ISSN 2816-9174
CAT D98-4E-PDF

CANADIAN CENTRE FOR CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT

2025
2026

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

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

ISSN 2816-9174
CAT D98-4E-PDF

Table of contents

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 Canada (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, 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, municipal, and Indigenous governments, and private sector partners to solve Canada's most complex cyber challenges
- developing and sharing our specialized cyber defence technology and knowledge
- defending cyber systems, including Government of Canada networks, by developing and deploying sophisticated cyber defence tools and technology
- leading the Government of Canada'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.

Minister's foreword

Cyber threats to Canada are becoming more complex and sophisticated, threatening our national security and economic prosperity. As a nation with a significant global presence, Canada is a valuable target for cybercriminals looking to make a profit and state adversaries aiming to disrupt the systems we rely on.

In the last two years, we have witnessed a sharp increase in both the number and severity of cyber incidents, many of which target our essential services. Actors outside our borders have also attempted to influence public opinion and intimidate our population, including in the Canadian diaspora, through coordinated cyber campaigns.

The Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025-2026 is an instrumental tool in our comprehension of cyber threats to Canada. The threat assessment draws on public reporting and classified intelligence to paint an overall picture of the current threat landscape, while also forecasting future trends. By offering reliable and timely information, the report empowers Canadian organizations and individuals to prepare for and defend against current and emerging threats.

Deepening our understanding of cyber threats enables us to enhance our readiness and, as threats evolve, the Cyber Centre will continue to look for new ways to combat them. Its team is at the forefront of enhancing our cyber security to protect Canadians. Our government is supporting their invaluable work and Budget 2024 allocates $917.4 million to enhance intelligence and cyber operations programs to respond to evolving national security threats.

The insights provided in this threat assessment are critical as we work to strengthen Canada's security in an increasingly digital world.

The Honourable Bill Blair
Minister of National Defence

Message from the Head of the Cyber Centre

It's hard to believe it's already been two years since our last report. At first glance, it seems that the cyber threat environment hasn't changed much. Cybercrime remains a persistent threat, ransomware attacks continue to target our critical infrastructure, and state-sponsored cyber threat activity is still affecting Canadians.

What has changed, however, is that state adversaries are getting bolder and more aggressive. Cybercriminals driven by profit are increasingly benefiting from new illicit business models to access malicious tools and are using artificial intelligence to enhance their capabilities. Non-state actors are seizing on major global conflicts and political controversies to carry out disruptive activities.

These new developments and other trends are outlined in detail in this edition of the National Cyber Threat Assessment. This year's report goes further than previous editions, offering more tangible examples of cyber threat activity in Canada and around the world, as well as providing some of our own statistics on cyber incidents.

While our assessments describe trends that should concern anyone who reads about them, you can rest assured that the Cyber Centre remains focused on tackling these threats. Working in close collaboration with the private sector, industry, government and critical infrastructure, we're helping to protect the systems that are vital to our daily lives.

Whether you're a first-time reader or an avid consumer, an individual Canadian or a member of a small, medium or large organization, I'm confident that you will find the information in this report insightful. I hope that it also encourages you to reflect on what you can do to contribute to our collective resilience. After all, we all have a role to play in building a safer, more secure Canada.

Sincerely,

Rajiv Gupta
Head, Canadian Centre for Cyber Security

Executive summary

Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors, from cybercriminals to hacktivists, that are targeting our critical infrastructure and endangering our national security. These cyber threat actors are evolving their tradecraft, adopting new technologies, and collaborating in an attempt to improve and amplify their malicious activities.

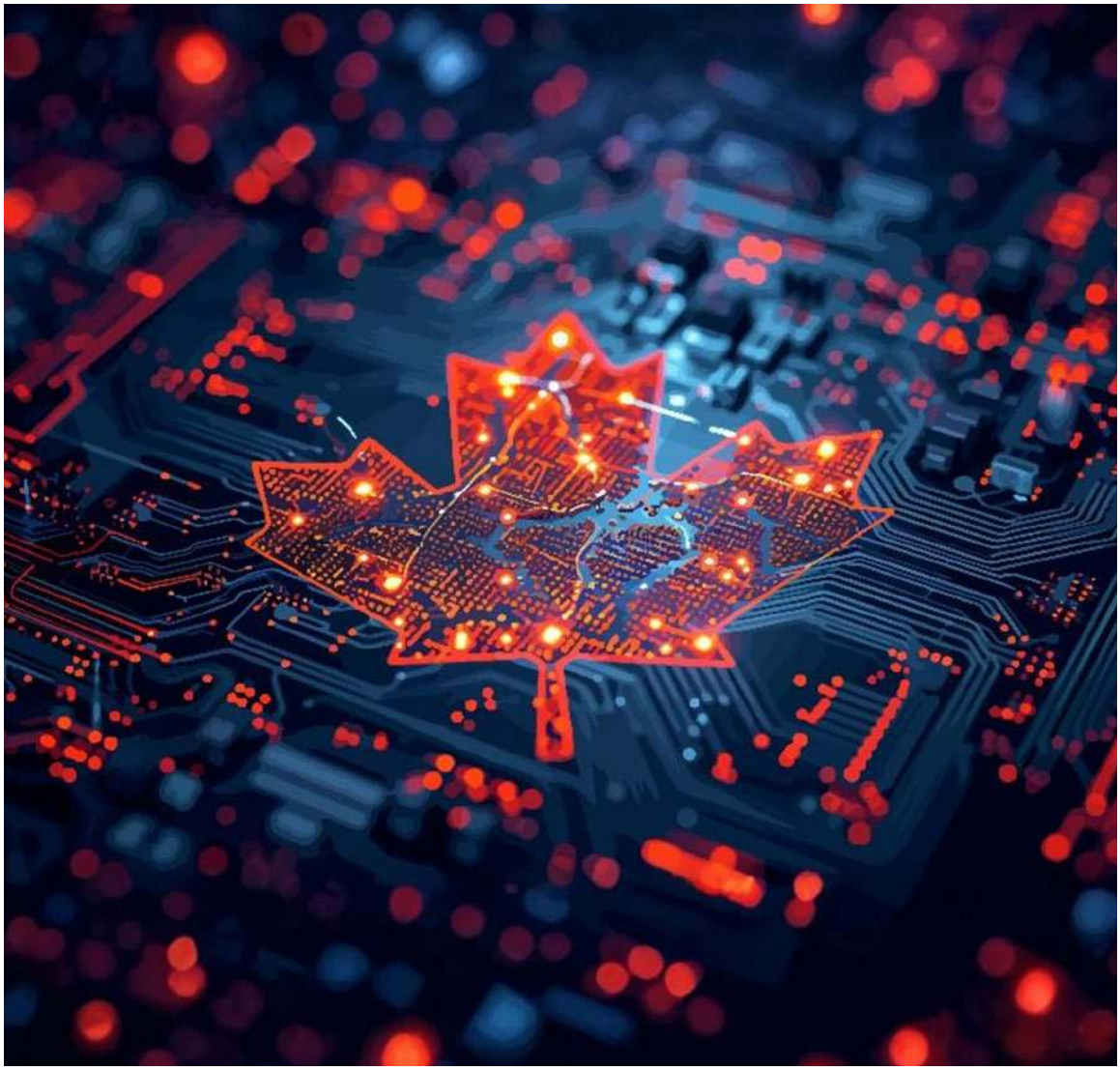
Canada's state adversaries are becoming more aggressive in cyberspace. State-sponsored cyber operations against Canada and our allies almost certainly extend beyond espionage. State-sponsored cyber threat actors are almost certainly attempting to cause disruptive effects, such as denying service, deleting or leaking data, and manipulating industrial control systems, to support military objectives and/or information campaigns. We assess that our adversaries very likely consider civilian critical infrastructure to be a legitimate target for cyber sabotage in the event of a military conflict.

