ISSN 2816-9182

CANADIAN CENTRE FOR
CYBER SECURITY

National Cyber Threat Assessment

2023 2024

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Communications Security Establishment
1929 Ogilvie Road
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISSN 2816-9182

© His Majesty the King in Right of Canada, as represented
by the Minister of National Defence, 2022

About the Cyber Centre

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's technical authority on cyber security. Part of the Communications Security Establishment (CSE), we are the single unified source of expert advice, guidance, services and support on cyber security for Canadians and Canadian organizations.

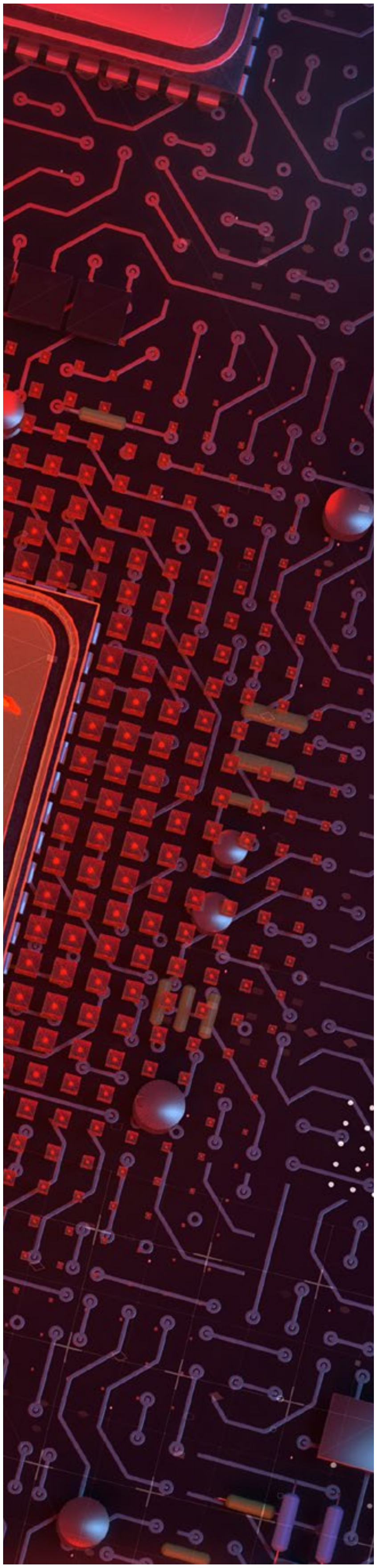
The Cyber Centre works in close collaboration with Government of Canada departments, critical infrastructure, Canadian businesses and international partners to prepare for, respond to, mitigate and recover from cyber events. The Cyber Centre is outward-facing, welcoming partnerships that help build a stronger, more resilient cyberspace in Canada. In line with the National Cyber Security Strategy,[1] the Cyber Centre represents a more cooperative approach to cyber security in our country.

As trusted experts in cyber security, we help keep Canada and Canadians safe by:

- being a clear, trusted source of relevant cyber security information for Canadians, Canadian businesses, and critical infrastructure owners and operators
- providing tailored 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, 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

Through our work and partnerships, we help raise Canada's cyber security bar so Canadians can live and work online safely and with confidence.

Learn more by visiting cyber.gc.ca[2] or follow us on
Twitter @cybercentre_ca.[3]



Minister's foreword

Over the last two years, cyber security has become a top concern for Canadians. Ransomware incidents hit the headlines on an almost daily basis both in Canada and around the world. Our essential services are being disrupted, from hospitals and schools to municipalities and utility providers. Our personal and financial data are being stolen, traded, or leaked online. Our online spaces are being flooded with false information and divisive rhetoric.

The National Cyber Threat Assessment 2023-2024 will help Canadians understand current cyber security trends, and how they are likely to evolve.

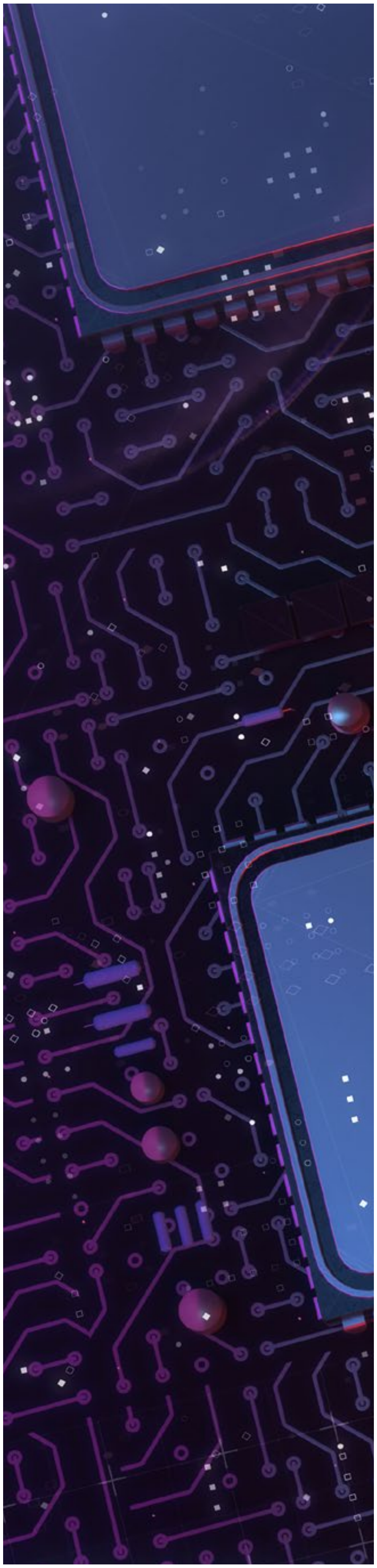
The Cyber Centre has provided an overview of the cyber threat landscape that is both thorough and accessible. The NCTA is especially helpful for Canadian decision-makers as the focus is on cyber threats most relevant to Canada. In addition to public reporting, the NCTA also benefits from CSE's classified sources and from the Cyber Centre's work defending the Government of Canada from malicious cyber activity day in day out. In short, this information is both credible and comprehensive.

As technology continues to accelerate with rapid speed, threats also continue to evolve. The Cyber Centre is working hard to bolster cyber security capabilities across Canada, in partnership with industry, academia and all levels of government.

It will take a coordinated effort to make Canada one of the safest places to live and work online. The Cyber Centre's work will protect Canadians and help ensure we are prepared to act, adapt, and react to cyber threats.

The Honourable Anita Anand
Minister of National Defence

Message from the Head of the Cyber Centre



Thank you for making cyber security a priority by reading this report.

If you have read either of our previous National Cyber Threat Assessments, published in 2018 and 2020, much of what you read here will seem familiar.

Cybercrime is still the number one cyber threat activity affecting Canadians. The state-sponsored cyber programs of China, Russia, Iran and North Korea continue to pose the greatest strategic cyber threat to Canada. Critical infrastructure is still a prime target for both cybercriminals and state-sponsored actors alike.

While it may be reassuring to know that our analysis of the key trends holds true, the overall picture of the threat landscape is anything but reassuring. You may be tempted to stop reading halfway through, disconnect all your devices and throw them in the nearest dumpster. Or perhaps, more realistically, to shrug your shoulders in resignation and carry on exactly as before. My hope is that instead, you will see this report as a call to action.

Canadians benefit greatly from living in one of the most Internet-connected nations in the world, and the cyber risks we identify in this report **can** be mitigated. In fact, the vast majority of cyber incidents can be prevented by basic cyber security measures.

To help bridge the gap between knowledge and action, we have prepared advice and guidance tailored to the five narratives identified in this report. These companion publications outline practical steps to mitigate the risks associated with each theme. Further advice and guidance[4] can be found on the Cyber Centre's website. And as ever, the Get Cyber Safe[5] website offers a wealth of simple and effective cyber security tips for individual Canadians.

Whether you are new to the topic, or a seasoned expert, I hope you find this report and the accompanying guidance helpful in taking the next step towards better cyber security.

Sami Khoury
Head, Canadian Centre for Cyber Security

Executive summary

Canadians use the Internet for financial transactions, to connect with friends and family, attend medical appointments and work. As Canadians spend more time and do more on the Internet, the opportunities grow for cyber threat activity to impact their daily lives. There's been a rise in the amount of personal, business and financial data available online, making it a target for cyber threat actors. This trend towards connecting important systems to the Internet increases the threat of service disruption from cyber threat activity. Meanwhile, nation states and cybercriminals are continuing to develop their cyber capabilities. State-sponsored and financially motivated cyber threat activity is increasingly likely to affect Canadians. In NCTA 2023-24, we have chosen to focus on five cyber threat narratives that we judge are the most dynamic and impactful and that will continue to drive cyber threat activity to 2024.

Key judgements

- **Ransomware is a persistent threat to Canadian organizations.** Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations. Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. Cybercriminals deploying ransomware have evolved in a growing and sophisticated cybercrime ecosystem and will continue to adapt to maximize profits.

- **Critical infrastructure is increasingly at risk from cyber threat activity.** Cybercriminals exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve. State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities, and as a form of power projection and intimidation. However, we assess that state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities.

- **State-sponsored cyber threat activity is impacting Canadians.** We assess that the state-sponsored cyber programs of China, Russia, Iran, and North Korea pose the greatest strategic cyber threats to Canada. State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these states. State actors can target diaspora populations and activists in Canada, Canadian organizations and their intellectual property for espionage, and even Canadian individuals and organizations for financial gain.

- **Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces.** We have observed cyber threat actors' use of misinformation, disinformation, and malinformation (MDM) evolve over the past two years. Machine-learning enabled technologies are making fake content easier to manufacture and harder to detect. Further, nation states are increasingly willing and able to use MDM to advance their geopolitical interests. We assess that Canadians' exposure to MDM will almost certainly increase over the next two years.

- **Disruptive technologies bring new opportunities and new threats.** Digital assets, such as cryptocurrencies and decentralized finance, are both targets and tools for cyber threat actors to enable malicious cyber threat activity. Machine learning has become commonplace in consumer services and data analysis, but cyber threat actors can deceive and exploit this technology. Quantum computing has the potential to threaten our current systems of maintaining trust and confidentiality online. Encrypted information stolen by threat actors today can be held and decrypted when quantum computers become available.

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[6] (NCTA 2018) and the National Cyber Threat Assessment 2020[7] (NCTA 2020), with analysis of the interim years and forecasts until 2024. We recommend reading the NCTA 2023-24 along with the updated Introduction to the Cyber Threat Environment[8] and the tailored advice and guidance that we have released as companions to this assessment.

As envisioned in the National Cyber Security Strategy,[9] we prepared this document to help Canadians shape and sustain our nation's cyber resilience. It is only when the government, private sector and public work together 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. Cyber security guidance[10] can be found on the Cyber Centre website and on the Get Cyber Safe website.[11]

Sources

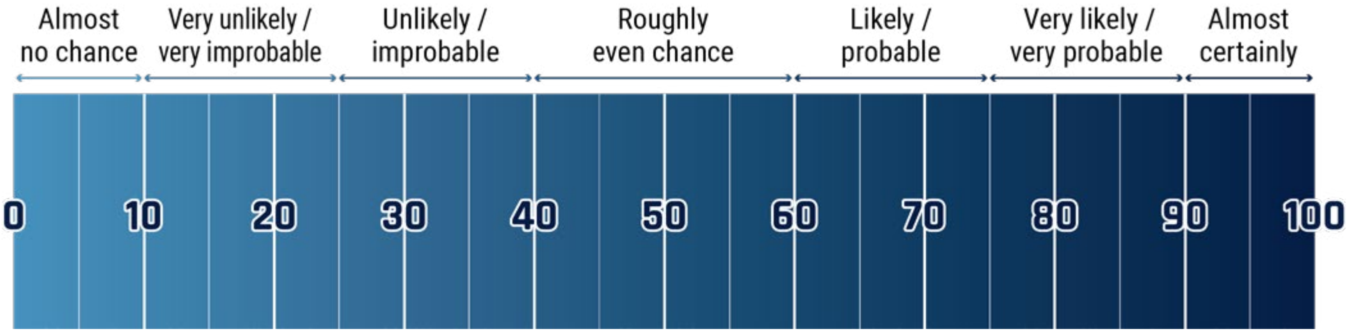
The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the Cyber Centre's knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective 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 4 October 2022.

Estimative language



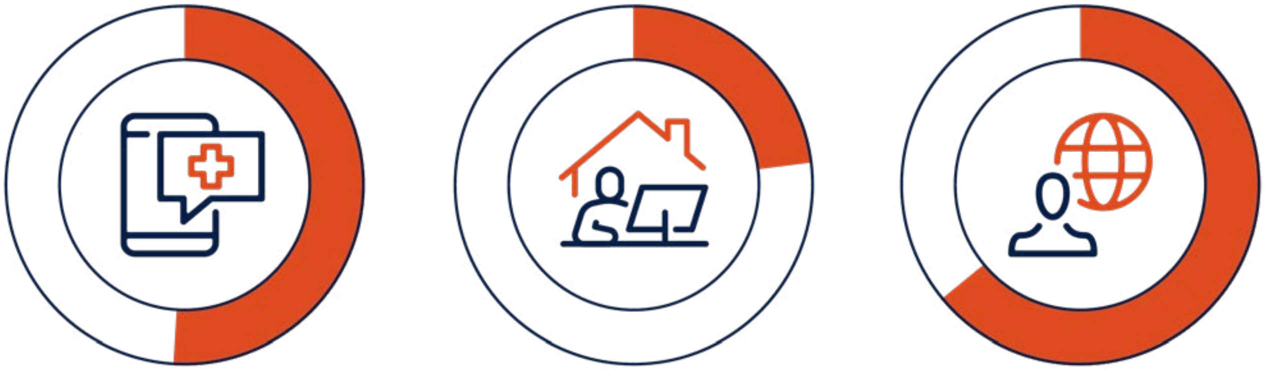
Introduction – Cyber threats are evolving

In previous editions of the National Cyber Threat Assessment (NCTA), we outlined the cyber threats faced by Canadian individuals, organizations, and critical infrastructure providers and assessed how they would evolve over the following years. Many of the threats that we identified remain relevant today, but the nature of these threats has changed. Threat actors have adapted their techniques, new technologies have spurred new cyber capabilities, and Canadians are using the Internet more and in novel ways.

