[58] Selon certaines évaluations, entre 2016 et 2019, on comptait plus de 1 200 cas reportés de fraude par compromission de courriel d'affaires au Canada, ce qui a entraîné des pertes de plus de 45 millions $ CA.[59] La perte moyenne liée à cette fraude et impliquant des virements bancaires se chiffre à environ 47 000 $ CA.[60]



Exploitation des systèmes de paiement

Les cybercriminels ciblent les données des cartes de paiement dans le but de voler les détails relatifs aux cartes de crédit ainsi que d'autres renseignements que les victimes entrent sur les sites de commerce électronique. C'est ce que l'on appelle le détournement de formulaire.[61] En 2018, environ 4 800 sites Web étaient victimes de détournement de formulaire chaque mois.[62] Plusieurs grands sites Web ont été compromis par cette technique, dont des compagnies aériennes, des vendeurs de billets et bien d'autres.[63] En 2019, plus de 200 librairies universitaires au Canada et aux États-Unis ont été touchées par le détournement de formulaire.[64] On considère que cette tendance devrait augmenter au cours des deux prochaines années, car de plus en plus de Canadiens ont recours au commerce électronique en raison notamment de la pandémie de COVID-19.[65]

Comme nous l'avons vu dans l'évaluation de 2018, les auteurs de cybermenace continuent également à cibler les systèmes de point de vente (PDV) qu'utilisent les boutiques traditionnelles. Ils le font en installant des maliciels afin de voler l'information des clients, de nuire aux activités de l'entreprise, d'effectuer des achats frauduleux, de manipuler les prix et de provoquer d'autres formes de perturbation. À la fin de 2019, des cybercriminels ont ciblé les systèmes PDV de certaines stations-service en Amérique du Nord pour voler leurs données financières.[66] Les données stockées dans la bande magnétique des cartes de crédit et recueillies à partir de terminaux de PDV infectés sont vendues sur les marchés noirs de la cybercriminalité. Elles permettent aux criminels de recréer ou de cloner les cartes.

Compromission de la chaîne d'approvisionnement

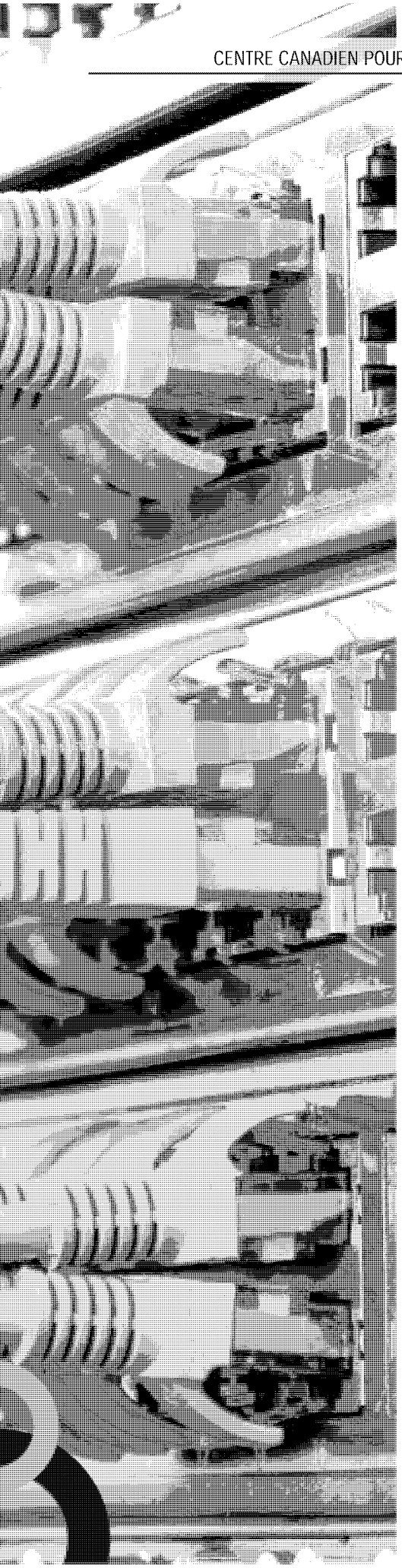
Plusieurs entreprises comptent sur une chaîne d'approvisionnement complexe – et souvent répartie mondialement – pour de nombreux aspects de leurs opérations, dont la fabrication de précurseurs, l'infrastructure de TI, le soutien informatique et les services financiers.[67] Les auteurs de cybermenace ciblent les réseaux de fournisseurs de confiance pour ensuite profiter de leurs accès et s'infiltrer dans les réseaux de leurs véritables cibles. Les compromissions de la chaîne d'approvisionnement peuvent survenir avant ou après la livraison d'un produit ou service, ou au cours des mises à jour logicielles et des mises à niveau matérielles. Les auteurs de cybermenace ciblent particulièrement les mises à jour et les mises à niveau parce qu'ils savent qu'elles seront téléchargées et installées des milliers, voire des millions de fois dans plusieurs entreprises, ce qui multiplie ainsi les occasions de fraude. Tel qu'il est illustré dans la figure 6, chaque maillon d'une chaîne d'approvisionnement mondiale peut représenter un risque pour la cybersécurité. Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les auteurs de cybermenace continueraient de tirer profit des chaînes d'approvisionnement. On considère qu'il est probable que les auteurs de cybermenace continuent d'exploiter ces vulnérabilités au cours des deux prochaines années.