At the same time, cybercrime remains a persistent, widespread, and disruptive threat to individuals, organizations, and all levels of government across Canada that is sustained by a thriving and resilient global cybercrime ecosystem. We assess that the financial motivations underpinning cybercrime will almost certainly drive the cybercrime ecosystem to continuously evolve and diversify as cybercriminals attempt to evade authorities.

Key judgements

- **Canada's state adversaries are using cyber operations to disrupt and divide.** State-sponsored cyber threat actors are almost certainly combining disruptive computer network attacks with online information campaigns to intimidate and shape public opinion. State-sponsored cyber threat actors are very likely targeting critical infrastructure networks in Canada and allied countries to pre-position for possible future disruptive or destructive cyber operations.
- **The People's Republic of China's (PRC) expansive and aggressive cyber program presents the most sophisticated and active state cyber threat to Canada today.** The PRC conducts cyber operations against Canadian interests to serve high-level political and commercial objectives, including espionage, intellectual property (IP) theft, malign influence, and transnational repression. Among our adversaries, the PRC cyber program's scale, tradecraft, and ambitions in cyberspace are second to none.
- **Russia's cyber program furthers Moscow's ambitions to confront and destabilize Canada and our allies.** Canada is very likely a valuable espionage target for Russian state-sponsored cyber threat actors, including through supply chain compromises, given Canada's membership in the North Atlantic Treaty Organization, support for Ukraine against Russian aggression, and presence in the Arctic. Pro-Russia non-state actors, some of which we assess likely have links to the Russian government, are targeting Canada in an attempt to influence our foreign policy.

- **Iran uses its cyber program to coerce, harass, and repress its opponents, while managing escalation risks.** Iran's increasing willingness to conduct disruptive cyber attacks beyond the Middle East and its persistent efforts to track and monitor regime opponents through cyberspace present a growing cyber security challenge for Canada and our allies.
- **The Cybercrime-as-a-Service (CaaS) business model is almost certainly contributing to the continued resilience of cybercrime in Canada and around the world.** The CaaS ecosystem is underpinned by flourishing online marketplaces where specialized cyber threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals. This has almost certainly enabled a growing number of actors with a range of capabilities and expertise to carry out cybercrime attacks and evade law enforcement detection.
- **Ransomware is the top cybercrime threat facing Canada's critical infrastructure.** Ransomware directly disrupts critical infrastructure entities' ability to deliver critical services, which can put the physical and emotional wellbeing of victims in jeopardy. In the next two years, ransomware actors will almost certainly escalate their extortion tactics and refine their capabilities to increase pressure on victims to pay ransoms and evade law enforcement detection.



About this threat assessment

The National Cyber Threat Assessment 2025-2026 (NCTA 2025-2026) highlights the cyber threats facing individuals and organizations in Canada. It provides an update to the National Cyber Threat Assessment 2018[1] (NCTA 2018), the National Cyber Threat Assessment 2020[2] (NCTA 2020), and the National Cyber Threat Assessment 2023-2024[3] (NCTA 2023-2024), with analysis of the interim years and forecasts until 2026. We recommend reading the NCTA 2025-2026 along with the Introduction to the Cyber Threat Environment[4] and the advice and guidance that we have released as companions to this assessment.

We prepared this assessment to help Canadians shape and sustain our nation's cyber resilience. It is only when the government, the private sector, and the public work together that we can build resilience to cyber threats in Canada.

Sources

The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on CSE's knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides CSE 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 assessment methodology 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 **September 20, 2024**.

Limitations

This assessment does not provide an exhaustive list of all cyber threat activity in Canada or mitigation advice. The purpose of this threat assessment 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 can be found on the Cyber Centre website and on the Get Cyber Safe website.[5]

Estimative language

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

Introduction

Canada has entered a new era of cyber vulnerability where cyber threats are ever-present, and Canadians will increasingly feel the impact of cyber incidents that have cascading and disruptive effects on their daily lives.

Advancements in communications and computing technologies have ushered in a world of ubiquitous connectivity for Canadians. In this environment, online platforms and digital technologies continue to shape and mediate Canadians' interactions with the physical world—the way we work, shop, travel, socialize, get informed, and access critical services.[6] These systems record and process vast amounts of data about us, often over poorly secured or untrustworthy digital networks.[7] These systems are also interconnected and fragile: cyber incidents, from cyber attacks to flawed software updates, can knock airlines, hospitals, banks, and retailers around the world offline.[8]

CSE and its partners in Canada and across the Five Eyes are attuned to the cyber threats to Canada from state and non-state cyber threat actors and are tracking them as they evolve. NCTA 2025-2026 provides the Canadian public with CSE's current insights on the state and non-state cyber threat actors conducting malicious cyber threat activity against Canada and how we assess the cyber threat landscape will evolve in the next two years. This assessment is divided into three sections that are designed to stand independently and together.

- **Section 1—Cyber threat from state adversaries:** introduces the state cyber threat ecosystem and discusses the cyber threats to Canada from
  - the People's Republic of China (PRC)
  - the Russian Federation (Russia)
  - the Islamic Republic of Iran (Iran)
  - the Democratic People's Republic of Korea (DPRK)
  - the Republic of India (India)
- **Section 2—Cybercrime threats:** discusses the interconnectivity of the Cybercrime-as-a-Service (CaaS) ecosystem and the cybercrime threats facing Canada, specifically from fraud, scams, and ransomware. This section also highlights the ransomware threat to Canada's critical infrastructure.
- **Section 3—Trends shaping Canada's cyber threat landscape:** identifies five trends that will shape Canada's cyber threat landscape and drive cyber threat activity impacting Canadians up to 2026.

Readers interested in more detailed information on the evolving cyber threat landscape, including definitions of important terms and concepts referenced in this NCTA, are invited to consult the following:

- An Introduction to the Cyber Threat Environment[9]
- Cyber Threats to Canada's Democratic Process: 2023 update[10]
- The threat from large language model text generators[11]

CYBER THREAT FROM **STATE ADVERSARIES**

Canada is confronting an expanding and more complex state cyber ecosystem

Strategic adversaries

The cyber programs of the PRC, Russia, and Iran remain the greatest strategic cyber threats to Canada. These countries are united in their desire to challenge United States (U.S.) dominance in multiple domains, including cyberspace, and promote an authoritarian vision for Internet governance and domestic surveillance.[12] The PRC's cyber program surpasses other hostile states in both the scope and resources dedicated to cyber threat activity against Canada.