COVID-19 and the cyber threat landscape

In 2020, we discussed how the COVID-19 pandemic quickly changed the cyber threat landscape. Over two years after the start of the pandemic, Canadians have a different relationship with the Internet. More people now use the Internet to shop, buy groceries, regularly connect with friends and family, attend medical appointments and work. Today, Canadians are working through a combination of in-person, virtual and hybrid means. Since 2020, more organizations have adopted cloud-based services to work efficiently in a hybrid environment.

Figure 1: COVID-19 has lasting impacts on how Canadians use the Internet[12]



Interacting online

Half (51%) of Canadians received medical care online for the first time since the pandemic began

Working online

23% of Canadians would be willing to work for an organization that doesn't allow employees to work remotely

Living online after the pandemic

Daily Internet use has increased since 2020, and **64%** don't plan to unplug more often

We judge that the threat surface available to malicious cyber actors has expanded since 2020. The amount of data collected on individual Canadians today is significant. It will only increase as new technologies enter the mainstream, creating a wealth of opportunities for threat actors looking to steal sensitive personal information. Moreover, the global threat landscape is changing as nation states increasingly use cyber activity as a tool for strategic competition and conflict.

To help Canadians gain a deeper understanding of the cyber threat landscape, we have also updated and expanded the Cyber Centre's Introduction to the Cyber Threat Environment.[13]

In this section we describe the trends driving today's cyber threat landscape and assess how we expect them to evolve.

Hybrid work and work-from-anywhere broadens the threat surface for individuals and organizations

More than one third of Canadians worked from home more often during the pandemic.[14] Now, more than two years on, many Canadians are transitioning to a more permanent hybrid work environment.[15] Securely implemented and maintained work-from-anywhere offers flexibility to employees and their employers, but it also creates a larger threat surface through which threat actors can access organizations' and individuals' networks or devices.

Business networks are becoming integrated into employees' homes and public spaces. We assess that cyber threat actors will very likely continue to exploit hybrid work infrastructure and target employees' home networks and personal devices to gain access to Canadian organizations. Cyber threat actors are taking advantage of organizations' remote accessibility, attempting to compromise corporate networks via remote connections.[16] When employees access corporate networks and information from their home networks and devices, they create opportunities for cyber threat actors to do the same. This allows them to access sensitive business or employee information.[17]

Faster, broader connections and more devices connected to the Internet

More Canadians are using Internet-connected technology for day-to-day interactions

Canadians have become more proficient Internet users, increasingly using the Internet for entertainment, information, work and social interactions.[18] Canadians are also becoming more widely connected as government initiatives extend reliable high-speed Internet to remote areas and new technologies, such as satellite Internet, ease the geographic element of the digital divide.[19] The COVID-19 pandemic has underscored the importance of accessible and reliable Internet connections. It made it necessary to move previously physical interactions online and required the quick adoption of technologies related to telework and education, contact tracing, and online retail and banking. The widespread adoption of contactless technologies for Canadians' day-to-day activities increases their exposure to cyber threat activity, such as data theft, fraud and extortion.

Internet-connected operational technology and smart systems expand the reach of cyber threat activity

The continued trend towards connecting devices that interact with the physical world, including deployment of Internet of Things (IoT) and Industrial IOT (IIoT) devices, is expanding the cyber threat surface. Their use will almost certainly grow as Canada fully adopts fifth generation cellular technology (5G). 5G provides significant improvements over 4G/LTE that will allow more devices to connect at much higher speeds. This has implications for smart cities, precision agriculture and other uses of "smart" systems such as applications that rely on sensors, automation and large amounts of data.[20] As Canada adopts smart systems and becomes more digitally transformed, more sectors and services will become vulnerable to cyber threat activity. This includes espionage, fraud, extortion and sabotage. Smart systems generate large amounts of data which, in certain applications, may include detailed personal information from users. As smart systems are incorporated into physical services and exposed to the Internet, the potential for service disruption from cyber threat activity increases.

Cybercrime represents a sophisticated threat to Canada

As we assessed in previous NCTAs, cybercrime remains the cyber threat that is most likely to affect Canadians. This is in part driven by a flourishing market for cybercrime tools and services readily available via online marketplaces and forums, or in private cybercrime communities. Such tools and services include initial network access, distributed denial of service (DDoS) attacks, web defacement tools, malware (including ransomware) and money laundering technologies. This allows cybercriminals to purchase specialized capabilities instead of developing their own skills over time. This lowers the barrier to entry for cybercriminals, enabling even unsophisticated threat actors to take advantage of more effective and specialized tools and services.

The availability and ease of access to leaked and stolen information like login credentials, financial information and personal information continues to grow on cybercrime forums.[21] This stolen data enables further cybercrime, including fraud, scams, and more disruptive cyber activity like ransomware. Ransomware is one of the most impactful cyber threats in Canada, benefiting significantly from the specialized cybercrime economy and the growing availability of stolen information. Cybercriminals leverage cryptocurrencies, use encrypted communications to maintain their anonymity and evade enforcement activity.[22] Cybercriminals are also quick to adopt and manipulate new technologies for their own gain. For example, cybercriminals have leveraged decentralized finance, which uses cryptocurrencies to enable large-scale borrowing and lending of funds without intermediaries, to steal large sums of money.[23] The significant payouts of cybercrime, including from ransomware and from fraud and scams such as business email compromise (BEC), will very likely continue to attract interest from new groups of criminal actors even as others are constrained by increased law enforcement activity.

Threat actors are attacking targets indirectly, exploiting vulnerabilities in supply chain and Internet infrastructure

Instead of targeting organizations directly, cyber threat actors are increasingly targeting the software tools and services used by organizations via supply chain compromises. The threat from supply chain compromises increases where vendors have elevated access to their clients' networks. This kind of relationship is becoming more common as cloud-based software, infrastructure, and platform "as-a-service" models proliferate. By spreading malware through a vendor's updates and services, cyber threat actors introduce vulnerabilities on the vendor's clients' networks. Supply chain compromises tend to be more complex than direct compromises. As such, we assess they will very likely remain a tool primarily for state-sponsored threat actors and sophisticated cybercriminals.

Cyber threat actors are also exploiting weaknesses in code that is widely used across the Internet and in software development. Web services and computer applications often rely on open-source code maintained by third parties. When vulnerabilities are found in common third-party code, any project using that code is vulnerable. For applications such as Log4J, a popular open-source software with a vulnerability disclosed in late 2021 and exploited widely by cyber threat actors, the impact can be pervasive.[24] In just the four months prior to the exploit becoming widely known, Log4J was downloaded over 28 million times.[25] The exploit, Log4Shell, was made publicly available, providing cyber threat actors broad access to the tools to compromise any service using Log4J.[26]

We assess that vulnerabilities in common services and software components will almost certainly continue to be discovered and exploited by threat actors at scale. We also assess that, even after patches are developed, threat actors will almost certainly continue to scan the Internet to opportunistically target unpatched systems.

Geopolitical competition in cyberspace puts everyone at risk

Nation states use malicious cyber activity as a tactic for subversion and power projection to achieve their geopolitical goals. Malicious cyber threat activity by state-sponsored cyber threat actors has become an important tool for states to influence events without reaching the threshold of conflict and to support conventional warfare.

Canadian critical infrastructure is almost certainly targeted by malicious cyber activity from nation state-backed cyber actors. While we maintain that state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities, these actors are developing the ability to disrupt the critical systems of Canada and our allies. If carried out, this activity can have significant implications for Canadians' ability to communicate and receive essential goods and services. Likewise, state-sponsored cyber threat actors proliferate misinformation, disinformation, and malinformation (MDM) to influence international populations and exploit social divisions.[27] This activity serves to justify or build support for states' ideological goals, impact international discourse related to current events, or build mistrust to weaken Canadian democratic institutions.

RUSSIA'S INVASION OF UKRAINE – A NEW PERSPECTIVE ON CYBER

Russia's invasion of Ukraine in February of 2022 gave the world a new understanding of how cyber activity is used to support wartime operations. Russian-sponsored malicious cyber activity against Ukraine has disrupted or attempted to disrupt organizations in government, finance and energy, often coinciding with conventional military operations. These attacks have expanded beyond Ukraine to implicate European critical infrastructure as well. For example, Russia's attack on a European satellite Internet provider that resulted in a significant outage in several European countries.[28] Cyber and military activities have also been supported by coordinated disinformation operations to support Russia's narrative about the invasion.[29]

The global Internet continues to diverge

In NCTA 2020, we described how nation states are developing competing standards and norms governing the flow of information on the Internet. One approach, which focuses on state sovereignty, sees online information primarily through the lens of stability and national security and promotes an Internet that will allow states to track their citizens and censor information. Using the Internet to censor and monitor populations threatens the openness, transparency, and multi-stakeholder approach to the Internet that Canada and its allies champion. Yet, an increasing number of states are managing their domestic Internet in this way. In 2021, AccessNow reported that 34 countries used Internet shutdowns as a tool to suppress social or political unrest or control the flow of information during elections and in conflict.[30] Freedom House estimates that 56% of the world's Internet users live in countries where political, social, or religious content was blocked online.[31]

Over the next two years, it is very likely that the divergence between an open and transparent Internet and an Internet based on state sovereignty will continue to grow. Russia and China have invested in their own Internet infrastructure and, alongside other states, are advocating for information and communications technology standards. These would allow more state-led control of the Internet in their respective countries.[32] In 2022, China introduced a new international organization evolving from the World Internet Conference dedicated to Internet governance and comprised of members from 20 countries.[33] While Internet governance may appear abstract and quite removed from daily life, we judge that competing technological ecosystems and disparate information environments inhibit the free flow of information, build distrust, and make it more difficult to combat misinformation and disinformation.

Ransomware is a persistent threat to Canadian organizations

As we assessed in previous NCTAs, cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations. Fraud and scams are almost certainly the most common form of cybercrime that Canadians will experience over the next two years as threat actors attempt to steal personal, financial, and corporate information via the Internet. Fraud and scams, including malicious cyber threat activity such as phishing, result in significant financial losses. According to the Canadian Anti-Fraud Centre, there have been over 150,000 reports of fraud in Canada with over $600 million stolen since January 2021.[34]

Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. Aside from the financial cost of the ransom itself, ransomware can stop the operation of important systems, damage or destroy an organization's data, and reveal sensitive information. This is in addition to imposing costs and time to recover from an attack. The disruption caused by a ransomware attack can prevent access to essential services and, in some cases, threaten Canadians' physical safety.

Ransomware almost certainly has more impact on Canadian organizations today than it did in 2020. Since 2020, the frequency of ransomware attacks worldwide has increased, and payment demands against large organizations have grown.[35]

Ransomware enables other malicious cyber threat activity

Ransomware is malicious software that restricts access to or operation of a computer or device, potentially restoring it following payment. Typically, threat actors will compromise a victim, encrypt their data, and demand a ransom to provide a decryption key. Today, most ransomware attacks are double extortion attacks. This means that ransomware actors will exfiltrate files before encrypting them and threaten to leak sensitive information publicly if the ransom is not paid.[36]

Beyond the impact of ransomware itself, data stolen during a ransomware attack almost certainly enables further cyber threat activity from a range of actors. Leaked information often contains sensitive personal and business information that can be accessed freely on the ransomware actors' websites or sold to a buyer, either privately or on online cybercrime marketplaces.[37] Other threat actors can use this information to enable further cybercrime activity, such as identity fraud against individuals or even additional ransomware. Threat actors can also leverage sensitive business information to support commercial espionage. In May 2022, a Canadian defence company confirmed in media reporting that it was investigating a possible ransomware incident.[38] Given the sensitive nature of the organization's data, this information would likely be of interest to other threat actors for espionage or to enable further cybercriminal activity.