EXPLOITATION DES VULNÉRABILITÉS DE LA CHAÎNE D'APPROVISIONNEMENT

Depuis le début de la pandémie de COVID-19, les auteurs de cybermenace ont pu obtenir accès à un grand nombre d'hôpitaux à l'échelle mondiale, compromettant ainsi les réseaux informatiques et les composants des SCI ainsi que les produits d'imagerie utilisés dans le secteur de la santé.[68] En 2018, ces mêmes auteurs ont ciblé des organismes du domaine de la santé dans au moins 24 pays, dont le Canada, ainsi que des organismes dans d'autres domaines, comme le secteur manufacturier, l'informatique, la logistique et l'agriculture.[69]

On considère que ces auteurs malveillants ont probablement utilisé les mises à jour logicielles provenant de fournisseurs de confiance pour propager les maliciels et compromettre les données de leurs victimes.[70] Il est fort probable que les responsables de cette attaque aient été parrainés par un État et aient cherché à obtenir de l'information sensible ou exclusive pour faire avancer les priorités de leur pays.

Figure 6 : Vulnérabilités liées à la chaîne d'approvisionnement

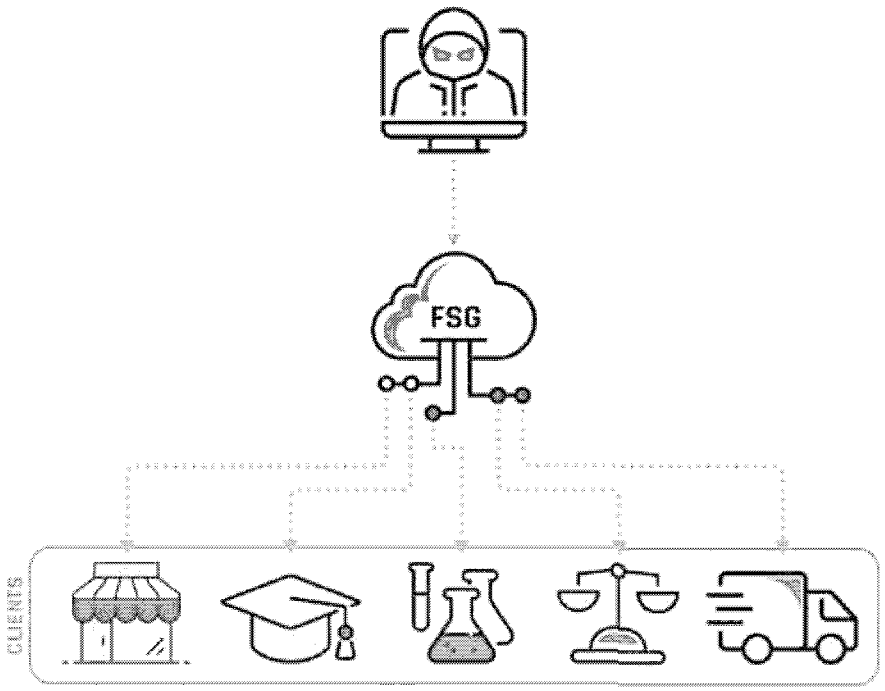


Exploitation de fournisseurs de services gérés

Un fournisseur de services gérés (FSG) est une entreprise utilisée par des organisations pour répondre à leurs besoins en TI et réduire les coûts associés au maintien de l'infrastructure et du personnel des TI en interne. Lorsqu'un réseau d'entreprise est bien protégé contre des attaques directes, les auteurs de cybermenace peuvent cibler les FSG pour avoir un accès indirect aux réseaux des clients. De plus, les auteurs de menace qui réussissent à compromettre un FSG peuvent atteindre un grand nombre de victimes, soit les clients de ce dernier.

Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les FSG allaient demeurer des cibles intéressantes pour les auteurs de cybermenace. Tout au long de l'année 2019, des cybercriminels ont compromis des FSG afin de tirer parti des logiciels de gestion à distance des systèmes de TI et installer automatiquement et simultanément des rançongiciels sur plusieurs réseaux de clients.[71] On s'attend à ce qu'au cours des deux prochaines années les campagnes de rançongiciel ciblent de plus en plus les FSG dans le but de compromettre leurs clients et d'accroître la portée de ces campagnes.

Figure 7 : Exploitation de fournisseurs de services gérés (FSG)



Les auteurs de menace ciblent les FSG en vue d'accéder à leurs clients (notamment les entreprises, les établissements d'enseignement et les autres institutions) sans avoir à compromettre chaque client directement.

CONCLUSION

Au Canada, le contexte des cybermenaces est en pleine évolution et les auteurs malveillants continuent d'adapter leurs activités en conséquence. La présente évaluation des cybermenaces nationales visait à relever les tendances actuelles et à faire le point sur l'évolution des activités de cybermenace auxquelles font face les entreprises et les citoyens canadiens. L'adoption par les Canadiens de nouvelles technologies et de nouveaux dispositifs connectés à Internet donnera certainement lieu à de nouvelles menaces.

Selon les observations consignées dans l'évaluation de 2018, il est possible d'atténuer plusieurs des cybermenaces grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de sécurité et de continuité des activités. De nos jours, les cybermenaces et les opérations d'influence sont souvent fructueuses, car elles ne reposent pas uniquement sur les vulnérabilités technologiques, mais exploitent des habitudes sociales et des comportements humains profondément ancrés. Pour défendre le Canada contre les cybermenaces et les opérations d'influence connexes, il faut se pencher sur les aspects techniques et sociaux des activités de cybermenace. Des investissements en cybersécurité permettront aux Canadiens de tirer avantage des nouvelles technologies tout en s'assurant qu'elles ne posent aucun risque sur le plan de la sécurité, de la protection de la vie privée, de la prospérité économique et de la sécurité nationale.

Le CCC s'est engagé à faire avancer la cybersécurité et à accroître la confiance des Canadiens dans les systèmes qu'ils utilisent au quotidien, en soutenant les réseaux des infrastructures essentielles et les autres systèmes qui sont importants pour le Canada.