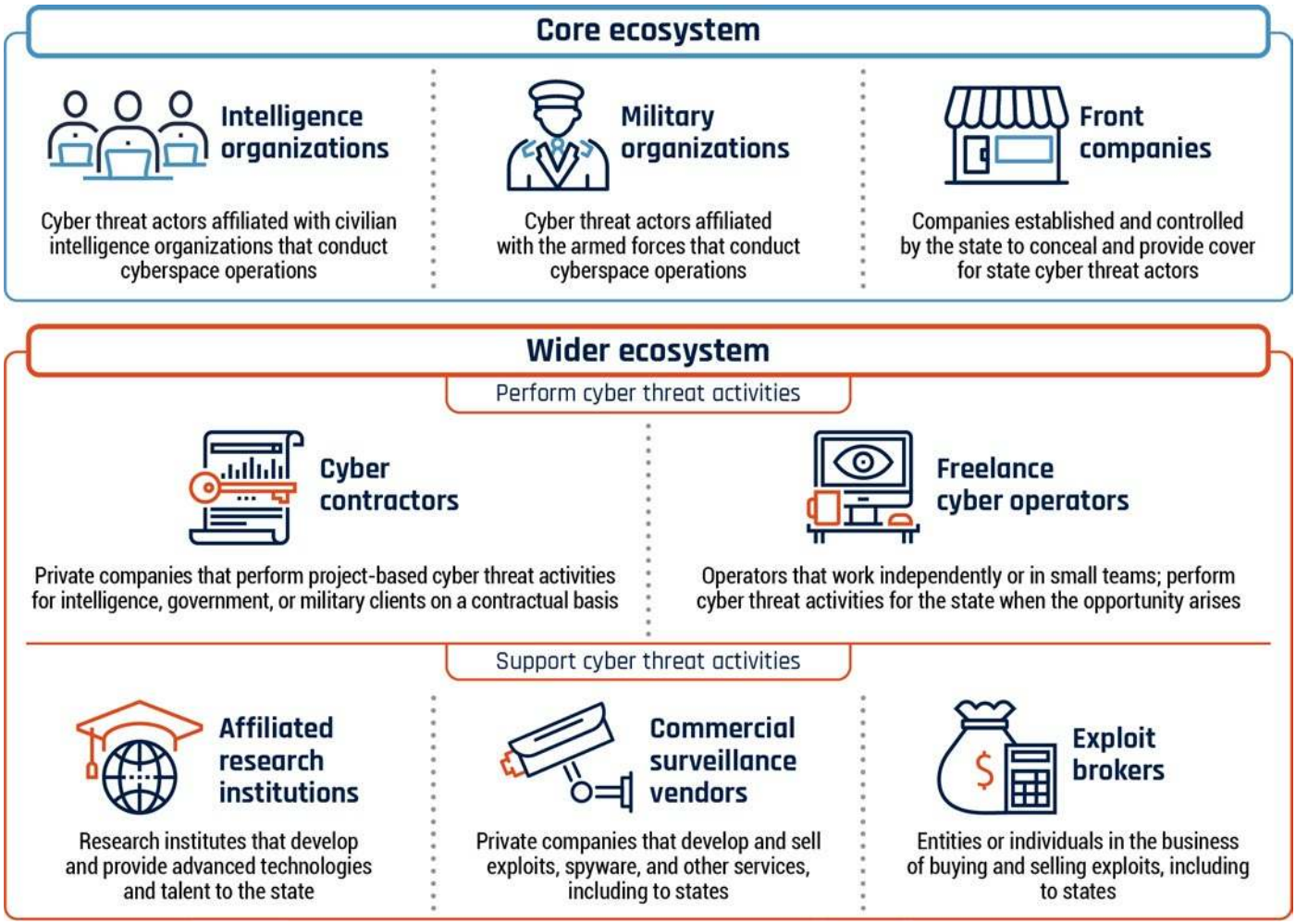
Emerging cyber programs

At the same time, countries that aspire to become new centres of power within the global system, such as India, are building cyber programs that present varying levels of threat to Canada.[13] While emerging states focus their cyber efforts on domestic threats and regional rivals, they also use their cyber capabilities to track and surveil activists and dissidents living abroad.

Wider cyber ecosystem

Both advanced and emerging states are leveraging a complex ecosystem of commercial surveillance vendors, contractors, and affiliated research institutions to support or perform cyber threat activities (Figure 1).[14] States use these entities to mask their cyber operations or to acquire exploits, digital infrastructure, and data. Emerging states are very likely using the wider ecosystem to try and move up the ladder of sophistication and acquire capabilities that may be beyond their capacity to develop internally.

Figure 1: State cyber program ecosystem[15]



People's Republic of China

The PRC presents the most sophisticated and active cyber threat to Canada

The PRC's expansive and aggressive cyber program has global cyber surveillance, espionage, and attack capabilities and is the most comprehensive cyber security threat facing Canada today. Canada, along with our Five Eyes partners, is an ongoing target for the PRC's cyber program. The PRC conducts cyber operations against Canadian interests to serve high-level political and commercial objectives, including espionage, IP theft, malign influence, and transnational repression. Among our adversaries, the PRC cyber program's scale, tradecraft, and ambitions in cyberspace are second to none.

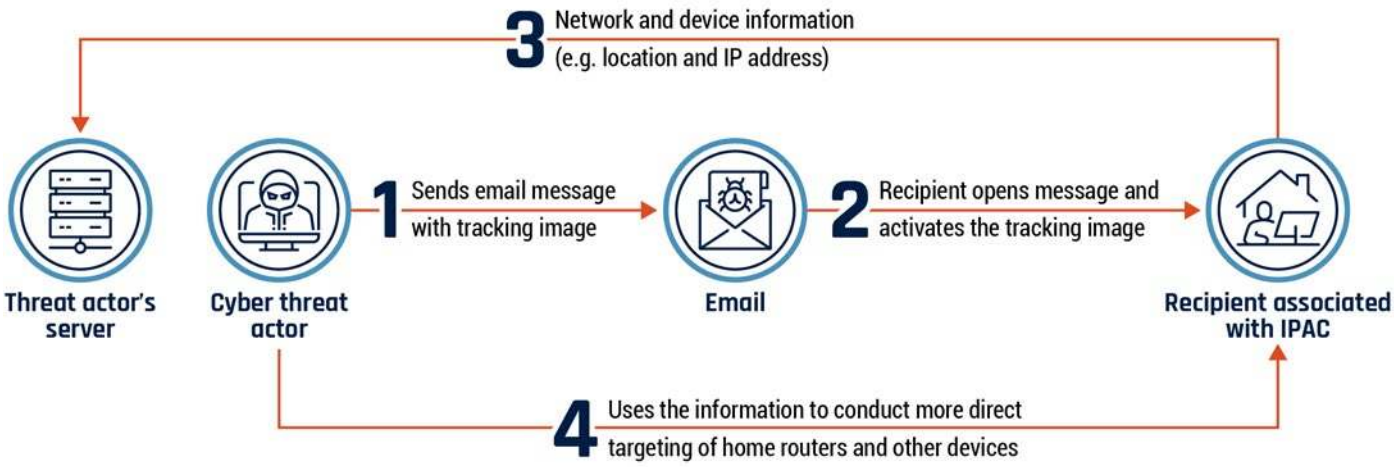
The PRC targets all levels of government and public officials for valuable intelligence

PRC state-sponsored cyber threat actors persistently conduct cyber espionage against federal, provincial, territorial, municipal, and Indigenous government networks in Canada. PRC cyber threat actors have compromised and maintained access to multiple government networks over the past five years, collecting communications and other valuable information.[16] While all known federal government compromises have been resolved, it is very likely that the actors responsible for these intrusions dedicated significant time and resources to learn about the target networks.

Over the past four years, at least 20 networks associated with Government of Canada agencies and departments have been compromised by PRC cyber threat actors.

PRC state-sponsored cyber threat actors also target Canadian government officials, particularly individuals that the PRC perceives as being critical of the Chinese Communist Party (CCP). According to a U.S. Department of Justice indictment, in 2021, PRC state-sponsored cyber threat actors targeted members of the Inter-Parliamentary Alliance on China (IPAC), a group of global lawmakers whose stated purpose is to counter the threats posed by the CCP to the international order and democratic principles. The threat actors sent email messages with tracking images to recipients to conduct network reconnaissance (see Figure 2).[17] A number of Canadian politicians who are members of IPAC have come forward to confirm that they were targeted in this operation.[18]

Figure 2: PRC email operation against members of Inter-Parliamentary Alliance on China



The PRC targets Canadian government networks and public officials to acquire information that will advance its strategic, economic, and diplomatic interests, and give the PRC government an advantage in China-Canada bilateral relations and commercial matters. For example, provincial and territorial governments are likely a valuable target given that they have decision-making power over regional trade and commerce, including resource extraction (e.g., energy and critical minerals).[19] In addition to fulfilling PRC intelligence collection priorities, the information collected is also likely used to support the PRC's malign influence and interference activities against Canada's democratic processes and institutions.