Ransomware affects critical infrastructure

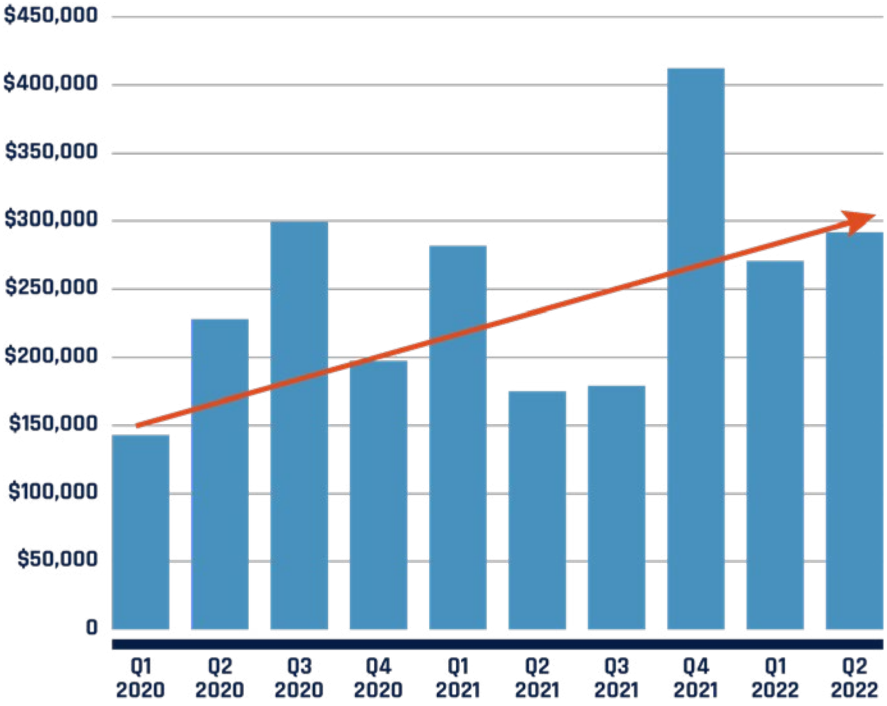
Critical infrastructure is a particularly attractive target for ransomware. As we note when discussing threats to critical infrastructure, these organizations are perceived by cybercriminals to be more willing to pay significant ransoms to limit or avoid physical disruption and impacts to their customers. Ransomware incidents in May 2021 against Colonial Pipeline in the United States (US) and the North American and Australian operations of JBS Foods resulted in multimillion-dollar payouts for threat actors. These incidents caused significant disruptions to fuel and food supply chains.[39]

In Canada, a ransomware attack resulted in a loss of essential services at an Ontario hospital in June 2021. In October 2021, due to some of their servers being encrypted and locked, a municipal transit service was unable to share route and scheduling information.[40] The Cyber Centre is aware of reported ransomware activity against several industries in Canada since 2020, including most of Canada's critical infrastructure sectors. While critical infrastructure and large enterprises are attractive targets, cybercriminals are opportunistic and will almost certainly not limit their activities to those sectors in Canada over the next two years.

The impact of ransomware

Cyber security reporting indicates that ransom payments have increased since 2020, likely driven in part by increasingly significant demands against large enterprises.[41] Even if victims choose to pay the ransom, there are no guarantees that their data will be recovered. One survey of Canadian businesses found that only 42% of organizations who paid the ransom had their data completely restored.[42] The ransom value often represents only a portion of the total cost to the organization. Lost value associated with downtime or unrecoverable data, costs of repairing systems, and reputational damage are just some of the additional costs that can be imposed by ransomware.

Figure 2: Average ransomware payments since 2020 (Data from Coveware converted from USD to CAD)[43]



LAW ENFORCEMENT ACTION AGAINST CYBERCRIMINALS USING RANSOMWARE

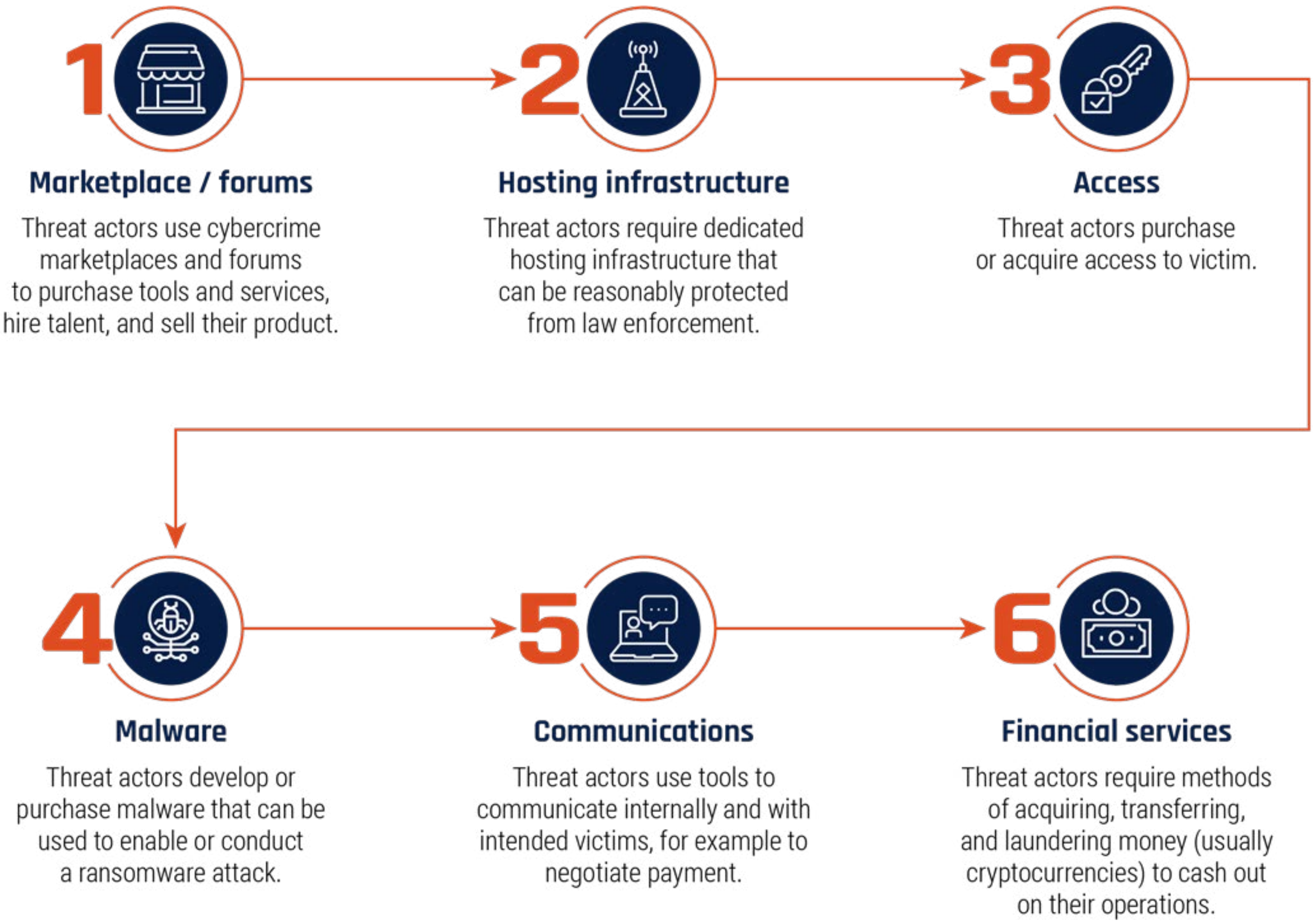
In May 2021 and again in early 2022, the Cyber Centre observed a decrease of ransomware incidents against Canadians. We assess this was likely a result of threat actors seeking to avoid law enforcement attention directly following international action.

While law enforcement action almost certainly disrupts cybercriminal operations, we judge that these disruptions rarely have an enduring effect on the ransomware environment. Weeks after Russia's arrest of 14 individuals associated with a prominent ransomware gang in early 2022, cyber security researchers observed the ransomware group back up in operation.[44]

Ransomware-as-a-service has made ransomware more accessible and profitable

Much of the ransomware affecting Canadians is very likely owned by ransomware-as-a-service (RaaS) cybercrime groups. These groups create and maintain ransomware variants and sell access to other cybercriminals who deploy the ransomware against a victim. Ransomware-as-a-service groups request upfront payment, subscription fees, a cut of profits, or all three in exchange for access to their ransomware.[45] We judge that this service model lowers the barrier to entry for cybercriminals, making it easier for less-sophisticated cyber threat actors to access ransomware capabilities and extort victims.

Figure 3: The Ransomware-as-a-service supply chain



1 **Marketplace / forums**

Threat actors use cybercrime marketplaces and forums to purchase tools and services, hire talent, and sell their product.

2 **Hosting infrastructure**

Threat actors require dedicated hosting infrastructure that can be reasonably protected from law enforcement.

3 **Access**

Threat actors purchase or acquire access to victim.

4 **Malware**

Threat actors develop or purchase malware that can be used to enable or conduct a ransomware attack.

5 **Communications**

Threat actors use tools to communicate internally and with intended victims, for example to negotiate payment.

6 **Financial services**

Threat actors require methods of acquiring, transferring, and laundering money (usually cryptocurrencies) to cash out on their operations.

Cybercriminals will continue to adapt their methods to maximize profits

So long as ransomware remains profitable, we will almost certainly continue to see cybercriminals deploying it. A combination of permissive state attitudes, particularly in Russia, towards cybercrime that targets victims outside of the Former Soviet Union countries and an available talent pool of cybercriminals facilitates the growth and development of criminal organizations dedicated to developing and deploying ransomware. Cyber threat actors also demonstrate flexibility and leverage the ransomware supply chain in new ways to ensure that their operations remain feasible. For example, media and vendor reporting indicates that some ransomware operators are transitioning to using privacy coins (cryptocurrencies that provide higher levels of anonymity) to hide their activity more effectively, although Bitcoin remains the most common ransomware payment method.[46]

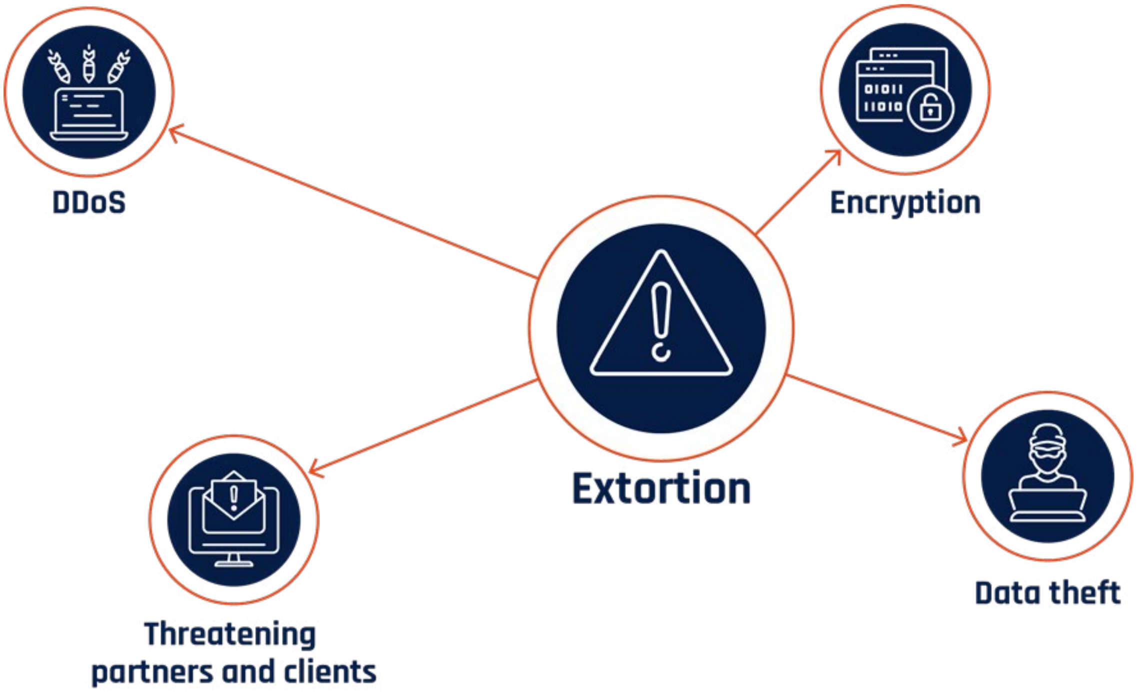
Targeting supply chains and Managed Service Providers

Cybercriminals will almost certainly continue to target Managed Service Providers (MSP), companies that host and manage their clients' IT resources, and software supply chains to maximize the reach of ransomware operations. In 2021, media reports indicated that cybercriminals compromised and spread ransomware via Kaseya's Virtual System Administrator, a system used by MSPs to manage their clients' networks. Cybercriminals were able to distribute the ransomware to approximately 60 MSPs and 1,500 of their clients.[47]

Methods of extortion are evolving

We assess that over the next two years, cyber threat actors will very likely use a variety of extortion techniques against their victims to maximize their chance of receiving payment. Beyond encrypting systems and stealing data, in some instances ransomware operators will likely use additional techniques, such as threatening an organization's partners or clients and distributed denial of service (DDoS). By threatening the business partners or clients of a victim, cybercriminals very likely anticipate that these organizations will increase pressure on the victim to pay the ransom, fearing that their sensitive business information or operations are in the hands of the threat actor.[48] DDoS places additional pressure on a victim by adding another layer of disruption to the organization's network. One cybercriminal group, which has targeted victims in Canada, has conducted DDoS attacks during payment negotiations.[49] While multiple extortion attacks are common, some cyber threat actors are moving away from the traditional encryption of victims' systems to focus solely on other single-extortion methods.[50]

Figure 4: Ransomware extortion methods



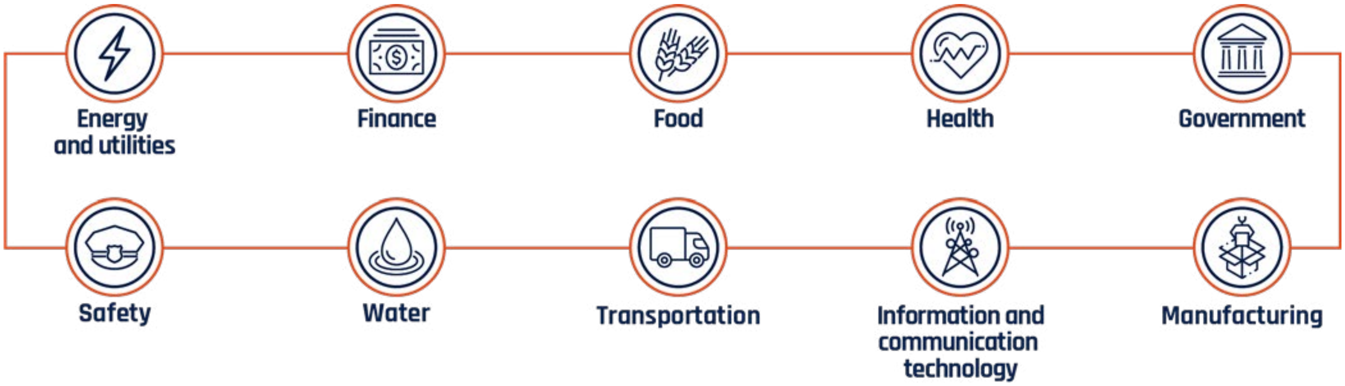
Critical infrastructure is increasingly at risk from cyber threat activity

Critical infrastructure underpins many of the services Canadians use every day. When service interruptions occur, the impacts can be significant. While not linked to malicious cyber activity, cellular and Internet outages in Canada in 2021 and 2022 illustrated the importance of connectivity and the interconnectedness between critical infrastructure sectors.[51] In addition to the impacts to individuals, the outages impacted payment processing and emergency safety lines.[52] The opportunities for critical infrastructure disruption expand as operators increasingly expose the operational technology (OT) underpinning industrial processes to the Internet. Internet-connected OT increases the threat surface of the organizations that employ it and increases the opportunity for cyber threat activity to have effects in the physical world.