Son approche collaborative en matière de sécurité permet de combiner l'expertise du gouvernement, du secteur privé et du milieu universitaire. En travaillant ensemble, nous rendrons le Canada plus fort et plus résilient face aux cybermenaces.

RESSOURCES UTILES

- Introduction à l'environnement de cybermenaces
- Pratiques exemplaires en cybersécurité
- Campagne Pensez cybersécurité
- Reconnaître les courriels malveillants
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage
- À bas l'arnaque – Protégez-vous contre la fraude
- Utilisation sûre des services bancaires en ligne
- Comment faire des achats en ligne en toute sécurité
- Utiliser son dispositif mobile en toute sécurité
- Application des mises à jour sur les dispositifs
- Pratiques exemplaires de création de phrases de passe et de mots de passe
- Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques
- Biométrie
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur
- Conseils de sécurité sur les gestionnaires de mots de passe
- Utiliser la technologie Bluetooth
- Intelligence artificielle
- Rapport conjoint sur les outils de piratage publiquement accessibles
- Protéger l'organisme contre les maliciels
- Rançongiciels : comment les prévenir et s'en remettre
- Protéger son organisation contre les attaques par déni de service
- Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer
- Utilisation de comptes personnels de médias sociaux au travail
- Utiliser un poste de travail virtuel à la maison et au bureau
- Les réseaux privés virtuels
- Conseils de cybersécurité pour le télétravail
- Conseils de sécurité pour les organisations dont les employés travaillent à distance
- Sécurité de l'Internet des objets pour les petites et moyennes organisations
- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations
- Facteurs à considérer sur le plan de la recherche et du développement
- La cybersécurité pour les organismes de santé : se protéger contre des cyberattaques courantes
- La COVID-19 et les sites Web malveillants
- Conseils ciblés sur la cybersécurité applicables durant la pandémie de COVID-19 : Liste des publications par public cible
- Avis et conseils en matière de cybersécurité à l'intention des organismes de recherche et de développement durant la pandémie de la COVID-19
- Bouclier canadien – Le Centre pour la cybersécurité fournit des renseignements sur les menaces afin de protéger les Canadiens pendant la pandémie de COVID-19

NOTES DE FIN DE TEXTE

[1] *BlueLeaks Data Breach Involved 38 Canadian Police Forces*, CBC News, 22 septembre 2020. https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311.

[2] *IoT Makes Industrial Manufacturers "Smart"*, PwC, (consulté le 15 juillet 2020). https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov/manufacturing-iot-snapshot.html.

[3] *Dossier documentaire sur Internet au Canada 2019*, Autorité canadienne pour les enregistrements Internet, 2019. https://www.cira.ca/fr/resources/corporation/dossier-documentaire/canadas-internet-factbook-2019.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 10 mai 2010. https://www150.statcan.gc.ca/n1/daily-quotidien/100510/dq100510a-fra.htm.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 10 novembre 2013. https://www150.statcan.gc.ca/n1/daily-quotidien/131126/dq131126d-fra.htm.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 29 octobre 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm.

[4] David Vigneault, *Allocution de David Vigneault au Economic Club of Canada*, Gouvernement du Canada, 4 décembre 2018. https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2018/12/allocution-pour-david-vigneault-au-economic-club-of-canada.html.

[5] *Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir*, Commissariat à la protection de la vie privée du Canada, 31 octobre 2019. https://www.priv.gc.ca/fr/blogue/20191031/.

[6] *Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019*, Commissariat à la protection de la vie privée du Canada, 11 mars 2019. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/

[7] *Cyper Operations Tracker*, Council on Foreign Relations, (consulté le 15 septembre 2020). https://www.cfr.org/cyber-operations/.

[8] *Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023*, Markets and Markets, septembre 2018. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html.

[9] *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware*, Département du Trésor des États-Unis, 5 décembre 2019. https://home.treasury.gov/news/press-releases/sm845; Tim Maurer, *Why the Russian Government Turns a Blind Eye to Cybercriminals*, Slate, 2 février 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html. *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, Département de la Justice des États-Unis, 16 septembre 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; *Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East*, Département de la Justice des États-Unis, 16 septembre 2020. https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[10] *Rapport Forum canadien sur la gouvernance de l'Internet 2019*, ACEI, 27 février 2019. https://canadianigf.ca/wp-content/uploads/2019/06/2019_CIGF_report_FR.pdf.

[11] Hascall Sharp et Oaf Kolkman. *Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T*, Internet Society, 24 avril 2020. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

[12] Jon Fingas, *China, Huawei propose internet protocol with a built-in killswitch*, Engadget, 30 mars 2020. https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

[13] Craig Silverman, *How to Spot a Deepfake Like the Barack Obama - Jordan Peele Video*, Buzzfeed News, 17 avril 2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed.

[14] *XR Belgium posts deepfake of Belgian premier linking COVID-19 with climate crisis*, The Brussels Times, 14 avril 2020. https://www.brusselstimes.com/all-news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/.

[15] *Enquête canadienne sur l'utilisation d'Internet*, Statistique Canada, 29 octobre 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm.

[16] *Dossier documentaire sur Internet au Canada*, Autorité canadienne pour les enregistrements Internet, 2019. https://www.cira.ca/fr/resources/corporation/dossier-documentaire/canadas-internet-factbook-2019.

[17] *The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.* International Data Corporation, 18 juin 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[18] Sawyer Bogdan, *Canadians have lost $43 Million to Cybercrime in 2019: OPP*, Global News, 24 octobre 2019. https://globalnews.ca/news/6077016/canadians-lost-43-million-cybercrime-2019/.

[19] *Fraudes par moyen utilisé*, Centre antifraude du Canada, 13 février 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-fra.htm

[20] *Fraudes par moyen utilisé*, Centre antifraude du Canada, 13 février 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-fra.htm

[21] John MacFarlane, *4.2 million Desjardins members affected by data breach, credit union now says*, CBC News, 1er novembre 2019. https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[22] Aidan Wallace, *Major Data Breaches in 2019*, Toronto Sun, 1er janvier 2020. https://torontosun.com/news/world/major-data-breaches-in-2019.