PRC cyber threat activity against Canada appears to intensify following events that increase bilateral tensions between Canada and the PRC. In this context, PRC cyber threat activity is likely designed to gather timely intelligence on official reactions and to monitor unfolding developments.

PRC cyber-enabled transnational repression targets individuals in Canada

PRC cyber threat actors very likely support China's actions abroad designed to silence activists, journalists, diaspora communities, and other groups that the PRC views as security threats. These groups, collectively referred to by PRC officials as the "Five Poisons," include:

- Falun Gong practitioners
- Uyghurs
- Tibetans
- supporters of Taiwanese independence
- pro-democracy activists

PRC actors very likely facilitate transnational repression by monitoring and harassing these groups online and tracking them using cyber surveillance.[20] For example, the PRC has been publicly linked to cyber espionage operations against the Uyghur minority group, including members living in Canada, using spear phishing emails and spyware.[21]

The PRC government very likely leverages Chinese-owned technology platforms, some of which likely cooperate with the PRC's intelligence and security services, to facilitate transnational repression.[22]

The PRC targets Canada's private sector and innovation ecosystem for competitive advantage

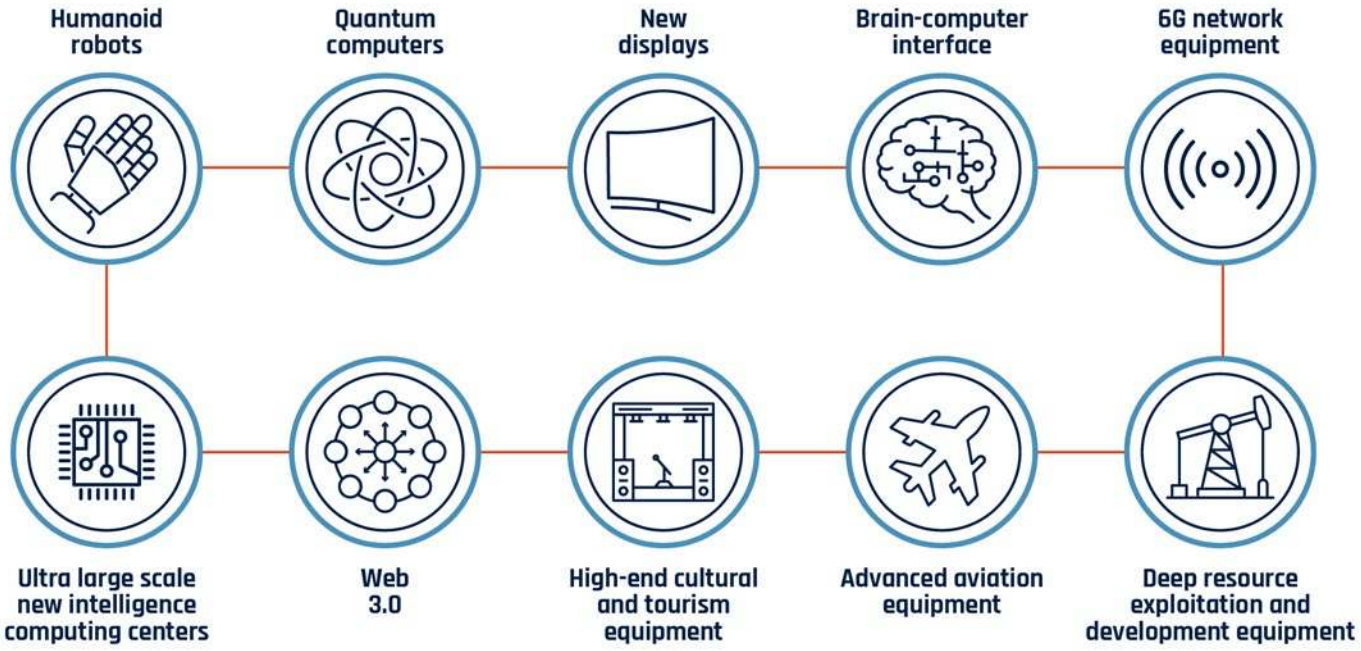
Canada's innovation ecosystem has been a long-standing priority of PRC intelligence collection. The PRC cyber program almost certainly continues to support the PRC's espionage activities against Canada's private sector, academia, supply chains, and government-affiliated research and development (R&D). PRC cyber threat actors have very likely stolen commercially sensitive data from Canadian firms and institutions.

The PRC uses cyber contractors and freelancers to support espionage

The PRC uses a competitive marketplace of contract and freelance cyber actors to support the PRC's intelligence collection requirements. For example, I-Soon is a PRC-based private contractor that provides "hacker-for-hire" services. According to leaked documents, the company worked on projects on a contractual basis for various PRC government and military entities and state-owned enterprises. I-Soon reportedly sold exfiltrated data from targets to its clients.[23]

PRC cyber threat actors targeting Canada likely prioritize collecting confidential and proprietary information that supports the PRC's economic and military interests and that can help accelerate the PRC's development of advanced and strategic technologies (Figure 3). The PRC will likely intensify its espionage activities against Canada's innovation sector as economic tensions between the PRC and Canada (and our allies) rise.[24]

Figure 3: Future industries "iconic products" identified as priorities for PRC industrial policy (2024)[25]



PRC pre-positioning within United States critical infrastructure increases risk to Canada

In a strategic shift, the PRC is very likely integrating offensive cyber operations into its military planning to gain an advantage during a potential conflict with the U.S. PRC state-sponsored cyber threat actors, tracked as Volt Typhoon, are almost certainly seeking to pre-position within U.S. critical infrastructure networks for disruptive or destructive cyber attacks in the event of a major crisis or conflict with the U.S. According to U.S. officials, the PRC's operation is designed to slow the U.S. military's response and to sow societal panic.[26] Volt Typhoon is especially noteworthy because the PRC has not historically conducted disruptive or destructive cyber operations against critical infrastructure.[27]

We assess that the direct threat to Canada's critical infrastructure from PRC state-sponsored cyber threat actors is likely lower than that to U.S. infrastructure. While the focus of future PRC cyber warfare operations will likely be concentrated on the U.S., disruptive or destructive cyber threat activity against integrated North American critical infrastructure, such as pipelines, power grids, and rail lines, would likely affect Canada as well due to cross-border interoperability and interdependence.[28]

Russian Federation

Russia is leveraging its cyber program to confront the West

Russia's unpredictable cyber program routinely challenges existing norms in cyberspace and furthers Moscow's ambitions to confront and destabilize Canada and our allies.

Russia almost certainly views its cyber program as part of a multi-layered strategy to influence and shape the information environment. Russia combines conventional cyber espionage and computer network attacks with disinformation and influence operations to:[29]

- promote Russia's global status and reinforce pro-Russia narratives
- erode trust in democratic institutions
- generate popular support for Russia's war efforts, both at home and abroad
- psychologically weaken or embarrass its opponents

Russia's cyber threat activities are supported by a network of state and non-state cyber actors, including an ever-shifting group of Russia-nexus cybercriminals, hacktivists, and "hackers-for-hire" who are likely motivated by a mix of patriotism, profit, or opportunism. This hybrid strategy, which provides Russia with deniability, appears to have been emulated by other states, creating a more complex cyber threat environment for Canada and our allies.[30]

Russian cyber threat actor conducts destructive cyber attack against Ukraine for psychological effects

In December 2023, a Russian cyber threat actor conducted a destructive wiper cyber attack against the Ukrainian telecom company Kyivstar, leaving millions of Ukrainians without Internet and mobile service for days. The cyber threat actor was reportedly in Kyivstar's systems since at least May 2023 and may have been able to steal subscriber information and intercept SMS messages. The actor claimed credit for the attack in a Telegram post addressed to Ukrainian President Volodymyr Zelenskyy. According to Ukrainian officials, the aim of the destructive attack was to land a psychological blow against Ukraine.[31]