Cyber threat actors are aware of the impact targeting critical infrastructure can have, exploiting their sensitivity to service interruptions to extort them for ransom. State-sponsored cyber threat actors target critical infrastructure to collect information through espionage, pre-position in case of future hostilities, and as a form of power projection and intimidation. However, we assess that state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities.

Critical infrastructure providers house large amounts of sensitive or valuable information that can be targeted by cyber threat actors, including intellectual property on the design and maintenance of OT and personal information the provider may have collected from consumers. Sensitive information may also be revealed incidental to financially motivated cyber threat activity. Researchers suggest nearly 1 in 7 ransomware attacks against critical infrastructure where information is stolen and released reveals sensitive information about OT.[53] Technical information on OT can be used by threat actors to plan future threat activity or can be valuable for sale or as a target for commercial espionage.

Figure 5: Critical infrastructure sectors[54]

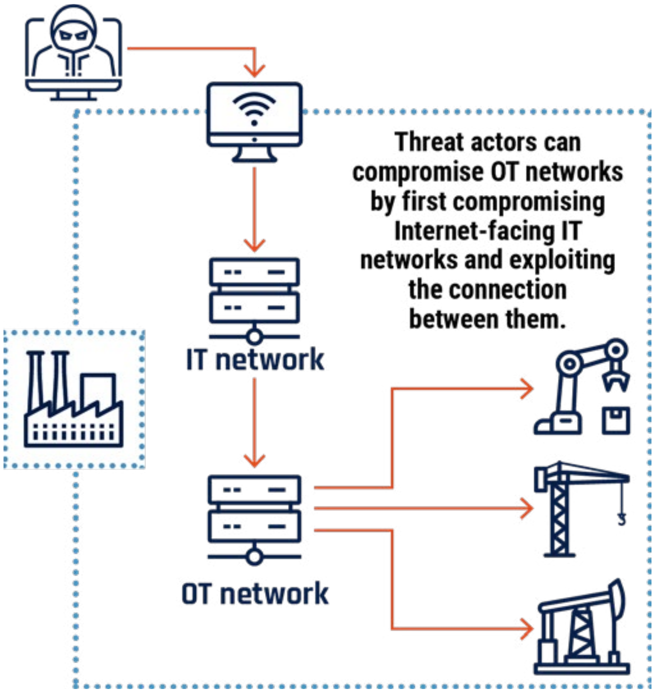


Connected OT increases critical infrastructure's cyber threat surface

In NCTA 2020, we described how OT, which is used to control and monitor physical processes, is increasingly being connected to information technology (IT) by industry and critical infrastructure providers. Connected, or smart, OT increases process efficiency through improved data exchange, centralized management, and automation. The global market for smart OT in 2020 was about $280.05 billion CAD and is expected to grow to over $1 trillion CAD in the early 2030s.[55] This is in addition to the overall trend towards digitization across all industries to account for the challenges of the COVID-19 pandemic.[56] The adoption of connected OT has been accelerated by improvements in technology making it even easier to connect devices remotely and at scale, including 5G and satellite Internet infrastructure. While connecting OT brings many benefits, it also increases critical infrastructure providers' vulnerability to cyber threat activity.

Connecting OT to an Internet-connected IT network provides a pathway for threat actors to access and disrupt sensitive OT devices and processes. Threat activity against the IT network can have incidental effects on the OT network. Operators may shut down OT processes out of caution, or IT malware may accidentally spread and affect OT.[57] We are also observing an increase in use of malware that directly targets and disables OT. Cybercriminals have deployed OT-specific ransomware, and state-sponsored actors have demonstrated the capacity to deploy malware against critical infrastructure to degrade its performance and damage OT and IT assets.[58] Russian state-sponsored threat actors have been particularly active in developing and testing these capabilities against their neighbours, including against NATO member states.[59]

Figure 6: OT compromise through IT networks

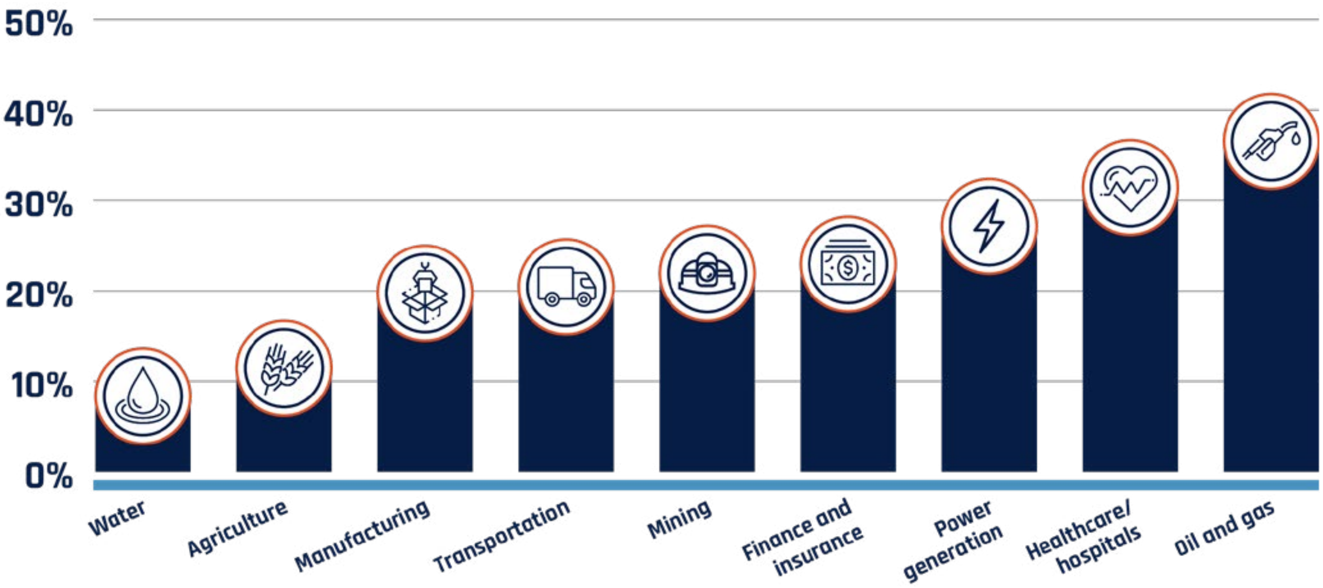


Threat actors can compromise OT networks by first compromising Internet-facing IT networks and exploiting the connection between them.

Critical infrastructure depends on its supply chain

Critical infrastructure providers, especially energy and utilities, are reliant on their vendors and suppliers for expertise and equipment as they operate, maintain, and modernize their OT processes. We assess that this makes them particularly vulnerable to supply chain compromises, where cyber threat actors first compromise a vendor and use that access to compromise one or more of their clients. Cyber threat actors target critical infrastructure supply chains for two purposes: to steal intellectual property and information about the OT deployed by a critical infrastructure provider and to obtain indirect access to networks.

Figure 7: Percentage of CI sectors reporting a cyber incident (2019)[60]



Cybercriminals target critical infrastructure

Financially motivated cyber threat actors, predominantly cybercriminals, exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve. Cybercriminal activity against critical infrastructure can interrupt operations that support essential services, utilities, and the production of important goods, including food, fuel and medical equipment in support of their extortion demands.

For the healthcare sector in particular, the impacts of cybercriminal activity can be significant.[61] Since March 2020, over 400 healthcare organizations in Canada and the United States experienced a ransomware attack.[62] In 2021, a cyber incident heavily impacted Newfoundland and Labrador's healthcare system, disrupting medical services in their entire Eastern Health region.[63]

We have also observed an increase in threat activity against municipal and provincial governments.[64] The Cyber Centre is aware of over 100 cases of cyber threat activity targeting Canadian municipalities since the beginning of 2020. Most cases involved social engineering, unauthorized network access or the deployment of malicious code, such as ransomware. Compromises against any level of government can implicate residents' personal information, service continuity, and trust in the compromised institutions.[65]

State-sponsored actors targeting critical infrastructure

State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities and as a form of power projection and intimidation. In previous NCTAs, we assessed that state-sponsored actors were very unlikely to intentionally disrupt Canadian critical infrastructure. Over the next two years, we assess that this will very likely remain true in the absence of direct hostilities with Canada. The invasion of Ukraine has demonstrated that Russia is increasingly willing to use cyber activity against critical infrastructure as a foreign policy lever. The Cyber Centre issued cyber threat bulletins in 2022 advising of foreign cyber threat activities, including by Russian state-sponsored threat actors, targeting Canadian critical infrastructure network operations and OT.[66]

NEWFOUNDLAND AND LABRADOR HEALTHCARE COMPROMISE

The Newfoundland and Labrador healthcare system was paralyzed on October 30, 2021, when cybercriminals compromised its networks. Healthcare providers could not access internal communications or diagnostic information, forcing them to adopt a paper-based approach to appointments and emergency procedures. Thousands of medical procedures and appointments were delayed. In addition to service disruptions, sensitive information pertaining to thousands of staff and patients was stolen.[67]

State-sponsored cyber threat activity is impacting Canadians

We assess that the state-sponsored cyber programs of China, Russia, Iran, and North Korea continue to pose the greatest strategic cyber threats to Canada. State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these specific states. These campaigns target Canada for a variety of reasons, including our association with groups such as NATO and the G7. While state-sponsored cyber activity targets Canada directly, our high degree of global connectivity and technological integration with our allies also increases our threat exposure. Malicious cyber threat activity sponsored by states almost certainly impacts Canadian individuals and organizations, whether they are the intended targets or not.

Foreign states are targeting Canadian individuals

Targeting diaspora populations and activists in Canada

Adversary states are interested in monitoring and disrupting the activities of individuals who they believe threaten their domestic security and stability. State-sponsored cyber threat actors almost certainly target foreign nationals, diaspora groups, activists, and journalists to monitor and control these individuals. This activity likely threatens individuals' safety and security, in addition to increasing distrust and polarization in Canadian society.

We assess that threat actors are almost certainly using cyber tools against these populations in Canada.This activity takes several forms, including content monitoring on foreign-based applications, social media-enabled activity and espionage against individuals using spyware. We assess that Chinese, Iranian, and Saudi Arabian state-sponsored cyber threat actors have almost certainly monitored diaspora populations and activists abroad using a combination of these means.[68] We judge it very likely that these cyber threat actors are targeting these individuals in Canada.

According to reporting from The Citizen Lab at the University of Toronto, a research organization focusing on cyber security and human rights, cyber threat activity targets activists in Canada through disinformation or intimidation on social media, denial of service attacks against their organizations, and compromise of their personal devices.[69]

Spyware tools used by cyber threat actors to compromise a personal device can be highly sophisticated, with some providing access to an individual's personal device without requiring them to click on a malicious link or open a malicious attachment.[70]

Beyond cyber threat activity against individuals, states very likely use foreign-based social media and messaging applications popular with diaspora groups in Canada and around the world to monitor communications. States take advantage of permissive terms of use and their own legislative powers to compel data sharing.[71] This activity threatens the privacy of the communities using these applications.

COMMERCIAL CYBER TOOLS AND SERVICES ON THE RISE

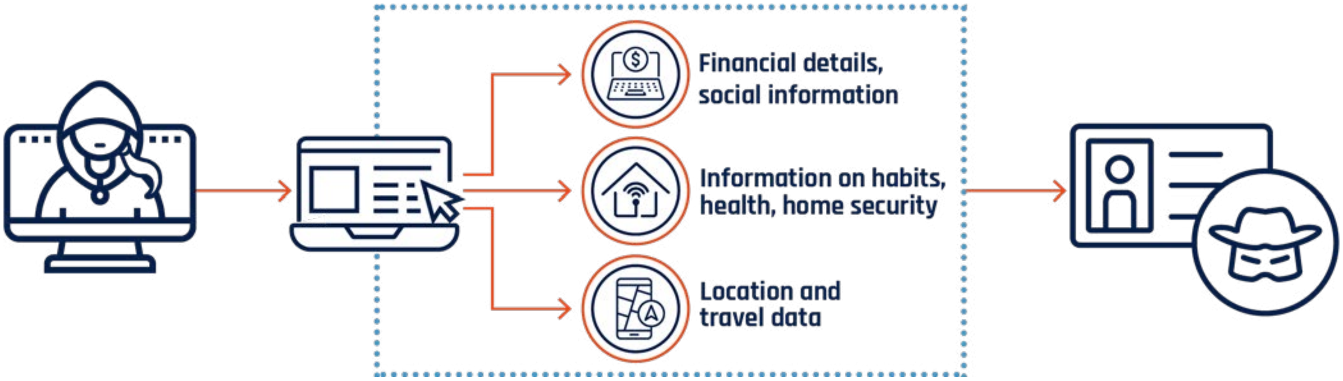
Nation states without sophisticated cyber capabilities can purchase tools and services from commercial providers. We assess that foreign governments are almost certainly leveraging commercial software, such the NSO Group's Pegasus spyware, to monitor dissidents, activists, journalists, and diaspora groups. Foreign governments have almost certainly used these commercial tools against Canadians and groups of interest inside Canada.