[23] Ken Hsu, Durgesh Sangvikar, Zhibin Zhang et Chris Navarrete, *Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices*, Palo Alto Networks: Unit 42, 24 juin 2020. https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/.

[24] *LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario*, CBC News, 17 décembre 2019. https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577.

[25] Maham Abedi, *Capital One data breach: here's what Canadians need to know*, Global News, 30 juillet 2019. https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/.

[26] Josh Fruhlinger, *Marriott data breach FAQ: How did it happen and what was the impact?* CSO Online, 12 février 2020. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

[27] Roberto Rocha et Jeff Yates, *Twitter Trolls Stoked Debates About Immigrants and Pipelines in Canada, Data Shows*, CBC News, 12 février 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[28] Reis Thebault, *A woman's stalker used an app that allowed him to stop, start, and track her car*, The Washington Post, 6 novembre 2019. https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/.

[29] *Tech Abuse and Empowerment Service*. Refuge, (consulté le 15 juillet 2020). https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/.

[30] *Vulnérabilités de cybersécurité associées à certains dispositifs médicaux dotés de puces Bluetooth Low Energy*, Santé Canada, 11 mars 2020. https://canadiensensante.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-fra.php.

[31] *Infrastructures essentielles du Canada*, Sécurité publique Canada, 19 mai 2020. https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/pci-iec-fr.aspx.

[32] Andy Greenberg, *The Highly Dangerous 'Triton' Hackers Have Probed the US Grid*, Wired, 14 juin 2019. https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[33] Andy Greenberg, *A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems*, Wired, 20 novembre 2019. https://www.wired.com/story/iran-apt33-industrial-control-systems/.

[34] *Top 2019 Cyber Attacks on ICS*, Waterfall Security, 19 décembre 2019. https://waterfall-security.com/top-2019-attacks-on-ics/.

[35] Joe Tidy, *How a Ransomware Attack Cost One Firm £45m*, BBC News, 25 juin 2019. https://www.bbc.com/news/business-48661152.

[36] Andy Greenberg, *Mysterious New Ransomware Targets Industrial Control Systems*, Wired, 3 février 2020. https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Nathan Brubaker, et. al. *Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families*, FireEye Threat Research, 15 juillet 2020. https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.

[37] *EKANS Ransomware and ICS Operations*, Dragos, 3 février 2020. https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[38] Ben Dooley et Hsako Ueno, *Honda Hackers May Have Used Tools Favored by Countries*, New York Times, 12 juin 2020. https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html.

[39] James Lewis, *Economic Impact of Cybercrime—No Slowing Down*, Center for Strategic and International Studies and McAfee, février 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

[40] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://www.bankinfosecurity.com/whitepapers/2019-internet-security-threat-report-w-5357.

[41] *Q1 2020 Ransomeware Marketplace Report*, Coveware, 29 avril 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[42] Ryan Flanagan, *Canadian Insurance Company Lost Nearly US$1M in Ransomware Attack*, CTV News, 30 janvier 2020. https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490.

[43] *Ransomware Payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020*, Coveware, 29 avril 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

[44] Catharine Tunney, *Ransomware Attack on Construction Company Raises Questions About Federal Contracts*, CBC News, 26 janvier 2020. https://www.cbc.ca/news/politics/ransowmare-bird-construction-1.5434308; *Time's Up for Agromart Group and their Data Got Leaked by REvil Ransomware Operators*, Cyble, Inc., 2 juin 2020. https://cybleinc.com/2020/06/02/times-up-for-agromart-group-and-their-data-got-leaked-by-revil-ransomware-operators/.

[45] David Burke, *Hospitals 'Overwhelmed' by Cyberattacks Fuelled by Booming Black Market*, CBC, 2 juin 2020. https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422.

[46] *Alerte : Cybermenaces pesant sur les organismes de santé canadiens*, Centre canadien pour la cybersécurité, 31 mars 2020. https://cyber.gc.ca/fr/avis/cybermenaces-pesant-sur-les-organismes-de-sante-canadiens.

[47] Catharine Tunney, *CSIS chief calls commercial espionage 'the greatest threat to our prosperity'*, CBC News, 4 décembre 2018. https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407/.

[48] *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, Département de la Justice des États-Unis, 20 décembre 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[49] Dustin Volz, *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets*, The Wall Street Journal, 5 mars 2019. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800.

[50] *Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités de cybermenaces*, Centre canadien pour la cybersécurité, 27 avril 2020. https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-incidence-de-la-covid-19-sur-les-activites-de.

[51] *Advisory: APT29 targets COVID-19 vaccine development*, National Cyber Security Centre, 16 juillet 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

[52] *What do Cybercriminals do with the Data They Steal?* Sysnet Global Solutions, (consulté le 10 juillet 2020). https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/.

[53] Scott Ikeda, *Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit*, CPO Magazine, 8 janvier 2020. https://www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/.

[54] Danny Palmer, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNet, 14 juillet 2020. https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[55] *2020 Data Breach Investigations Report*, Verizon, 2 juin 2020. https://enterprise.verizon.com/resources/reports/dbir/.

[56] Bruce Sussman, *BEC Scam Costs Canadian City $500k*, SecureWorld, 18 juin 2019. https://www.secureworldexpo.com/industry-news/canada-bec-scam-example.

[57] *The Sprawling Reach of Complex Threats: 2019 Annual Security Roundup*, Trend Micro, 25 février 2020. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats.

[58] *2019 Internet Crime Report*, Federal Bureau of Investigation, 11 février 2020. https://pdf.ic3.gov/2019_IC3Report.pdf.