Russia targets Canada for espionage

Canada is very likely a valuable espionage target for Russian state-sponsored cyber threat actors given Canada's membership in the North Atlantic Treaty Organization, support for Ukraine, and presence in the Arctic. Russian cyber threat actors are very likely targeting Canadian government, military, private sector, and critical infrastructure networks as part of Russia's foreign and military intelligence collection operations.[32]

Public and private sector organizations in Canada are also vulnerable to global supply chain compromises by Russian cyber threat actors. For example, in 2020, Russian state-sponsored cyber threat actors compromised the supply-chain by implanting malware into a SolarWinds software update.[33] Russian-state-sponsored cyber threat actors are almost certainly targeting cloud-based services with large numbers of customers in Canada.[34]

Russian cyber threat actors compromise Microsoft corporate email system for espionage

In January 2024, Microsoft detected that a Russian state-sponsored cyber threat actor publicly tracked by Microsoft as Midnight Blizzard had breached Microsoft's cloud-based enterprise email service. Midnight Blizzard accessed Microsoft's own corporate email accounts, exfiltrating correspondences between Microsoft and government officials in Canada, the U.S., and the United Kingdom.[35] According to Microsoft, the Russian cyber threat actor was initially seeking information about itself.[36] The threat actor later used personal data and credentials in the emails to attempt to gain access to Microsoft customer systems.

Pro-Russia non-state cyber threat actors target Canada to influence our foreign policy

Following Russia's invasion of Ukraine in 2022, pro-Russia non-state (PRNS) cyber threat actors, some of which we assess likely have links to the Russian government and intelligence services, have almost certainly conducted disruptive cyber threat activity against Canada and leveraged social media to draw attention to these attacks (Figure 4).[37] We assess that the intent of these campaigns is very likely to influence and undermine Canada's support for Ukraine. For example, a distributed denial of service (DDoS) attack campaign in April 2023 by PRNS actors against Government of Canada and Canadian private sector websites coincided with the Ukrainian Prime Minister's visit to Canada.[38]

Although PRNS cyber threat activity against Canada has primarily consisted of DDoS attacks and website defacements, some PRNS actors have attempted to compromise operational technology (OT) systems within critical infrastructure in North America and Europe with the intent to disrupt those systems. This activity opportunistically targets Internet-accessible devices and exploits basic vulnerabilities, such as insecure remote access software or the use of default passwords.[39] For example, in January 2024, a PRNS group claimed responsibility for the overflow of water storage tanks at water facilities in Texas. The group reportedly posted a video of the compromise and manipulation of control systems at each facility on a public forum.[40]

We assess that PRNS actors will likely attempt to disrupt vulnerable Internet-connected OT systems within Canadian critical infrastructure when the opportunity arises. PRNS cyber threat activity against OT may cause systems to malfunction, leading to damage or destruction of those systems and possible harm to public safety.

Figure 4: Notable examples of pro-Russia non-state cyber threat activity against Canada (2023)[41]

February 2023

Pro-Russia non-state cyber groups participate in a cyber campaign attempting to sabotage critical infrastructure in countries providing assistance to Ukraine, including Canada.

April 2023

Pro-Russia non-state cyber group claims responsibility for DDoS campaign against Canadian websites, including the Prime Minister's Office's public-facing website.

September 2023

Pro-Russia non-state cyber group claims responsibility for a DDoS campaign against Canadian websites, including Quebec provincial government websites.

Islamic Republic of Iran

Iran is expanding its disruptive cyber threat activity against the West

Iran has an aggressive cyber program that the regime uses to coerce, harass, and repress Iran's opponents, while managing escalation risks. Iran's increasing willingness to conduct disruptive cyber attacks beyond the Middle East, and its persistent efforts to track and monitor regime opponents through cyberspace present a growing cyber security challenge for Canada and our allies.

Iran has taken advantage of its back-and-forth cyber confrontation with Israel to improve its cyber espionage and offensive cyber capabilities and hone its information campaigns, which it is now almost certainly deploying against targets in the West.[42] While it is unlikely that Canada is, at present, a priority target of Iran's cyber program, Iranian cyber threat actors likely have access to computer networks in Canada, including critical infrastructure.

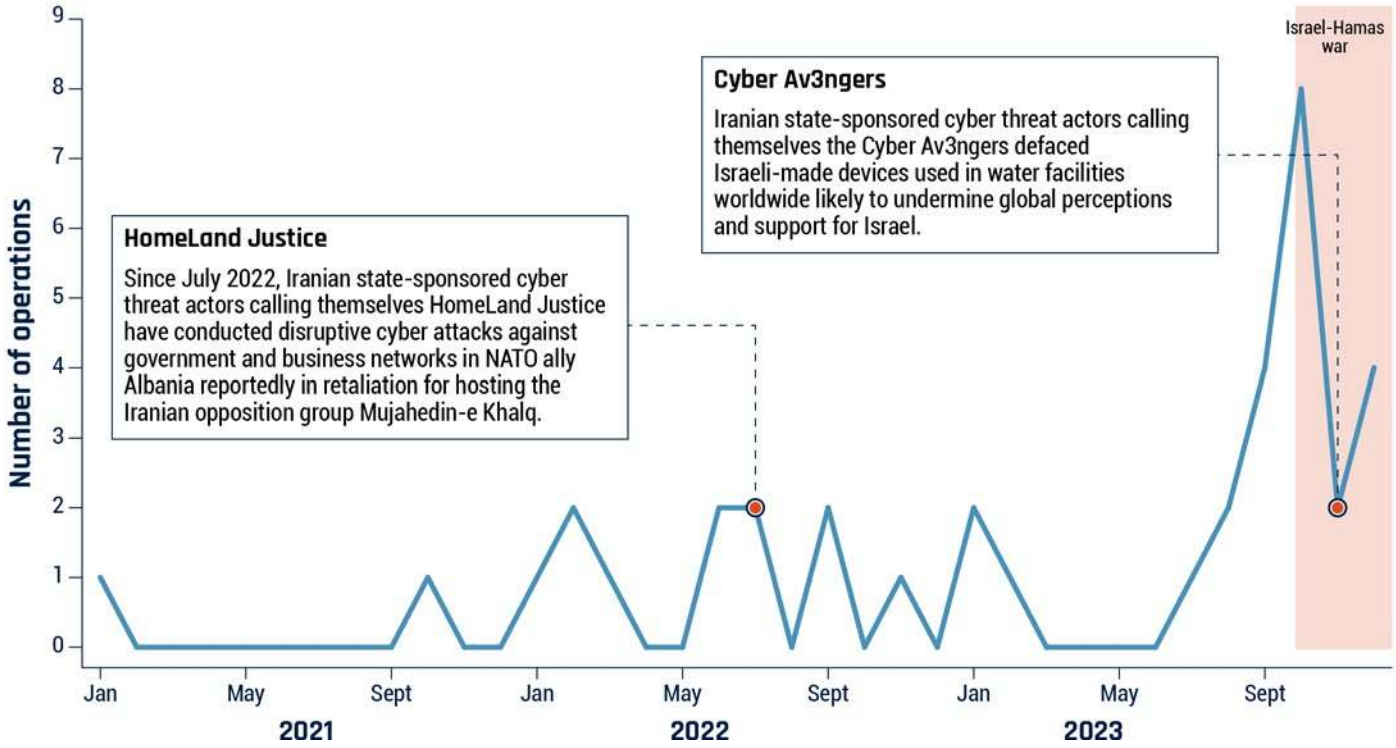
Iran's global coercive cyber operations present a risk to Canada

Iranian state-sponsored cyber threat actors have planned and conducted multi-stage disruptive cyber operations around the world to intimidate Iran's opponents, signal the regime's displeasure, and persuade a country to change its behaviour (Figure 5).[43]

Iranian cyber threat actors have performed denial of service attacks, attempted to manipulate industrial control systems, and accessed government and private networks to encrypt, wipe, and leak data. Iran has developed a network of hacktivist personas and social media channels that exploit these disruptive events to spread the regime's messages and influence the target society while keeping Tehran's official involvement ambiguous and deniable.[44]

We assess that escalation of tensions in Canada-Iran bilateral relations would very likely increase the risk that Canada would be a target of Iranian coercive cyber operations.