Targeting the personal information of Canadians

In NCTA 2020, we discussed how state-sponsored cyber threat actors target large databases of personal information and use data science to identify, profile, and track individuals, likely enabling further cyber threat activity. As the amount of personal information online increases, it becomes easier for threat actors to collect and analyze information. When data is transmitted through or stored on a server physically located in a foreign state, that state can more easily compel private organizations to supply this data, threatening the privacy of Canadians.[72] The interconnected nature of communications technology and data processing means that, without appropriate safeguards, Canadians' personal information can be compromised when cyber threat actors compromise foreign entities.[73]

Figure 8: How large datasets/personal information can be used by cyber threat actors

Online services often collect personal information from their users to function. When personal information is exposed through data breaches or willingly released by the user, it can be used by cyber threat actors to facilitate identity theft or targeted fraud against the user.

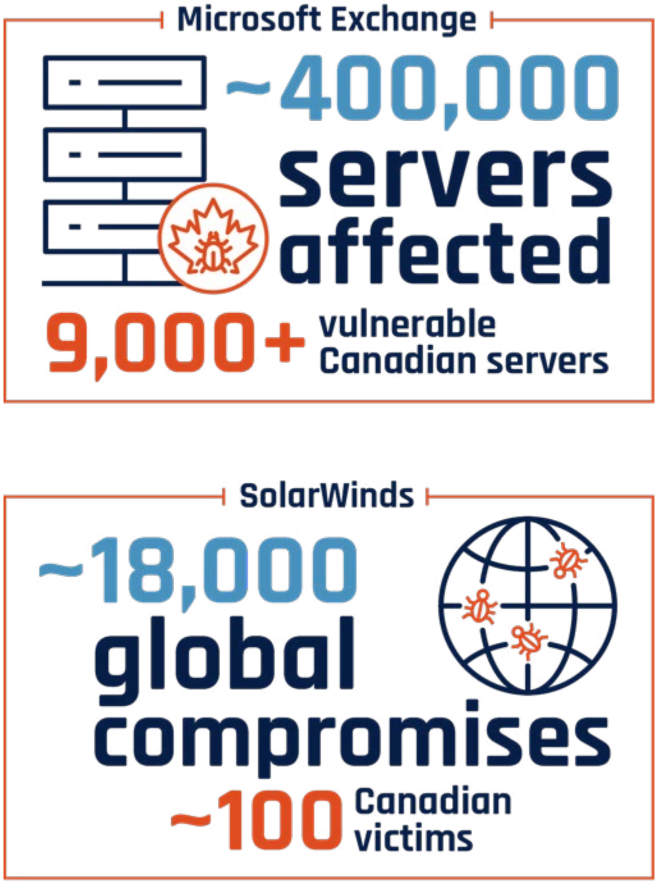

Financial details, social information
Information on habits, health, home security
Location and travel data

State-sponsored threat actors are attempting to compromise Canadians in worldwide, widespread campaigns

Since the publication of NCTA 2020, we have observed state-sponsored threat actors exploiting commonly used software platforms to target thousands, and sometimes hundreds of thousands, of victims across the globe. We are increasingly observing state-sponsored actors taking advantage of zero-day vulnerabilities to compromise victims at scale. By targeting unreported vulnerabilities in commonly used systems, threat actors maximize their range of potential victims and prioritize those of high intelligence value for further malicious cyber threat activity. In March 2021, Chinese state-sponsored cyber threat actors compromised Microsoft Exchange servers worldwide in what was very likely an effort to steal intellectual property and acquire personal information. Globally, an estimated 400,000 servers were affected by this activity.[74] While it is difficult to determine the number of compromises, we assess that upwards of 9,000 Canadian servers were very likely vulnerable.

We assess that state-sponsored cyber threat actors will almost certainly continue to opportunistically exploit victims in large-scale, worldwide cyber campaigns. Even if Canadian individuals and organizations are not specifically targeted, the widespread use of common Internet technologies and software amongst our allies and worldwide means that Canadians will likely be implicated in future campaigns of this nature.

Figure 9: Canadians are exposed to global cyber campaigns[75]



SOFTWARE VULNERABILITIES AND EXPLOITS

Software vulnerabilities are weaknesses or flaws in the design, implementation, operation or management of an information technology system, device, or service that provides access to cyber threat actors. Zero-day vulnerabilities are those that are unknown to the public or software vendor, and thus no patch is available.

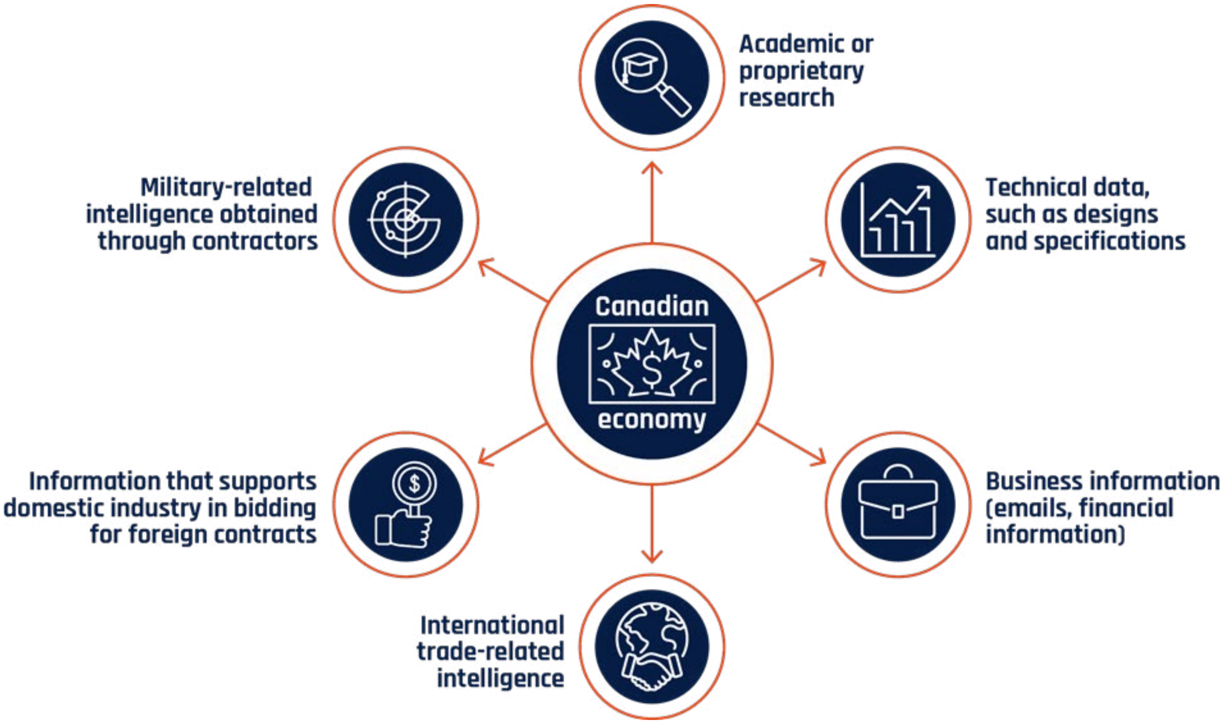
An **exploit** is malicious code that takes advantage of an unpatched vulnerability.

States are targeting Canada's economic value

State-sponsored threat actors engage in commercial espionage, targeting intellectual property and other valuable business information with the goal of sharing stolen information with state-owned enterprises or domestic industry in their home country. Commercial cyber espionage is often part of a broad spectrum of activity that includes intellectual property theft, foreign intelligence operations, covert equipment and materials acquisition, and export control violations. If successful, this activity can result in lost revenue, reputational damage, and lost investment for research and development. We assess that over the next two years, Canadian organizations with information of value to foreign states will almost certainly continue to be targeted by malicious cyber threat activity from state-sponsored actors.

Chinese, Russian, Iranian, and North Korean state-sponsored cyber actors each pose unique strategic threats to Canadian organizations. It is likely that over the next two years, these states will continue to target sectors of importance for their own domestic economic development. That said, the threat from China is very likely the most significant by volume, capability, and assessed intent. China-sponsored cyber threat actors will very likely continue targeting industries and technologies in Canada that contribute to the state's strategic priorities.[76] In 2021, the US Department of Justice unsealed indictments against Chinese state-sponsored cyber threat actors who targeted science and technology research in 12 countries, including Canada, between 2011 and 2018. The industries targeted included maritime technology, vaccines and virus treatments, information technology, aviation, and defence.[77] The information stolen by threat actors was very likely intended to support China's efforts to secure foreign contracts for its state-owned enterprises, in addition to its own research programs.

Figure 10: Targets of interest for espionage


Canadian economy
Academic or proprietary research
Technical data, such as designs and specifications
Business information (emails, financial information)
International trade-related intelligence
Information that supports domestic industry in bidding for foreign contracts
Military-related intelligence obtained through contractors

States are pursuing financial gain via cyber means

In 2021 and 2022, we observed state-sponsored cyber threat actors conducting operations for financial gain, very likely in part to alleviate the impact of international economic sanctions. States' encroachment into financially motivated cyber threat activity increases the likelihood that Canadian individuals and organizations will be impacted by state-sponsored cyber threat activity. For example, North Korean state-sponsored cyber threat actors will almost certainly continue targeting financial institutions to generate revenue over the next two years. North Korean cyber actors have targeted individuals and organizations, including in Canada, by developing malicious cryptocurrency trading applications that can be used to capture individuals' credentials and steal funds.[78]

States are using cybercrime tools and activities to avoid attribution

State-sponsored threat actors also use cyber tools and activities associated with cybercriminals to achieve geopolitical goals, including disrupting adversaries. Ransomware has been used by state-sponsored threat actors to disrupt their victims' operations and steal valuable business information, in addition to collecting funds from the ransom payment itself. By adopting the tactics, techniques and procedures of cybercriminals, state-sponsored cyber actors are likely attempting to avoid blame and hide their activities. For example, Iranian state-sponsored cyber threat actors have used ransomware against organizations in the Middle East and the US. Throughout late 2020 and 2021, researchers identified several Iranian cyber threat actors deploying ransomware. In many cases, these attacks are used to enable commercial espionage, while also resulting in a payout for the threat actors.[79]

Cyber threat actors are attempting to influence Canadians, degrading trust in online spaces

The Internet is a crucial source of information for Canadians. Since the start of the COVID-19 pandemic, 90% of Canadians have used online sources to stay up to date with infection rates, public health measures, and vaccine development.[80] The integrity of the information Canadians receive from online sources is important. It informs their opinions and decision-making regarding public health measures and international events and influences how they engage with democratic processes. Misinformation, disinformation and malinformation (MDM) pollute the online information space by spreading false and potentially harmful information, making it difficult for Canadians to separate truth from falsehoods. Of the Canadians who sought information about COVID-19 online, 96% reported being exposed to content they suspected was misleading, false or inaccurate.[81]

Individuals may be targeted by MDM to inflict reputational damage, or MDM may be intended to influence much larger groups. Some MDM activities are centered around an individual event, such as an election or census, while others are persistent campaigns. Social media algorithms have almost certainly contributed to the spread of MDM, and efforts by some social media platforms to moderate content have created a market for alternative, closed platforms. We have observed cyber threat actors' use of MDM evolve over the past two years. Machine-learning enabled technologies are making fake content easier to manufacture and harder to distinguish from legitimate content. Further, nation states are increasingly willing and able to use MDM to advance their geopolitical interests. We assess that Canadians' exposure to MDM will almost certainly increase over the next two years.