[59] C. Steven Baker, *Is That Email Really From "The Boss"? The Explosion of Business Email Compromise (BEC) Scams*, The Better Business Bureau, septembre 2019. https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-explosion-of-bec-scams.pdf.

[60] *Behind the 'From' Lines: Email Fraud on a Global Scale*, Agari Cyber Intelligence Division, (consulté le 15 août 2020). https://www.agari.com/insights/whitepapers/behind-the-from-lines/.

[61] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[62] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[63] Jin Chen, Tao Yan, Taojie Wang et Zhanglin He. *Anatomy of FormJacking Attacks*, Palo Alto Networks, Unit 42, 27 avril 2020. https://unit42.paloaltonetworks.com/anatomy-of-formjacking-attacks/.

[64] Joseph Chen, *Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada*, Trend Micro, 3 mai 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[65] Aanand Krishnan, *Web scammers are using the COVID-19 crisis to attack your customers with Magecart and other client-side exploits*, Tala Security, 9 juin 2020. https://blog.talasecurity.io/web-scammers-are-using-the-covid-19-crisis-to-attack-your-customers-with-magecart-and-other-client-side-exploits/.

[66] Merna Emara, *Cybercrime Attacks on the Rise at North American Gas Stations, Warns Card Giant Visa*, National Post, 17 décembre 2019. https://nationalpost.com/news/world/cybercrime-attacks-on-the-rise-at-north-american-gas-stations-warns-card-giant-visa.

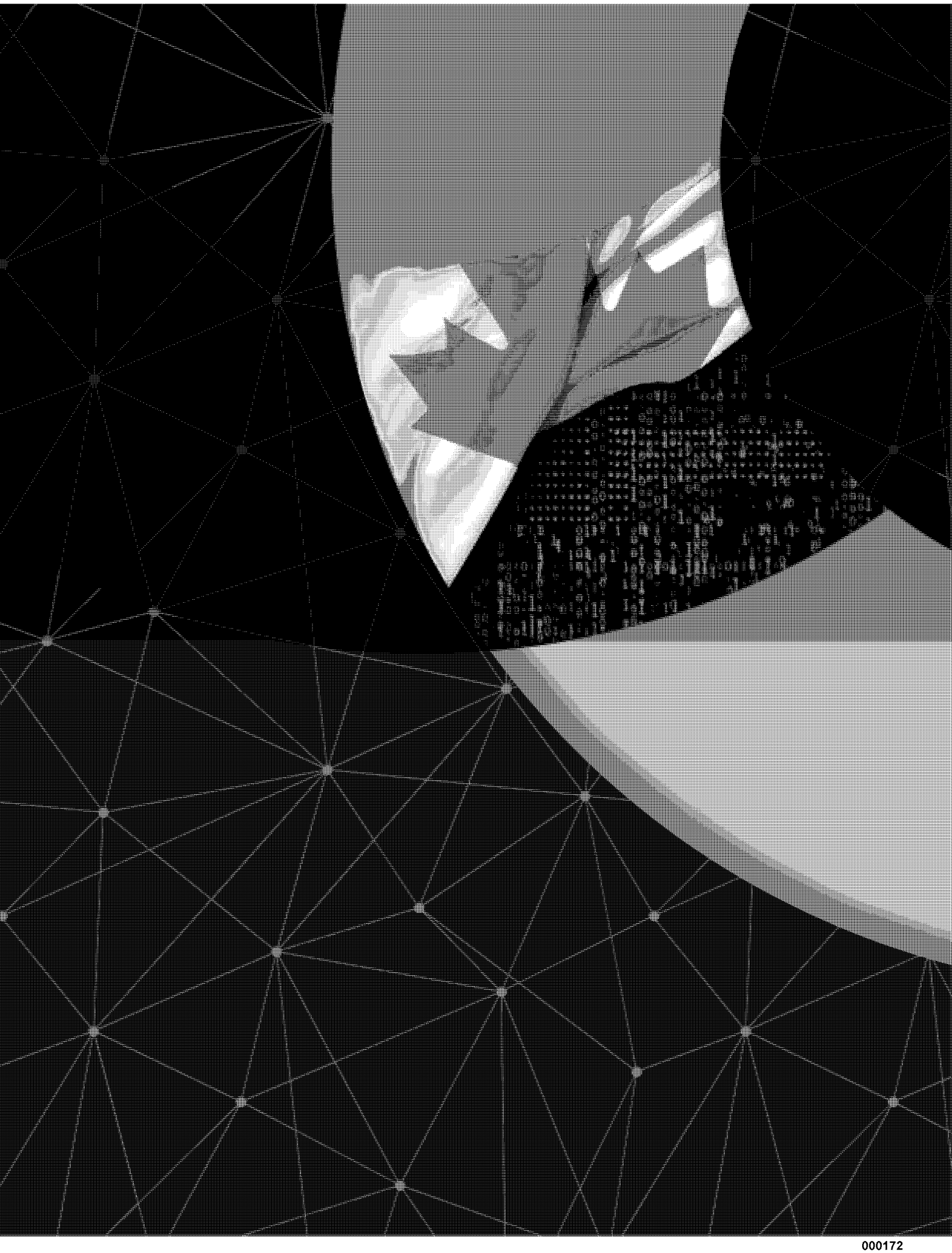
[67] Par chaîne d'approvisionnement, on entend un système d'organisations, de personnes, de technologies, d'activités, d'informations et de ressources permettant d'offrir un produit ou un service dans le cadre d'une relation fournisseur-client. Voir « Supply Chain Risk Management Practices for Federal Information Systems and Organizations. » National Institute for Standards and Technology, avril 2015. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

[68] Catalin Cimpanu, *FBI re-sends alert about supply chain attacks for the third time in three months*. ZDNet, 31 mars 2020. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/.