Figure 5: Coercive cyber operations publicly linked to Iran (2021-2023)[45]



Iran uses social engineering for transnational repression and espionage

Iranian state-sponsored cyber threat actors likely track and monitor individuals in Canada whom the Iranian regime considers a threat, such as political activists, journalists, human rights researchers, and members of the Iranian diaspora. Iranian cyber threat groups are particularly sophisticated in combining social engineering with spear phishing to support Iran's transnational repression and surveillance activities (Figure 6).[46] For example, Iran has very likely used the downing of Flight 752 over Tehran as a thematic lure for its social engineering and spear phishing operations. These efforts are especially concerning given recent public reports linking Iran to kidnapping and assassination plots against regime opponents living in the West.[47]

Figure 6: Elements of an Iranian social engineering campaign

Iran also uses its social engineering efforts to target public officials and gain access to government networks and private sector organizations globally, including in the aerospace, energy, defence, travel, and telecommunications sectors, in pursuit of its intelligence collection requirements.[48]

The Democratic People's Republic of Korea

The DPRK has a dual-purpose cyber program that prioritizes revenue generation alongside the pursuit of the regime's strategic and intelligence requirements. DPRK state-sponsored cyber threat actors routinely engage in cybercrime activities, such as ransomware and cryptocurrency theft, to fund the regime's political and military ambitions as well as the cyber program's own operations.[49] These financially motivated attacks are very likely conducted under the overarching strategic direction and protection of the North Korean regime, which likely tolerates cybercrime activities that have harmful and disruptive effects.[50]

While we assess that the DPRK's cyber program almost certainly does not pose a strategic cyber threat to Canada on par with countries like the PRC and Russia, the regime's commitment to cybercriminal statecraft almost certainly presents a persistent and well-resourced cybercrime threat to individuals and organizations in Canada across a broad range of industries and sectors of the economy. The DPRK will almost certainly continue to adapt and pivot to new cybercriminal enterprises as digital technologies evolve.[51]

Republic of India

India's leadership almost certainly aspires to build a modernized cyber program with domestic cyber capabilities.[52] India very likely uses its cyber program to advance its national security imperatives, including espionage, counterterrorism, and the country's efforts to promote its global status and counter narratives against India and the Indian government. We assess that India's cyber program likely leverages commercial cyber vendors to enhance its operations.[53]

We assess that Indian state-sponsored cyber threat actors likely conduct cyber threat activity against Government of Canada networks for the purpose of espionage. We judge that official bilateral relations between Canada and India will very likely drive Indian state-sponsored cyber threat activity against Canada.

2

CYBERCRIME **THREATS**

Interconnected online cybercrime ecosystem facilitates Cybercrime-as-a-Service

Financially motivated and opportunistic cybercrime continues to be the cyber threat activity that is most likely to affect Canadians and Canadian organizations. We judge that the continued resilience of cybercrime in Canada and around the world is almost certainly due, in part, to the rise of the Cybercrime-as-a-Service (CaaS) business model. With CaaS, specialized threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals online, enabling their illicit activities.[54]

CaaS services available online for cybercriminals to purchase

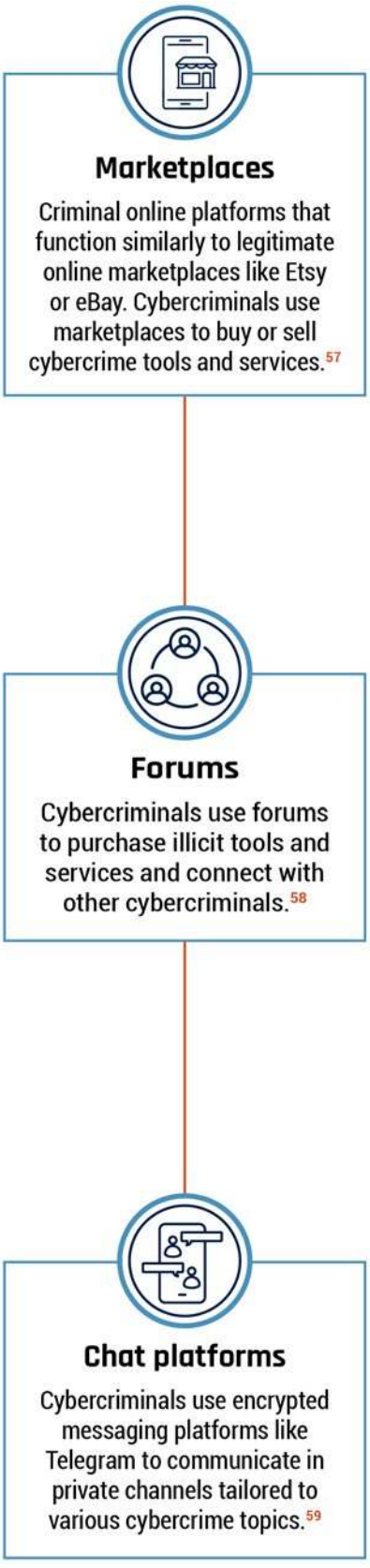
- **Malware-as-a-Service:** services to support the development and deployment of malware that can steal or encrypt victim data or gain remote control of victim systems
- **Ransomware-as-a-Service (RaaS):** a core group of developers will sell or lease their ransomware variant to other threat actors, called affiliates; the core developers will support affiliates' deployment of their ransomware in exchange for upfront payment, subscription fees, a cut of profits, or all three
- **Access-as-a-Service:** specialized threat actors gain access to victim systems and sell access to compromised systems to clients
- **Phishing-as-a-Service (PaaS):** detailed instructions, email templates, and ready-to-use tools for executing phishing attacks
- **DDoS-as-a-Service:** rented out botnets and user-friendly interfaces for clients to conduct DDoS attacks
- **Exploits-as-a-Service:** specialized actors lease or rent exploit kits and support clients on how to use exploits against software vulnerabilities

We assess that CaaS has almost certainly increased the number of actors participating in cybercrime by lowering the barrier to entry and enabling actors who are less technically sophisticated to carry out cybercrime attacks. Even large cybercriminal groups leverage CaaS offerings such as malware, cyber attack infrastructure (e.g., hosting infrastructure) and money laundering services to increase their capacity for cybercrime activity.[55]

Online platforms play an important role in enabling cybercrime

The cybercrime ecosystem is highly interconnected. Online platforms such as cybercrime marketplaces, forums and chat platforms facilitate the sale and resale of stolen data as well as interactions between CaaS providers and cybercriminals seeking their services. These online platforms also play a significant role by facilitating professional connections and resource sharing between a range of cybercriminals.[56]

Figure 7: How cybercriminals use online platforms



Genesis Market

Genesis Market was a cybercriminal marketplace that sold credentials stolen from millions of compromised computers worldwide. Cybercriminals used Genesis to purchase account access credentials and digital fingerprints, which allowed them to access victims' online accounts without triggering security warnings. Genesis Market has been linked to millions of financially motivated cyber incidents, including fraud and ransomware attacks,[60] from its inception in March 2018 until it was disrupted by law enforcement in April 2023.[61]