***Figure 11: Definitions of misinformation, disinformation, and malinformation*[82]**

Misinformation
False information not intended to cause harm

Disinformation
False information intended to manipulate, cause damage, or guide people, organizations and countries in the wrong direction

Malinformation
Information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm

Cyber threat actors exploit technology to spread MDM and deceive Canadians

Algorithms amplify MDM

Information flows on the internet are influenced by algorithms that serve users with targeted content and advertisements likely to lead to engagement. MDM content often contains emotive and controversial content that tends to receive higher rates of user engagement.[83] As these algorithms adapt over time to account for individuals' opinions and preferences, they can facilitate the spread of MDM by delivering to those predisposed towards believing it.[84] Cyber threat actors almost certainly exploit social media algorithms to spread their messaging. It is also likely that these actors leverage legitimate voices on social media to covertly promote their influence activities. For example, August 2021 reporting from Facebook suggests that a Russia-linked influence campaign created several fake accounts that promoted disinformation related to COVID-19 vaccinations, which was then further shared by influencers on Instagram.[85]

As more mainstream platforms work to remove false content, MDM has been observed on social media platforms catering to niche audiences that provide a space for like-minded people to interact and perpetuate extreme narratives. For example, during the 2020 US presidential election, Russian actors targeted far-right American users on applications such as Gab and Parler with online foreign influence activity that promoted the incumbent, former President Donald Trump and denigrated then-presidential candidate, Joe Biden.[86] Closed, largely unmoderated messaging applications such as Telegram are also increasingly serving as a forum for MDM content distribution.[87]

Synthetic content calls all information into question

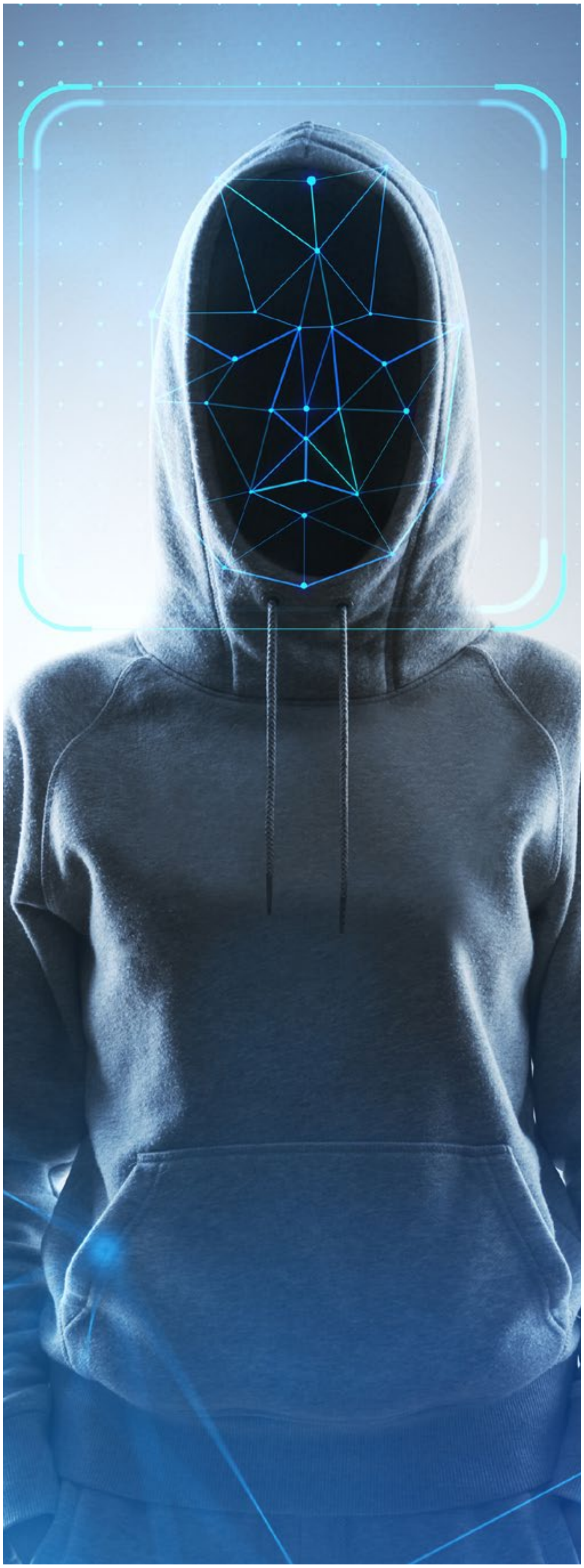
In NCTA 2020 and the 2021 update to our Cyber threats to Canada's democratic process[88] assessment, we described how the technology to make deepfake videos portraying public figures or events was becoming more accessible to cyber threat actors and more convincing. We have continued to observe the technology behind deepfakes evolve and witnessed its use around significant international events.

When targeted at individuals, synthetic content is often intended to intimidate and inflict reputational damage on its victims. For example, deepfake technologies have been used to target politicians and journalists, primarily women, to create non-consensual pornography to silence and discredit them.[89] As deepfakes become harder to distinguish from genuine content and the tools to create convincing deepfakes become more widely available, cyber threat actors will very likely further incorporate the technology into their MDM campaigns, allowing them to increase the scope, scale, and believability of influence activities.

Synthetic content augments MDM campaigns by providing visual evidence backing up false claims. Text generators have progressed to a point where the content they produce is often nearly indecipherable from legitimate material.[90] Commonly available methods of deepfake video and synthetic image generation can still be flagged as fake and some are easily distinguishable from real content. However, more sophisticated examples continue to improve in quality and present challenges for detection.[91] Throughout the Russian invasion of Ukraine, we have observed synthetic content being distributed alongside a concerted disinformation campaign by Russia.

DEEPFAKES' DISPROPORTIONATE IMPACT ON WOMEN

We assess almost certainly that the most immediate illicit use of deepfake technologies has been directed at women who are at a higher risk of being depicted in sexually explicit synthetic content without their consent. Some researchers estimate that 95% of all deepfake videos on the Internet contain non-consensual synthetic pornography and that about 90% of these depict women.[92] Some of the most popular deepfake tools available today are apps that "digitally undress" pictures and generate personalized deepfake pornographic material.[93]



DEEPFAKES DURING RUSSIA'S INVASION OF UKRAINE

The Russian invasion of Ukraine has involved a sustained campaign of disinformation designed to create confusion and interfere with international perceptions of the war. On March 16, 2022, a deepfake video of Ukrainian President Zelenskyy was circulated on social platforms. The deepfake had President Zelenskyy asking Ukrainian soldiers to surrender to Russia.[94] Earlier in 2022, unknown actors posing as the mayor of Kyiv secured video calls with several European mayors. Call participants had no idea that the other caller was a deepfake until the supposed mayor of Kyiv began making suspicious comments.[95]

Foreign actors use MDM to influence international narratives

We described in NCTA 2020 how online foreign influence activities have become a new normal, with adversaries seeking to influence elections and impact international discourse related to current events. This trend has continued since 2020. Adversary states constantly circulate and amplify MDM that supports their interests around significant events like the Russian invasion of Ukraine. We assess that MDM propagated by state-sponsored cyber threat actors represents an ongoing, persistent threat to Canadians. Canada's active participation in the international community and membership in key organizations, such as NATO and the G7, almost certainly makes Canadians a target for online foreign influence campaigns.

While we assess that Canada is not a primary target for Russian MDM activities, Russia disinformation does target the West and has opportunistically seized on events implicating Canada. In April 2022, CSE reported that Russia was spreading MDM about Canadian Forces members committing war crimes in Ukraine and using fake images to back up false narratives about Canada's involvement in the conflict.[96] In one online survey of Canadian social media users, over half of the respondents reported encountering MDM relating to the Russian invasion of Ukraine on social media.[97]

Online foreign influence activity very likely also targets linguistic minorities and diaspora communities in Canada. State-sponsored cyber threat actors aim to influence these groups in order to minimize dissent or support the policies of their country of origin.[98] These groups often interact on platforms that are semi-closed and censored according to restrictive content regulations, meaning that MDM can very likely spread more easily throughout these groups.[99] For example, WeChat, a social media app from China used by billions around the world, has been used to spread MDM and propaganda specific to the Chinese diaspora.[100]

Disruptive technologies bring new opportunities and new threats

The rapid development of technology has created many opportunities for those successful in creating, scaling, and deploying innovations. Some developments can be said to be "disruptive" because they fundamentally alter their area of application, providing significant improvements over existing technologies or new approaches that make incumbent technologies obsolete. However, regulation often struggles to keep up with leading-edge technological development, and the implications and risks of adoption are not always initially clear.

Just as advanced technologies can be used to support commercial and public objectives, they can be maliciously deployed by sophisticated threat actors. This section discusses three of the technological trends we assess as having the potential to disrupt their respective fields: digital assets and decentralized finance, machine learning, and quantum computing. While these technologies are in varying states of development and realization, they all have implications for Canada's economic prosperity, national security, and the individual safety and privacy of Canadians.

Digital assets are targets and tools for cyber threat actors

Since Bitcoin debuted as the first cryptocurrency in 2008, the number of cryptocurrencies and the value of cryptocurrency markets has exploded. There are now over 10,000 different cryptocurrencies being traded. The market cap peaked at almost $3 trillion USD during the COVID-19 pandemic before dipping just below $1 trillion in mid-2022, still well above pre-COVID-19 levels.[101] Cryptocurrencies and their supporting blockchain technologies have contributed to the development of a digital-based economic ecosystem, where digital assets have real-world value. An emerging aspect of this system is Decentralized Finance, often referred to as DeFi, which allows large-scale borrowing and lending of funds without intermediaries. These activities occur on DeFi platforms that provide a broad range of services and serve as an alternative to traditional, centralized financial systems based on banks and similar institutions.

According to vendor analysis, cryptocurrency theft peaked in 2021 to almost $3.2 billion in value from both cryptocurrency exchanges and DeFi platforms.[102] In addition to stealing cryptocurrency through fraud, scams, and digital wallet compromise, cyber threat actors rely on cryptocurrency to pay for illicit goods and services, to receive payments from ransomware victims, and to launder criminal proceeds. While law enforcement has had some success in tracking and, in some cases, recovering stolen funds, cyber threat actors continue to refine and develop techniques for obscuring illicit financial transactions, such as the use of mixers or privacy coins.[103] We assess that cryptocurrency money laundering will almost certainly continue to facilitate the growth of cybercrime and other illicit activities and impede law enforcement's ability to track and recover funds.

Figure 12: Cryptocurrency terms

Privacy coins

Cryptocurrencies such as Bitcoin operate on a public blockchain, meaning that all transfers and transactions are public. Privacy coins such as Monero are specifically designed to obscure transactions and ensure the anonymity of users. This makes privacy coins attractive for cyber threat actors who have an inherent interest in avoiding detection and making it difficult for law enforcement to follow illicit money flows.[104]

Mixers

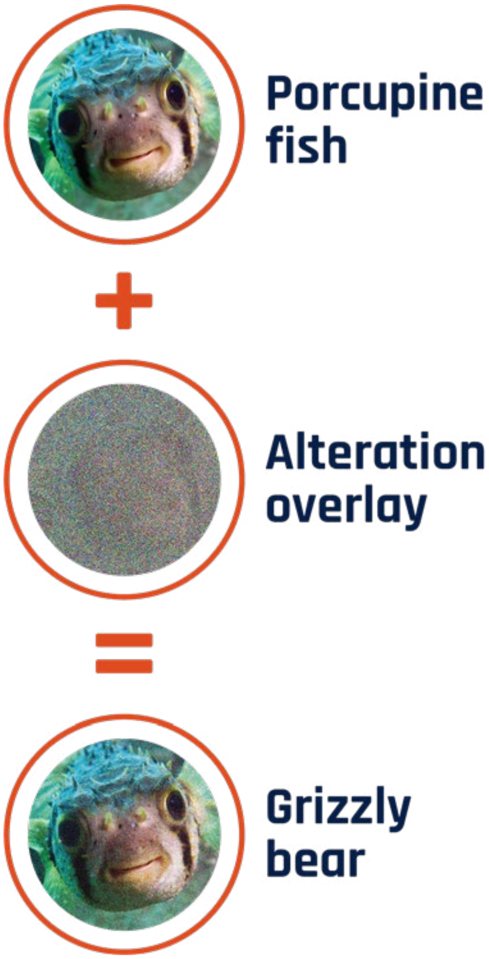
Mixers allow cyber threat actors to obfuscate the origin of illicitly obtained cryptocurrency. Mixers accept cryptocurrencies from users and combine them into a collective pool, effectively "mixing" them together. Users then withdraw the value of their deposit from the mixed pool, minus a service fee. Mixers have seen increased use, breaking $1 billion USD in quarterly value received at the end of 2020 and ranging from $2 billion to just over $3 billion USD every quarter since. The increase has been driven by funds received from suspected illicit sources, which in the second quarter of 2022 accounted for around 28%, or $700 million USD, of value sent to mixers.[105]

Machine learning automations can be deceived and exploited

Machine learning is a rapidly developing subset of artificial intelligence that has already become commonplace in consumer services and data analysis. Machine learning techniques present a fundamental shift in the automation of tasks such as image recognition, language translation, and online content moderation or curation. Researchers have demonstrated many other promising applications for machine learning in the future, including for self-driving vehicles and medical diagnostics.[106] As machine learning is incorporated into decision-making processes with significant societal or personal impacts, care will need to be taken to ensure its application is equitable, unbiased, and secure. Machine learning applications have unique vulnerabilities compared to traditional programming. These can be exploited by cyber threat actors, adding to the threat surface of the organizations that employ them.

Cyber threat actors attack machine learning models through adversarial machine learning techniques.[107] Broadly, these techniques exploit flaws in the machine learning model's logic to deceive it or force it to return unintended, sometimes confidential, information.

Figure 13: Adversarial machine learning in image recognition



As illustrated in Figure 13, image recognition machine learning models can be tricked into misidentifying objects by subtly altering the image. Some alterations are invisible to the human eye, making them difficult to detect.[108] The same principle applies to other machine learning applications, such as malware detection. By subtly altering the code of the malware in ways that confuse the algorithm, cyber threat actors may trick security software into misclassifying malware as benign. We assess that cyber threat actors are also very likely deceiving machine learning algorithms to enable their other threat activity, such as the distribution of misinformation and large-scale email fraud campaigns.[109]

By providing the machine learning model with carefully crafted queries, cyber threat actors may be able to infer information from the training data.[110] Where the machine learning model is applied to medical diagnosis or fraud protection, the training data may include sensitive personal information, including health history or financial details. Exposure of that information, or that an individual was part of the training data, can be used for further tailored threat activity like fraud and scams. Personal information stolen in this way is at risk of further exposure should it be sold or released publicly.

Quantum computing threatens modern cryptography

Quantum computing is an emerging technology intended to overcome the physical limitations of conventional computing through the application of quantum physics. Quantum computers threaten our current methods for ensuring the cyber security of information systems and protecting sensitive data transmitted over the Internet. Cryptography is used to protect data using mathematical problems that certify the source and scramble its contents from unintended viewers. Without the decryption key, breaking the security by solving the mathematical problem could not be done in a reasonable timeframe with classical computers. However, the mathematical problems underpinning current cryptographic standards are easily completed by quantum computers. Quantum devices powerful enough to break modern cryptography could be available as early as the 2030s, making it impossible to securely transmit sensitive information if changes to our current cryptographic methods are not made.[111] However, we have yet to observe quantum computers capable of completing problems providing commercial advantage that could not also be completed by classical computers.[112]

Cryptography is essential for common digital systems of trust that require transfers of sensitive data, such as personal details or financial information. We assess that the proactive development and adoption of quantum-resistant cryptography will likely diminish the threat to future information and communications should quantum computing become more capable and common. The Cyber Centre has been active in developing a solution to the quantum challenge, working with the US National Institute of Standards and Technology to certify standards for quantum-resistant cryptography.[113] However, encrypted information stolen by threat actors today can be held and decrypted when quantum computers become available. For most Canadians this may not be a significant threat; however, stolen commercial information and government data related to foreign affairs or national security may still be valuable or sensitive in the future.[114]

Conclusion

The cyber threat landscape in Canada continues to evolve. Canadians use the Internet more often and for a greater number of tasks. As more devices are connected to the Internet, the cyber threat surface expands. Cyber threat actors adapt their activities and utilize new technologies to achieve their financial, geopolitical, or ideological goals.