[69] Howard Solomon, *Canadian Organizations Among Victims of Global Attack on Healthcare-related Industries*, IT World, 24 avril 2018. https://www.itworldcanada.com/article/canadian-organizations-among-victims-of-global-attack-on-healthcare-related-industries/404475.

[70] Johannes B. Ullrich, *Kwampirs Targeted Attacks Involving Healthcare Sector*, SANS Internet Storm Center, 31 mars 2020. https://isc.sans.edu/forums/diary/Kwampirs+Targeted+Attacks+Involving+Healthcare+Sector/25968/?utm_medium=Social&utm_source=Twitter&utm_campaign=SANS+Central.

[71] Catalin Cimpanu, *GandCrab Ransomware Gang Infects Customers of Remote IT Support Firms*, ZDNet, 14 février 2019. https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/; Catalin Cimpanu, *Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems*, ZDNet, 20 juin 2019. https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/; Catalin Cimpanu, *Ransomware Hits Hundreds of Dentist Offices in the US*, ZDNet, 29 août 2019. https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.



Kopp, Ken

From: Kopp, Ken
Sent: November 26, 2020 12:38 PM
To: FPNS Secretariat / SNPF Secrétariat (RCMP/GRC); Gauvin, Brigitte; Dotzko, Chantale; Church, Glenn; Murphy, Nicole
Cc: Burchill, Richard; Efford, Sue
Subject: RE: FOR REVIEW: FYSA and/or additional input - Biden Admin Tasking - 10am tomorrow
Attachments: Ken Kopp suggestions PS-SP-#3698768-v1-Plnning_Eng_post-_U_S__Inauguration_2021_FPSDNSPOL_DRAFT_25112020.DOCX

FPNS Secretariat

I have added my suggestions for consideration to the attached document.

In case they are not easily readable my comments for #2 **In the first year of the Biden Administration, what are the new or high-level policy or operational activities that could be pursued?** Are below:

"Illegal" before harassment or intimidation

I suggest being more definitive in describing the threat by adding to the statement "… safeguard the economy from illicit interference and the protecting Canada's private and public technology from illegal acquirement". If we could add something about protection of Canada critical infrastructure is needed too but I realize there is a limit to the length of this paragraph.

Add multilateral and bilateral coordination or something to that effect as during previously work and discussions with the FBI there was a hesitancy to work multilaterally and primarily work bilaterally.

Thank you

Sgt. Ken Kopp
RCMP / GRC
Federal Policing National Security
Police fédérale Sécurité Nationale
M3 - 4- 616-95
73 Leikin Dr., Ottawa, ON K1A 0R2

Phone: 613-843-6569
cell:
email: ken.kopp@rcmp-grc.gc.ca

From: FPNS Secretariat / SNPF Secrétariat (RCMP/GRC) <RCMP.FPNSSecretariat-SNPFSecretariat.GRC@rcmp-grc.gc.ca>
Sent: November 26, 2020 9:16 AM
To: Gauvin, Brigitte <brigitte.gauvin@rcmp-grc.gc.ca>; Dotzko, Chantale <Chantale.Dotzko@rcmp-grc.gc.ca>; Church, Glenn <Glenn.Church@rcmp-grc.gc.ca>; Kopp, Ken <ken.kopp@rcmp-grc.gc.ca>; Murphy, Nicole <nicole.murphy@rcmp-grc.gc.ca>
Cc: Burchill, Richard <richard.burchill@rcmp-grc.gc.ca>; Efford, Sue <Sue.Efford@rcmp-grc.gc.ca>
Subject: FOR REVIEW: FYSA and/or additional input - Biden Admin Tasking - 10am tomorrow

Good Morning,

As per below, FP Strat is contributing to a document prepared by Public Safety to inform Minister Blair for his early conversations with the Biden Administration.

There are 2 sections drafted in the attached related to FAI and IMVE (in red). Can you please review these sections only and advise if you have any comments/input to the material drafted by FPSD.

The sections are limited, as the document covers a variety of topics.

DD for response is 10am tomorrow.

Thank you,

Leslie

>>> "Audette-Longo, Michael" <michael.audette-longo@rcmp-grc.gc.ca> 2020-11-26 8:54 AM >>>
Hello FPNS Secretariat,

FP received the following Tasking relating to a document being prepared by PS relating to a briefing package/deck for the Min of PS that will contribute to early conversations between Canada and the Biden admin. Multiple areas of FP have received this tasking, along with SPS and C&IP.

Please find attached in this email, FYSA, the input that Strat-Pol NS has drafted relating to FAI and IMVE. Our material's in red. If you have further input to add, please let me know and return back to me by **noon November 27, 2020.**

Thanks for your time today and if you have any questions please let me know,

Mike

Planning for Public Safety Portfolio Engagement Post-Inauguration

Please address the following questions to provide material aimed at briefing the Minister on the scope of opportunities with the incoming U.S. Administration:

1) **What are quick high-level wins/early asks the Public Safety Portfolio could put forward during first phone calls or first meetings with U.S. counterparts?** (Include a brief description)

   Some examples could include: EM/pandemic response, criteria for border reopening, health screening at POE, Cargo Preclearance

2) **In the first year of the Biden Administration, what are the new or high-level policy or operational activities that could be pursued?** (Include a brief description)

   Some examples could include: EM/pandemic response, response to HASA, research security, cybersecurity standards

   Foreign Actor Interference (FAI) continues to be a key consideration for a number of likeminded countries. Protecting democratic processes and diaspora communities from foreign actor-based harassment or intimidation; securing the health care supply chain, particularly when COVID-19 vaccines are distributed amongst populations; and safeguarding the economy and research efforts from national security threats are major concerns that thread through FAI. The coordination of efforts and sharing of best practices to protect against FAI and hostile activities by state actors in these realms will be an ongoing consideration for the foreseeable future. The Biden Administration would likely be interested in most, if not all, of these FAI/HASA-related concerns, including discussing or exploring ways to improve in this regard.