Fraud and scams remain a persistent threat to Canadians

As assessed in NCTA 2023-2024, we judge that fraud and scams are almost certainly the most common forms of cybercrime impacting Canadians. Cybercriminals attempt to steal personal, financial, and corporate information using social engineering tactics like phishing.[62] Phishing is one of the most reported types of fraud in Canada and spear phishing has one of the highest reported levels of financial impact to victims.[63] For example, spear phishing can lead to compromises that result in the theft of sensitive data and can cause significant financial losses for businesses.[64]

Figure 8: Losses from fraud in Canada (in CAD)[65]

Phishing attacks becoming more accessible and sophisticated with new tools and services

We judge that the threat from fraud and scams will continue to grow in the next two years with the proliferation of Phishing-as-a-Service kits that cybercriminals can purchase online, as well as chatbots powered by artificial intelligence (AI) that craft convincing phishing emails for cybercriminals. These tools make phishing attacks more accessible for cybercriminals who are less technically sophisticated.[66]

Ransomware threat to Canada continues to grow and evolve

Ransomware is one of the most disruptive forms of cybercrime facing Canada and our allies. Since 2020, ransomware attacks have increased in scope, frequency, and complexity.[67] We judge that ransomware will almost certainly continue to be the most impactful cyber threat facing Canadian organizations in the next two years as ransomware actors constantly refine their tactics to maximize profits.[68]

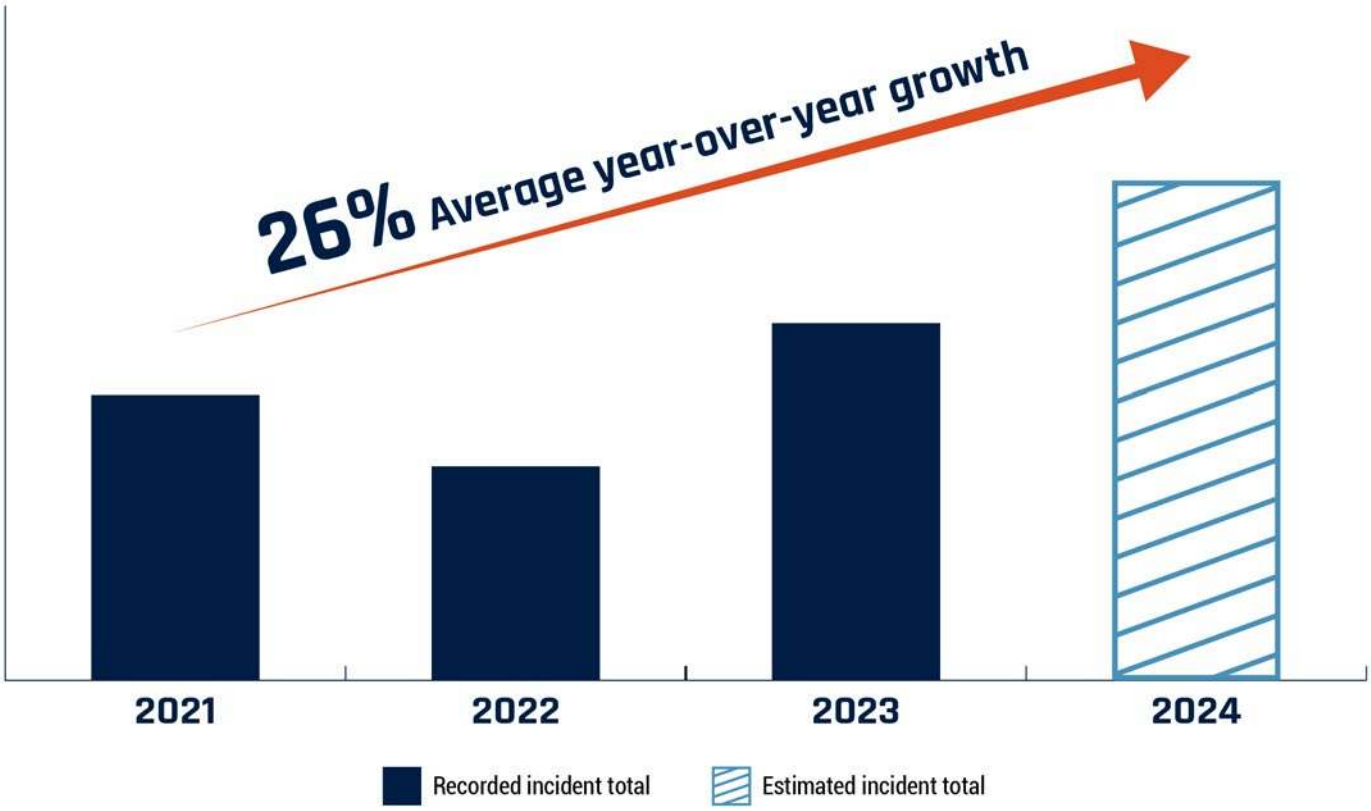
Ransomware incidents and ransom payments are growing

2023 was a record-breaking year for ransomware. By some estimates, the global number of ransomware incidents rose 74% in 2023 compared with 2022,[69] and global ransom payments reached a record of $1 billion USD.[70] By one estimate, the average ransom paid in Canada in 2023 was $1.130 million CAD, an increase of almost 150% in two years.[71] Open-source reporting reveals that these trends continued into the first half of 2024, with ransom payments and incidents on track to exceed numbers observed in 2023.[72] Observed increases in ransomware are almost certainly higher since many incidents go unreported.[73] We judge that the ransomware threat will almost certainly continue to grow in the next two years unless significant disruptions to the ransomware ecosystem occur.

Global top ransomware threats 2023

1. **LOCKBIT:** LockBit is a RaaS cybercrime group that operates a ransomware variant of the same name that has been used to impact a wide range of critical infrastructure entities, including healthcare, energy, and government organizations.[74]
2. **ALPHV:** ALPV is a RaaS cybercrime group that operates the ransomware variant named BlackCat and has been used to impact a wide range of industries, including financial, manufacturing, legal, and professional services organizations.[75]
3. **CL0P:** CL0P is a RaaS operated by the Russian-speaking cybercriminal group TA505 that has been used to impact a wide range of industries by exploiting unpatched software vulnerabilities.[76]
4. **PLAY:** Play is a RaaS cybercrime group operating a ransomware variant of the same name that has been used to impact healthcare and manufacturing organizations.[77]
5. **BLACK BASTA:** Black Basta is a RaaS cybercrime group operating a ransomware variant of the same name that has been used to impact critical infrastructure entities, including healthcare and government organizations.[78]

Figure 9: Relative growth from 2021 of Canadian ransomware incidents known to the Cyber Centre[79]



In 2022, we judged that ransomware incidents decreased, in part, due to heightened law enforcement pressure that likely caused some ransomware actors to temporarily pause their activities. Russia's invasion of Ukraine also likely caused disruptions in the ransomware ecosystem. For example, some ransomware actors likely shifted their focus from financially motivated cybercrime to politically motivated attacks.[80] However, in 2023, ransomware actors very likely resettled and recovered from those disruptions and elevated their tactics to make up for financial losses from 2022.[81]