In this National Cyber Threat Assessment, we identified trends within the threat landscape and provided an overview of 5 themes that we anticipate will drive cyber threats to Canada over the next two years. While cybercrime remains the threat most likely to affect Canadians and Canadian organizations, state-sponsored cyber threat activity is also impacting Canadians. Critical infrastructure is increasingly at risk from cyber threat activity from both cybercriminals and state-sponsored actors, while nation states are evolving their use of misinformation, disinformation, and malinformation to influence Canadians. The cyber threat landscape will almost certainly evolve further over the next two years as technologies such as digital assets, machine learning, and quantum computing bring new opportunities and new threats.

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, 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 encourage readers to consult our cyber security guidance[115] for more information on the cyber threats and trends outlined in this document.

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

Endnotes

1 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

2 https://cyber.gc.ca/en/

3 https://twitter.com/cybercentre_ca

4 https://cyber.gc.ca/en/guidance

5 https://www.getcybersafe.gc.ca/en

6 https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

7 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

8 https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

9 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

10 https://cyber.gc.ca/en/guidance

11 https://www.getcybersafe.gc.ca/en/home

12 https://www.cira.ca/resources/state-internet/report/canadas-internet-factbook-2022

13 https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

14 Statistics Canada. **"Internet use and COVID-19: How the pandemic increased the amount of time Canadians spend online."** June 24, 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00027-eng.htm

15 Amazon Canada. **"OOO Until TBD? Majority of Canadian Office Workers Want Remote Work to Stay."** March 10, 2020
https://www.newswire.ca/news-releases/ooo-until-tbd-majority-of-canadian-office-workers-want-remote-work-to-stay-897250807.html;

16 Kaspersky. **"COVID-19: Examining the threat landscape a year later."** March 15, 2021.
https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154/

17 Microsoft. **"Microsoft Digital Defense Report."** October 2021.
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

18 Statistics Canada. **"Canadians' use of the Internet and digital technologies before and during the COVID-19 pandemic."** April 28, 2022.
https://www150.statcan.gc.ca/n1/pub/36-28-0001/2022004/article/00004-eng.htm

19 CBC News. **"Federal, Quebec governments to spend $826 million to expand high-speed internet."** March 22, 2021.
https://www.cbc.ca/news/canada/montreal/trudeau-quebec-high-speed-internet-1.5959741
Erik White. **"Satellite internet a 'game changer' for rural and northern Ontario, but some say fibre should still come first."**
https://www.cbc.ca/news/canada/sudbury/starlink-satellite-internet-northern-ontario-1.6263474

20 Government of Canada. **"Smart Cities and National Security."** February 16, 2022.
https://www.canada.ca/en/security-intelligence-service/corporate/publications/smart-cities-national-security/smart-cities-national-security.html

21 Patricia Ruffio. **"Dark Web Price Index 2022."** Privacy Affairs. July 7, 2022.
https://www.privacyaffairs.com/dark-web-price-index-2022/

22 Chainanalysis. **“The 2022 Crypto Crime Report.”** February 2022.
https://go.chainalysis.com/2022-Crypto-Crime-Report.html
Digital Shadows. **“Initial Access Brokers Report.”**
https://resources.digitalshadows.com/whitepapers-and-reports/initial-access-brokers-report?utm_source=blog&utm_medium=website&utm_campaign=initial_access_brokers_report

23 Chainanalysis. **“The 2022 Crypto Crime Report.”** February 2022.
https://go.chainalysis.com/2022-Crypto-Crime-Report.html

24 Canadian Centre for Cyber Security. **“Alert – Active exploitation of Apache Log4j vulnerability – update 7.”** December 29, 2021.
https://www.cyber.gc.ca/en/alerts-advisories/active-exploitation-apache-log4j-vulnerability

25 Ilkka Turunen. **“Log4shell by the numbers – Why did CVE-2021-44228 set the Internet on Fire?”** Sonatype. December 14, 2021.
https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire

26 Shachar Menashe, Or Peles, and Ori Hollander. **“Log4j Log4Shell 0-Day Vulnerability: All You Need to Know.”** JFrog. December 28, 2021.
https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/

27 **CSE official Twitter account** @cse_cst, April 2022.
https://twitter.com/cse_cst
Ben Nimmo, Ira Hubert, and Yang Cheng. **“Spamouflage Breakout.”** Graphika. February 2021.
https://graphika.com/reports/spamouflage-breakout/

28 Global Affairs Canada. **“Statement on Russia’s malicious cyber activity affecting Europe and Ukraine.”** May 10, 2022.
https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html

29 **CSE official Twitter account** @cse_cst, April 2022.
https://twitter.com/cse_cst

30 Marianne Díaz Hernández, Felicia Anthonio, Sage Cheng, and Alexia Skok. **“Internet shutdowns in 2021: the return of digital authoritarianism.”** AccessNow. April 28, 2022.
https://www.accessnow.org/internet-shutdowns-2021/

31 Freedom House. “Freedom on the Net 2021.”
https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

32 Flashpoint. **“Understanding Russia’s, ‘Sovereign Internet’: What Happens if Russia Isolates Itself from the Global Internet.”** March 11, 2022.
https://flashpoint.io/blog/russian-runet-sovereign-internet/

33 Yahoo Finance. **“China’s World Internet Conference goes ‘international’ as Beijing seeks to promote its own vision of global cyberspace.”** July 13, 2022.
https://finance.yahoo.com/news/chinas-world-internet-conference-goes-093000698.html

34 Canadian Anti-Fraud Centre. **“The impact of fraud so far this year.”** Updated June 30, 2022.
https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

35 Tara Seals. **“Ransomware Volumes Hit Record Highs as 2021 Wears On.”** Threat Post. August 3, 2021.
https://threatpost.com/ransomware-volumes-record-highs-2021/168327/
Sophos. **“Ransomware hit 66% of Organizations Surveyed for Sophos’ Annual ‘State of Ransomware 2022’.”** April 27, 2022.
https://www.sophos.com/en-us/press-office/press-releases/2022/04/ransomware-hit-66-percent-of-organizations-surveyed-for-sophos-annual-state-of-ransomware-2022
Lawrence Abrams. **“Computer giant Acer hit by $50 million ransomware attack.”** Bleeping Computer. March 19, 2021.
https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

36 TELUS. **“TELUS Canadian Ransomware Study.”** 2022.
https://www.telus.com/en/bc/business/ransomware-study?INTCMP=VAN_ransomwarestudy

37 Recorded Future. **“The Business of Fraud: Sales of PII and PHI.”** February 17, 2021.
https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf
Mandiant. **“1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information.”** January 31, 2022.
https://www.mandiant.com/resources/ransomware-extortion-ot-docs

38 Jonathan Greig. **"Canadian fighter jet training company investigating ransomware attack."** The Record. May 11, 2022.
https://therecord.media/top-aces-ransomware-attack-lockbit/

39 Dee-ann Durbin. **"Meat company JBS Foods confirms it paid US$11M ransom in cyberattack."** Global News. June 9, 2021.
https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid/
Christina Wilkie. **"Colonial Pipeline paid $5 million ransomware one day after cyberattack, CEO tells Senate."** CNBC. June 9, 2021.
https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html

40 Humber River Hospital. **"Code Grey Update."** June 15, 2021. Erica Vella.
https://www.hrh.ca/2021/06/15/code-grey/
"Toronto's Humber River Hospital under code grey after ransomware attack." Global News. June 18, 2021.
https://globalnews.ca/news/7963652/humber-river-hospital-ransomware-attack-toronto/
Toronto Transit Commission. **"TTC provides update on cybersecurity incident."** November 8, 2021. CBC News.
https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident
"Toronto transit system hit by ransomware attack, TTC says no significant disruptions." October 29, 2021.
https://www.cbc.ca/news/canada/toronto/ttc-ransomware-attack-1.6231349

41 Kartikay Mehrotra and William Turton. **"CNA Financial Paid $40 Million in Ransom After March Cyberattack."** Bloomberg. May 20, 2021.
https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

42 TELUS. **"TELUS Canadian Ransomware Study."** 2022.
https://www.telus.com/en/bc/business/ransomware-study?INTCMP=VAN_ransomwarestudy

43 Coveware. **"Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022."** July 28, 202.
https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

44 ESET Digital Security. **"Threat Report T1 2022."** 2022.
https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

45 Palo Alto Networks. **"2021 Palo Alto Networks Canada Ransomware Barometer."** June 2, 2021.
https://www.paloaltonetworks.ca/apps/pan/public/downloadResource?pagePath=/content/pan/en_CA/resources/research/2021-palo-alto-networks-canada-ransomware-barometer

46 Financial Times. **"Monero emerges as crypto of choice for cybercriminals."** June 22, 2021.
https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6

47 Malwarebytes Labs. **"Updated: Kaseya hijacked, thousands attacked by REvil, fix delayed again."** July 7, 2021.
https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/#thousands-affected

48 Lawrence Abrams. **"Ransomware gang plans to call victim's business partners about attacks."** Bleeping Computer. March 6, 2021.
https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/

49 United States Government. **"Indicators of Compromise Associated with AvosLocker Ransomware."** March 17, 2022.
https://www.ic3.gov/Media/News/2022/220318.pdf

50 Jessica Lyons Hardcastle. **"FBI, CISA: Don't get caught in Karakurt's extortion web."** The Register. June 3, 2022.
https://www.theregister.com/2022/06/03/fbi_cisa_warn_karakurt_extortion/

51 Rogers. **"An updated message from Jorge Fernandes, Chief Technology Officer at Rogers."** April 19, 2021.
https://about.rogers.com/news-ideas/a-message-from-jorge-fernandes-chief-technology-officer-at-rogers/
Rogers. **"An Update from Rogers President and CEO."** July 13, 2022.
https://about.rogers.com/news-ideas/an-update-from-rogers-president-and-ceo/
Pete Evans. **"What happened at Rogers? Day-long outage is over, but questions remain."** CBC News. April 20, 2021.
https://www.cbc.ca/news/business/rogers-outage-analysis-1.5994851
Darren Major. **"Ottawa calls on telecom companies to shore up networks after Rogers outage."** CBC News. July 11, 2022.
https://www.cbc.ca/news/politics/ottawa-demanding-improve-network-rogers-outage-1.6516970

52 Lawrence Abrams. **"Massive Rogers outage disrupts mobile service, payments in Canada."** Bleeping Computer. July 8, 2022.
https://www.bleepingcomputer.com/news/technology/massive-rogers-outage-disrupts-mobile-service-payments-in-canada/

53 Daniel Zafra, Corey Hidelbrandt, Nathan Brubaker, and Keith Lunden. **“1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information.”** Mandiant. January 31, 2022.
https://www.mandiant.com/resources/ransomware-extortion-ot-docs

54 Public Safety Canada. **“National Strategy for Critical Infrastructure.”** November 10, 2011.
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

55 Martin Placek. **“Industrial IoT – market size worldwide 2022-2028.”** Statista. March 14, 2022.
https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/ https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/
GlobeNewswire. **“Industrial IoT Market to reach US$ 1.3 Tn by 2032 - Comprehensive Research Report by FMI.”** April 6, 2022.
https://www.globenewswire.com/en/news-release/2022/04/07/2418081/0/en/Industrial-IoT-Market-to-reach-US-1-3-Tn-by-2032-Comprehensive-Research-Report-by-FMI.html

56 McKinsey & Company. **“How COVID-19 has pushed companies over the technology tipping point—and transformed business forever.”** October 5, 2020.
https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

57 David Sanger, Clifford Krauss, and Nicole Perlroth. **“Cyberattack Forces a Shutdown of a Top U.S. Pipeline.”** The New York Times. May 13, 2021.
https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
Communications Security Establishment. **“CSE Statement on the NotPetya Malware.”** February 15, 2018.
https://cse-cst.gc.ca/en/information-and-resources/news/cse-statement-notpetya-malware;
Andy Greenberg. **“The Untold Story of NotPetya, the Most Devastating Cyberattack in History.”** Wired. August 22, 2018.
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

58 Nathan Brubaker, Daniel Kapellmann Zafra, Keith Lunden, Ken Proska, and Corey Hildebrandt. **“Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families.”** Mandiant. July 15, 2020.
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

59 Cybersecurity and Infrastructure Security Agency. **“Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.”** April 20, 2022.
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

60 https://www150.statcan.gc.ca/t1/tbl1/en/cv.action?pid=2210007601

61 Kevin Poulsen, Robert McMillan, and Melanie Evans. **“A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death.”** Wall Street Journal. September 30, 2021.
https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

62 Jackie Drees. **“Meet the ransomware gang behind 235 attacks on US hospitals: 7 things to know.”** Becker’s Health IT. June 10, 2021.
https://www.beckershospitalreview.com/cybersecurity/meet-the-ransomware-gang-behind-235-attacks-on-us-hospitals-7-things-to-know.html
Kevin Poulson and Melanie Evans. **“The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: ‘They Do Not Care’.”** Wall Street Journal. June 10, 2021.
https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215