3) **What are the areas of policy or operational activities that could be pursued beyond the first year of the Biden Administration?** (Include a brief description)

   Some examples could include: countering illicit drug trafficking (incl. forensics on precursors, cross-border investigations), trafficking in person or combating irregular migration

4) **What are the active high-level irritants that U.S. counterparts may raise in first engagements?** (Include a brief description)

   Some examples could include: criteria for border reopening, 5G, information sharing on own citizens (incl. convicted sex offenders, immigration purposes)

5) **What are the areas of policy or operational divergence/potential conflict with an incoming Biden Administration?** (Include a brief description)

Commented [KK1]: "Illegal" before harassment or intimidation

Commented [KK2]: I suggest being more definitive in describing the threat by adding to the statement "... safeguard the economy from illicit interference and the protecting Canada's private and public technology from illegal acquirement". If we could add protection of Canada critical infrastructure is needed too would be good but I realize there is a limit to the length of this paragraph.

Commented [KK3]: Add Multilateral and bilateral coordination or something to that effect as during previously discussions there was a hesitancy to work multilaterally and only bilaterally. This is for consideration.

Some examples could include: approach to border reopening, 5G, national security transparency

6) **What are the most significant existing examples of successful policy or operational cooperation with the U.S.? Will the change in Administration have any impact?**

Biden Commitment Highlights

During the campaign Biden promised to: change immigration and border policies; reform law enforcement agencies' use of force tactics; explore decriminalizing marijuana; invest in cross-border infrastructure; and implement stricter firearms restrictions.

Border Innovation
It is expected that U.S. efforts on border innovation will continue as Biden is committed to investing in better technology both at and between ports of entry, including cameras, sensors, large-scale x-ray machines, and fixed towers. While it could provide opportunities to promote CBSA's Border of the Future and identify joint initiative, there could also be more pressure on Canada to invest more for upgrading/replacing aging infrastructure.

Climate Change and Emergency Management
As one of Biden's key priorities is to address Climate Change, there could be a shift in emergency management, focusing on climate change mitigation, unlike the current Trump Administration which focused on disaster response. Biden has committed to prioritizing disaster preparedness for disproportionately exposed, frontline, and vulnerable communities, including seniors, low-income families, and people with disabilities.

Cybersecurity
Biden announced "agency review teams" which for the security agencies include several cybersecurity experts. This may signals more top cybersecurity posts in government and a potential expansion of role of the director of the Cybersecurity and Infrastructure Security (CISA) including to insulate it from political influence. It is expected that a Biden Administration's cybersecurity priorities will include: election security; a tougher stance on Russian hacking and disinformation campaigns; continuing Trump policies to ban the Chinese telecom Huawei from building U.S. 5G networks; and limiting other Chinese companies access to U.S. key industry sectors.

National Security
No significant changes to the U.S. approach expected. Biden's Platform outlines actions to address violent extremism, home grown extremism and hate crimes (incl. right wing extremism). The Biden Administration is expected to leverage multilateral fora (e.g., Five Eyes) more.

The rise of racially and ethnically motivated violent extremism (REMVE), as well as anti-government/law enforcement extremist views, during the Trump era and the opposition that these groups hold towards the Biden Administration and Democrats in general, will likely augment interest in finding ways that Canada and the US can work together to address

Ideologically Motivated Violent Extremism (IMVE) in both countries. Further, it can be expected that these organizations will mobilize to combat policies being put forward by the Biden Administration in a similar manner to the Tea Party during the Obama Administration.

Cannabis / Drugs
Biden's commitments related to prevention, treatment and recovery efforts regarding substance use and the decriminalization of the use of cannabis will create good grounds for continued dialogue between Canada and the U.S. through existing fora on opioids and the North American Drug Dialogue.

Firearms / Gun Control
The Platform included ambitious gun control measures such as banning assault weapons and high capacity magazines, requiring background checks for all gun sales, and incentivizing more states to implement "red flag" laws. However, the new Administration may face challenges to deliver these commitments, should the Republican Senate majority hold. Nevertheless there might be opportunities for sharing info/data/research/best practices.

Police reform and racial justice
Biden's key priorities relate to investing in community-oriented policing, limiting use of force tactics, and addressing systemic misconduct in police departments. These appear to be more aligned with Canada's efforts on police and justice reform, and could provide opportunities to collaborate.

Regular/Irregular Migration
Biden's commitments include: revoking the Travel Ban; reinstating the Deferred Action on Childhood Arrivals (DACA) program; exploring a potential pathway to citizenship for some irregular arrivals; ordering an immediate review of Temporary Protected Status for vulnerable populations; reforming the visa program for temporary workers in select industries; and increasing the number of visas offered for permanent, work-based immigration based on macroeconomic conditions. Irregular migration and regular asylum claims via the U.S. could decrease and more migrants may seek to remain in the U.S., potentially reducing irregular and regular asylum claims across the border.

Pages 178 to / à 180

are not relevant

sont non pertinentes

Kopp, Ken

From: Kopp, Ken
Sent: March 8, 2021 1:17 PM
To: FPNS Secretariat / SNPF Secrétariat (RCMP/GRC)
Cc: Gauvin, Brigitte
Subject: FW: [DD to DCFP 2021-03-09] TASKING: For reply: Letter to NSERC - Canadian CC C-46 (2) (b)

FPNS Secretariat:

OIC FAI has approved the message below.

FAIT is in agreement with the assessment that at this time there is nothing for the RCMP to investigate.

FP Strat should be able to formulate a response that the RCMP takes allegations of Treason seriously and if I has specific information to please forward the information to the RCMP via National Security Information Network phone number 1-800-420-5805 or email address: RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Should you have any questions please contact Ken Kopp.