63 Newfoundland and Labrador Health and Community Services. **“Information and Updates on Cyber Incident.”** March 30, 2022.
https://www.gov.nl.ca/hcs/information-and-updates-on-cyber-incident/
Sarah Smellie. **“N.L. rebuilding systems downed by cyberattack from scratch, Eastern Health says.”** CBC News. December 16, 2021.
https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cp-cyberattack-rebuilding-1.6287934

64 Elgin County. **“Information Privacy.”** May 13, 2022.
https://www.elgincounty.ca/services/privacy-information/
Matthew Trevithick. **“Sensitive personal data among thousands of files exposed in Elgin Cybersecurity incident: Gonyou.”** Global News. May 16, 2022.
https://globalnews.ca/news/8838788/personal-data-files-elgin-cybersecurity-exposure/

65 Packetlabs. **“Are Municipal Cyber Attacks Threatening Citizens’ Privacy?”** December 13, 2021.
https://www.packetlabs.net/posts/municipal-cyber-attacks/

66 Canadian Centre for Cyber Security. **"Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity."** January 26, 2022.
https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise
Canadian Centre for Cyber Security. **"Cyber threat bulletin: Cyber Centre reminds Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity."** February 13, 2022.
https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators

67 Howard Solomon. **"Newfoundland and Labrador health system attackers copied 200,000 patient and employee files."** IT World Canada. March 31, 2022.
https://www.itworldcanada.com/article/newfoundland-and-labrador-health-system-attackers-copied-200000-patient-and-employee-files/478645

68 Check Point Research. **"Rampant Kitten – An Iranian Espionage Campaign."** September 18, 2020.
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/
United States Department of Justice. **"Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election."** November 18, 2021.
https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
The Citizen Lab. **"The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil."** October 1, 2018.
https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
The Citizen Lab. **"WeChat Surveillance Explained."** May 7, 2020.
https://citizenlab.ca/2020/05/wechat-surveillance-explained/

69 The Citizen Lab. **"Psychological and Emotional War: Digital Transnational Repression in Canada."** March 1, 2022.
https://tspace.library.utoronto.ca/bitstream/1807/120575/1/Report%23151--dtr_022822_lowres.pdf

70 The Citizen Lab. **"The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit."** December 20, 2020.
https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

71 Australian Strategic Policy Institute. **"TikTok and WeChat: Curating and controlling global information flows."** September 2020.
https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ=
The Citizen Lab. **"We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus."** May 7, 2020.
https://citizenlab.ca/2020/05/we-chat-they-watch/

72 Australian Strategic Policy Institute. **"TikTok and WeChat: Curating and controlling global information flows."** September 2020.
https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ=

73 Office of the Privacy Commissioner of Canada. **"Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information."** April 9, 2019.
https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/
United States Department of Justice. **"Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax."** February 10, 2020.
https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

74 Global Affairs Canada. **"Statement on China's cyber campaigns."** July 19, 2021.
https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html

75 Global Affairs Canada. **"Statement on China's cyber campaigns."** July 19, 2021.
https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html
Global Affairs Canada. **"Statement on SolarWinds cyber compromise."** April 15, 2021.
https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html
Dan Goodin. **"SolarWinds hackers breach new victims, including a Microsoft support agent."** ArsTechnica. June 26, 2021 (English only).
https://arstechnica.com/gadgets/2021/06/solarwinds-hackers-breach-new-victims-including-a-microsoft-support-agent/

76 Cybersecurity and Infrastructure Security Agency. **"Potential for China Cyber Response to Heightened U.S. – China Tensions."** October 1, 2020.
https://www.cisa.gov/uscert/ncas/alerts/aa20-275a

77 The United States Department of Justice. **"Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research."** July 19, 2021.
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

78 Cybersecurity and Infrastructure Security Agency. **"AppleJeus: Analysis of North Korea's Cryptocurrency Malware."** February 17, 2021.
https://www.cisa.gov/uscert/ncas/alerts/aa21-048a

79 Sergiu Gatlan. **“Iranian nation-state hackers linked to Pay2Key ransomware.”** Bleeping Computer. December 17, 2020.
https://www.bleepingcomputer.com/news/security/iranian-nation-state-hackers-linked-to-pay2key-ransomware/
Microsoft Threat Intelligence Center. **“Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021.”** November 16, 2021.
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

80 Statistics Canada. **“Misinformation during the COVID-19 pandemic.”** February 2, 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00003-eng.htm
Simon Kemp. **“Digital 2021 Canada.”** February 9, 2021.
https://datareportal.com/reports/digital-2021-canada

81 Statistics Canada. **“Misinformation during the COVID-19 pandemic.”** February 2, 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00003-eng.htm
Simon Kemp. **“Digital 2021 Canada.”** February 9, 2021.
https://datareportal.com/reports/digital-2021-canada

82 CCCS. **“How to identify misinformation, disinformation, and malinformation (ITSAP.00.300).”** February 2022.
https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

83 Chris Meserole. **“How misinformation spreads on social media—And what to do about it.”** Brookings Institute. May 9, 2018.
https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/

84 Jim Fournier. **“How algorithms are amplifying misinformation and driving a wedge between people.”** The Hill. November 10, 2021.
https://thehill.com/changing-america/opinion/581002-how-algorithms-are-amplifying-misinformation-and-driving-a-wedge/

85 Meta. **“July 2021 Coordinated Inauthentic Behaviour Report.”** August 10, 2021.
https://about.fb.com/news/2021/08/july-2021-coordinated-inauthentic-behavior-report/
Elizabeth Culliford. **“Facebook removes Russian networks that targeted influences to peddle anti-vax messages.”** Reuters. August 10, 2021.
https://www.reuters.com/technology/facebook-removes-russian-network-that-targeted-influencers-peddle-anti-vax-2021-08-10/

86 Graphika. **“Step into My Parler.”** October 1, 2020.
https://graphika.com/reports/step-into-my-parler/

87 Craig Timberg and Elizabeth Dwoskin. **“With Trump gone, QAnon groups focus fury on attacking coronavirus vaccines.”** The Washington Post. March 11, 2021.
https://www.washingtonpost.com/technology/2021/03/11/with-trump-gone-qanon-groups-focus-fury-attacking-covid-vaccines/
Aliaksandr Herasimenka, Jonathan Bright, Aleksi Knuutila, and Philip Howard. **“Misinformation and professional news on largely unmoderated platforms: the case of telegram.”** Journal of Information Technology and Politics. May 25, 2022.
https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2076272

88 https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

89 Aayushi Pratap. **“Deepfake Epidemic Is Looming—And Adobe Is Preparing For The Worst.”** Forbes. June 29, 2022.
https://www.forbes.com/sites/aayushipratap/2022/06/29/deepfake-epidemic-is-looming-and-adobe-is-preparing-for-the-worst/?sh=4cdf6ea5b81d

90 Thanh Nguyen, Cuong Nguyen, Dung Nguyen, Duc Nguyen, and Saeid Nahavandi. **“Deep Learning for Deepfakes Creation and Detection: A Survey.”** arXiv. September 25, 2019.
https://arxiv.org/abs/1909.11573v2?utm_campaign=AI%20Scholar%20Weekly%20&utm_medium=email&utm_source=Revue%20newsletter

91 Thanh Nguyen, Cuong Nguyen, Dung Nguyen, Duc Nguyen, and Saeid Nahavandi. **“Deep Learning for Deepfakes Creation and Detection: A Survey.”** arXiv. September 25, 2019.
https://arxiv.org/abs/1909.11573v2?utm_campaign=AI%20Scholar%20Weekly%20&utm_medium=email&utm_source=Revue%20newsletter

92 Franziska Berczyk. **“Deepfake porn is ruining women’s lives. Now the law may finally ban it.”** MIT Technology Review. February 12, 2021.
https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/amp/?utm_medium=search&utm_source=google&utm_campaign=BL-ACQ-DYN&utm_content=categories&gclid=CjwKCAjwo_KXBhAaEiwA2RZ8hI3MIiDJNuYcDe5BcDr55qfUagpguO6PJgFTTIZBIfz6NfZ_V8KuSxoC5KMQAvD_BwE

93 Karen Hao. **“A deepfake bot is being used to “undress” underage girls.”** MIT Technology Review. October 20, 2020.
https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/

94 Bobby Allyn. **“Deepfake video of Zelenskyy could be ‘tip of the iceberg’ in info war, experts warn.”** NPR. March 16, 2022.
https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

95 Philip Oltermann. **“European politicians duped into deepfake video calls with mayor of Kyiv.”** The Guardian. June 25, 2022.
https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko

96 CSE official Twitter account @cse_cst, April 2022.
https://twitter.com/cse_cst

97 Philip Mai, Alyssa Saiphoo, Anatoliy Gruzd, and Felipe Soares. **“Russian propaganda is making inroads with right-wing Canadians.”** The Conversation. July 17, 2022.
https://theconversation.com/russian-propaganda-is-making-inroads-with-right-wing-canadians-186952

98 G7 Rapid Response Mechanism. **“Annual Report 2021.”** 2021.
https://www.international.gc.ca/transparency-transparence/assets/pdfs/international-assistance-report-rapport-aide-internationale/g7-rrm-2021-annual-report-en.pdf

99 Esther Chan and Stevie Zhang. **“Disinformation, stigma and Chinese diaspora: policy guidance for Australia.”** First Draft News. August 31, 2021.
https://firstdraftnews.org/long-form-article/disinformation-stigma-and-chinese-diaspora-policy-guidance-for-australia/
Miles Kenyon. **“WeChat Surveillance Explained.”** Citizen Lab. May 7, 2020.
https://citizenlab.ca/2020/05/wechat-surveillance-explained/

100 Nicole Hong. **“WeChat, Wild Rumors and All, Is Their Lifeline. Washington May End That.”** The New York Times. October 5, 2020.
https://www.nytimes.com/2020/10/05/nyregion/us-wechat-ban.html
Paul Mozur. **“Forget TikTok. China’s Powerhouse App is WeChat, and Its Power Is Sweeping.”** The New York Times. 4 September 2020.
https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html
Joe Fitzgerald Rodriguez, Shannon Lin, and Jessica Huseman. **“Misinformation Image on WeChat Attempts to Frighten Chinese Americans Out of Voting.”** ProPublica. November 2, 2020.
https://www.propublica.org/article/misinformation-image-on-wechat-attempts-to-frighten-chinese-americans-out-of-voting
Yaqiu Wang. **“WeChat Is a Trap for China’s Diaspora.”** Human Rights Watch. August 14, 2020.
https://www.hrw.org/news/2020/08/14/wechat-trap-chinas-diaspora
Jeanne Whalen. **“Chinese censorship invades the U.S. via WeChat.”** Washington Post. January 7, 2021.
https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/

101 CoinMarketCap. **“Global Cryptocurrency Charts; Total Cryptocurrency Market Cap.”** Retrieved August 16, 2022.
https://coinmarketcap.com/charts/
Reynor de Best. **“Quantity of cryptocurrencies as of February 3, 2022.”** Statista. March 22, 2022.
https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

102 Chainanalysis. **“The 2022 Crypto Crime Report,”** February 2022.
https://go.chainalysis.com/2022-Crypto-Crime-Report.html

103 Jacob Bunge. **“JBS Paid $11 Million to Resolve Ransomware Attack.”** Wall Street Journal. June 9, 2021.
https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
Department of Justice. **“Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency.”** February 8, 2022.
https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

104 Richard Clark, Sarah Kreps, and Adi Rao. **“Shifting crypto landscape threatens crime investigations and sanctions.”** Brookings Institute. March 7, 2022.
https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/

105 Chainalysis. **“Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume.”** July 14, 2022.
https://blog.chainalysis.com/reports/cryptocurrency-mixers/

106 Adam Zewe. **“Anticipating others’ behaviour on the road.”** MIT News. April 21, 2022.
https://news.mit.edu/2022/machine-learning-anticipating-behavior-cars-0421
Manjurul Ahsan, Shahana Luna, Zahed Siddique. **“Machine-Learning Based Disease Diagnosis: A Comprehensive Review.”** Healthcare. March 15, 2022.
https://doi.org/10.3390/healthcare10030541

107 Microsoft. **“The 2021 Microsoft Digital Defence Report.”** Microsoft (October 2021) at page 43.
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

108 Gabriel Machado, Eugênio Silva, and Ronaldo Goldschmidt. **"Adversarial Machine Learning in Image Classification: A Survey Towards the Defender's Perspective."** arXiv. September 8, 2020.
https://arxiv.org/abs/2009.03728

109 Lily Hay Newman. **"AI Wrote Better Phishing Emails Than Humans in a Recent Test."** Wired. August 7, 2021.
https://www.wired.com/story/ai-phishing-emails/

110 Hailong Hu and Jun Pang. **"Stealing Machine Learning Models: Attacks and Countermeasures for Generative Adversarial Networks."** ACSAC '21: Annual Computer Security Applications Conference. December 2021.
https://dl.acm.org/doi/10.1145/3485832.3485838

111 CCCS. **"Preparing your organization for the quantum threat to cryptography (ITSAP.00.017)."** February 2021.
https://cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

112 McKinsey & Company. **"Quantum computing: An emerging ecosystem and industry use cases."** December 2021.
https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf
Adrian Cho. **"Ordinary computers can beat Google's quantum computer after all."** Science. August 2, 2022.
https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all

113 CCCS. **"Cyber Centre's summary review of final candidates for NIST Post-Quantum Cryptography standards."** March 1, 2021.
https://cyber.gc.ca/en/news-events/cyber-centres-summary-review-final-candidates-nist-post-quantum-cryptography-standards/

114 Security Week. **"Predictions: SecurityWeek's 2022 Cybersecurity Outlook."** January 4, 2022.
https://www.securityweek.com/predictions-securityweeks-2022-cybersecurity-outlook
Stephen Shankland. **"Quantum computers could crack today's encrypted messages. That's a problem."** CNET. May 24, 2021.
https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/

115 https://cyber.gc.ca/en/guidance