Thank you.

Sgt. Ken Kopp
RCMP / GRC
Federal Policing National Security
Police fédérale Sécurité Nationale
M3 - 4- 616-95
73 Leikin Dr., Ottawa, ON K1A 0R2

email: ken.kopp@rcmp-grc.gc.ca

From: Gauvin, Brigitte <brigitte.gauvin@rcmp-grc.gc.ca>
Sent: March 8, 2021 1:01 PM
To: Kopp, Ken <ken.kopp@rcmp-grc.gc.ca>
Subject: RE: [DD to DCFP 2021-03-09] TASKING: For reply: Letter to NSERC - Canadian CC C-46 (2) (b)

Good with that, Ken, thanks !

Brig

From: Kopp, Ken <ken.kopp@rcmp-grc.gc.ca>
Sent: March 8, 2021 10:28 AM
To: Gauvin, Brigitte <brigitte.gauvin@rcmp-grc.gc.ca>
Subject: RE: [DD to DCFP 2021-03-09] TASKING: For reply: Letter to NSERC - Canadian CC C-46 (2) (b)

Brig,

I am in agreement with the assessment that at this time there is nothing for the RCMP to investigate.

I believed Strat should be able to formulate a response that the RCMP takes allegations of Treason seriously and if has specific information to please forward the information to the RCMP via National Security Information Network phone number 1-800-420-5805 or email address: RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Do you wish me to forward up this response.

Ken

From: FPNS Secretariat / SNPF Secrétariat (RCMP/GRC) <RCMP.FPNSSecretariat-SNPFSecretariat.GRC@rcmp-grc.gc.ca>
Sent: March 8, 2021 9:33 AM
To: Kopp, Ken <ken.kopp@rcmp-grc.gc.ca>; Gauvin, Brigitte <brigitte.gauvin@rcmp-grc.gc.ca>
Subject: [DD to DCFP 2021-03-09] TASKING: For reply: Letter to NSERC - Canadian CC C-46 (2) (b)

Good Morning,

As per other emails/letters sent to the Commissioner's office , another email was referred to Federal Policing with a request to draft a response. In the circumstances that an investigation is not applicable (therefore no involvement required by FPNS) FP Strat is responsible for drafting a response letter on behalf of the DCFP.

Below is the email sent to the Commissioner – I have reviewed it and due to the fact that the complainant is making general statements regarding Huawei and not related to a specific incident, I don't feel there is anything for FPNS to investigate, therefore no file is required. Seeking your confirmation of same.

In support of FP Strat drafting a letter to the complainant on behalf of the DCFP, if there are any specific lines you feel should/could be in the letter, please send them my way!

Thanks,

Leslie

From: Nugent, Jason <Jason.Nugent@rcmp-grc.gc.ca>
Sent: March 5, 2021 10:28 AM
To: FPNS Secretariat / SNPF Secrétariat (RCMP/GRC) <RCMP.FPNSSecretariat-SNPFSecretariat.GRC@rcmp-grc.gc.ca>

s.19(1)

Cc: FPTASKING <FPTASKING@rcmp-grc.gc.ca>; Hiegel, Shannon <shannon.hiegel@rcmp-grc.gc.ca>; Russell, Jillian <Jillian.Russell@rcmp-grc.gc.ca>
Subject: [DD to DCFP 2021-03-09] TASKING: For reply: Letter to NSERC - Canadian CC C-46 (2) (b)

Good morning team,

After discussions with the Deputy's Office, they have instructed us to forward this particular tasking to your office to have a simple email reply drafted to

wrote to the head of NSERC (natural Sciences and Engineering Research Council of Canada) expressing concern that trading tech and money from NSERC to China may constitute treason and that it might warrant an investigation by the RCMP.

Full details from the incoming from are below – as well as the Commissioner's initial reply to

The Deputy's office has asked that a reply be drafted for the Deputy's signature by Tuesday, March 9th.

Thank you,

Jason Nugent
FP TASKING

From: Lucki, Brenda <brenda.lucki@rcmp-grc.gc.ca>
Sent: February 17, 2021 9:28 AM
To:
Subject: RE: Natural Sciences and Engineering Research Council of Canada

Thank you for your correspondence. I can assure you that the RCMP takes all matters that may affect Canada's national security seriously.

I have forwarded your message to the Deputy Commissioner responsible for Federal Policing for his attention and appropriate action.

Regards,

Commissioner/Commissaire
Brenda Lucki
Tel: 613-843-4590

Follow me on Twitter / Suivez-moi sur Twitter : @CommrRCMPGRC

s.19(1)

From:
Sent: February 16, 2021 2:05 PM
To: Lucki, Brenda
Subject: Natural Sciences and Engineering Research Council of Canada

Dear Commissioner Lucki,

I wrote today to the head of the NSERC to express my concern at the continuing pattern of technology and money transfer from that organization to China, and I write to you on the same issue as I believe it constitutes an offence under the Canadian Criminal Code of 1985:

C-46 (2) (b)

"Every one commits treason who, in Canada,

Without lawful authority, communicates or makes available to an agent of a state other than Canada, military or scientific information or any sketch, plan, model, article, note or document of a military or scientific character that he knows or ought to know may be used by that state for a purpose prejudicial to the safety or defence of Canada."

May I draw your attention to the phrase, "...or ought to know..." which in this instance appears particularily relevant given the common knowledge that your sister service CSIS has repeatedly warned the government of the dangers represented by the Chinese Communist Party and very specifically, Huawei.

I believe that there is here a case for investigation by the RCMP .

Yours most sincerely,

Pages 185 to / à 187

are duplicates

sont des duplicatas

Pages 188 to / à 194

are not relevant

sont non pertinentes