Impact of CL0P—Compromises of digital supply chains

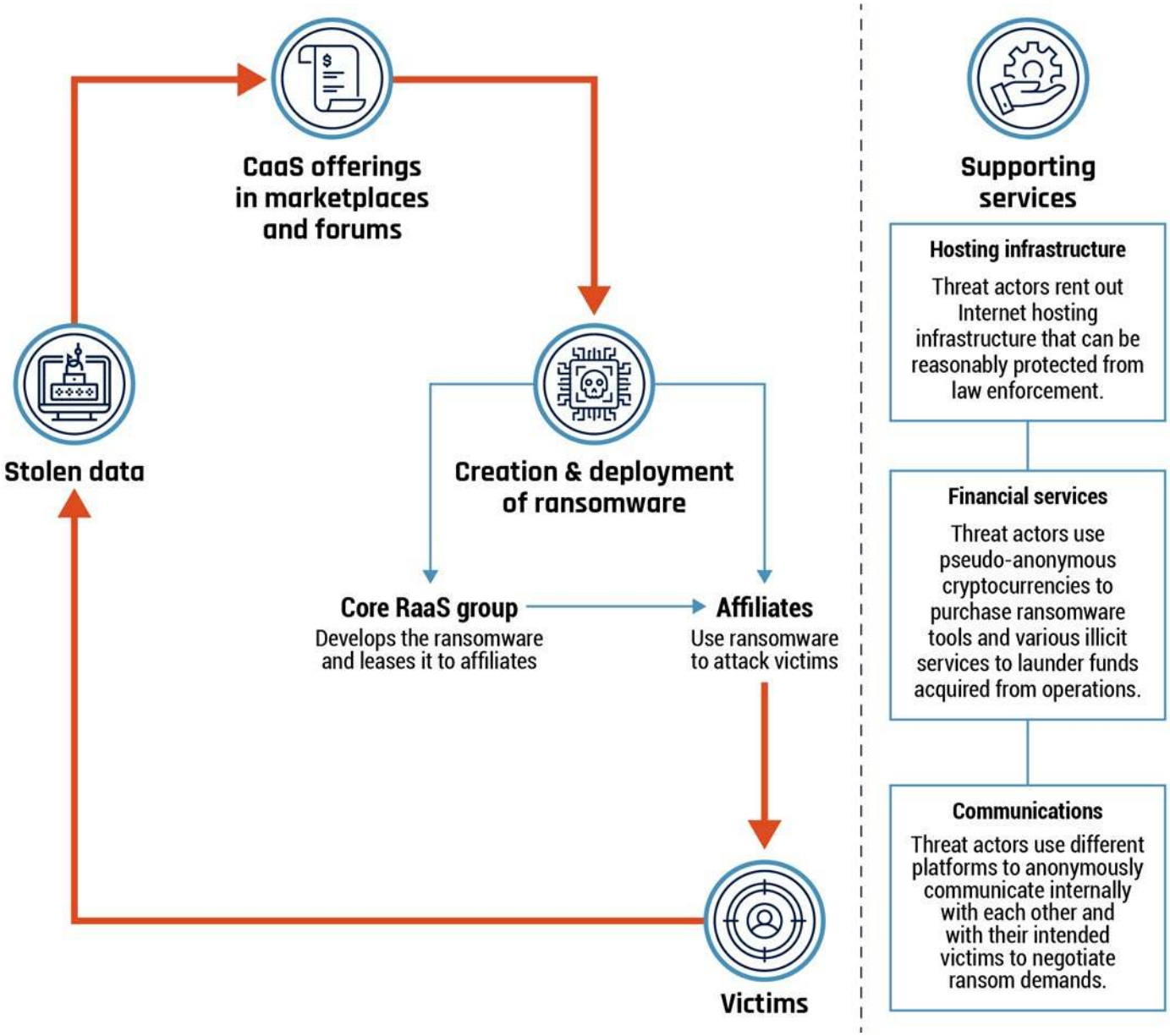
Many organizations rely on digital supply chains made up of various vendors for different applications and services. Cybercriminals can turn a breach against a single vendor into cascading incidents impacting multiple victim organizations.[82] As an example, the spike in global ransomware incidents in 2023 can very likely be partly attributed to CL0P, a ransomware strain operated by Russian-speaking cybercriminals.[83] CL0P was used to exploit unpatched vulnerabilities in the popular file transfer software applications GoAnywhere and MOVEit. In the MOVEit exploitation alone, CL0P impacted an estimated 2,750 enterprises and 94 million individuals[84] and amassed approximately $100 million USD in ransom payments.[85] Because of their profitability, ransomware attacks against digital supply chains will almost certainly continue in the next two years.

Top ransomware groups operate on Ransomware-as-a-Service Model

As highlighted in NCTA 2023-2024, most of the top ransomware groups impacting Canada operate on a Ransomware-as-a-Service (RaaS) business model where a core group of ransomware actors sell or lease their ransomware variant to affiliates who launch attacks. The RaaS ecosystem operates within the wider CaaS ecosystem. It is enabled by a complex supply chain of various actors offering different CaaS services that can be used to carry out ransomware attacks. This includes supporting services that underpin the functioning of the entire ecosystem (see Figure 10).[86]

We judge that the continued popularity of RaaS is almost certainly contributing to the rise in ransomware incidents by lowering the technical barriers to entry for more actors to carry out attacks without needing to develop their own malware.[87] It is difficult to assess the precise location of ransomware actors. However, we judge that the top ransomware groups impacting Canada have a core membership that is very likely based in countries that make up the former Soviet Union, although their affiliates operate globally.

Figure 10: RaaS ecosystem



Ransomware is impacting Canada's critical infrastructure

We assess that ransomware actors are almost certainly opportunistic and do not target specific industries. In the last few years, a wide range of Canadian businesses have been impacted by ransomware incidents, including large retailers and educational institutions. These incidents demonstrate that no entity is immune from the threat of ransomware. However, ransomware is almost certainly the top cybercrime threat facing Canada's critical infrastructure because it can immobilize critical business operations, destroy or damage important business data, and reveal sensitive information.[88] In addition to the financial losses associated with system repairs and operational disruptions, ransomware attacks can disrupt critical services that put victims' physical safety and emotional wellbeing in jeopardy.[89]

Critical infrastructure is an attractive target for ransomware actors because these entities are perceived as being more willing to pay large ransoms to prevent disruptions to critical operations. In 2021, ransomware incidents impacting Colonial Pipeline in the U.S. and the JBS Foods operations in North America and Australia resulted in multimillion-dollar payouts for ransomware actors.[90]

According to cyber security reporting, victims in 2023 were becoming less likely to pay ransom demands.[91] We judge that the perceived opportunities to earn high profits, combined with victims' reduced willingness to pay, has almost certainly encouraged more technically sophisticated ransomware groups to elevate their extortion techniques and hire skilled affiliates capable of targeting critical infrastructure entities to extract larger ransom payouts.[92] This is called "big game hunting," and we judge that it is the primary strategy used by many of the most prolific ransomware groups impacting Canada.[93]

Figure 11: Cyber incidents impacting Canada's critical infrastructure

Canada's critical infrastructure sectors have been impacted by various cyber incidents, including ransomware incidents and network breaches, that resulted in disruptions to critical business functions.

Energy sector

June 2023: Suncor Energy experienced a cyber incident that affected the company's Petro-Canada subsidiary. This temporarily impacted credit and debit processing at retail gas stations across Canada.[94]

Healthcare sector

December 2022: SickKids hospital in Toronto experienced a ransomware incident by an affiliate of the LockBit ransomware group. The impact of the incident was minimal and LockBit issued a public apology and offered to share the decryptor with the hospital.[95]

October 2023: 5 hospitals in Southern Ontario were impacted by a ransomware incident carried out by a ransomware group called Daixin. The incident impacted the hospitals' information technology (IT) provider, forcing the hospitals to temporarily shut down internal health systems. It resulted in the theft of sensitive files and caused delays in patient care.[96]

February 2024: LockBit reportedly claimed responsibility for a ransomware incident affecting Canadian pharmacy chain London Drugs, which forced the company to temporarily close some of its stores in Western Canada.[97]

Government sector

June 2023: The Government of Nova Scotia was impacted by CL0P's global exploitation of the MOVEit file transfer system. This resulted in a breach of personal information for an estimated 100,000 current and past provincial government employees.[98]

September 2023: Brookfield Global Relocation Services, which assists Canadian military and foreign service personnel with relocations, was subject to an unauthorized access breach that impacted information about Government of Canada personnel.[99]

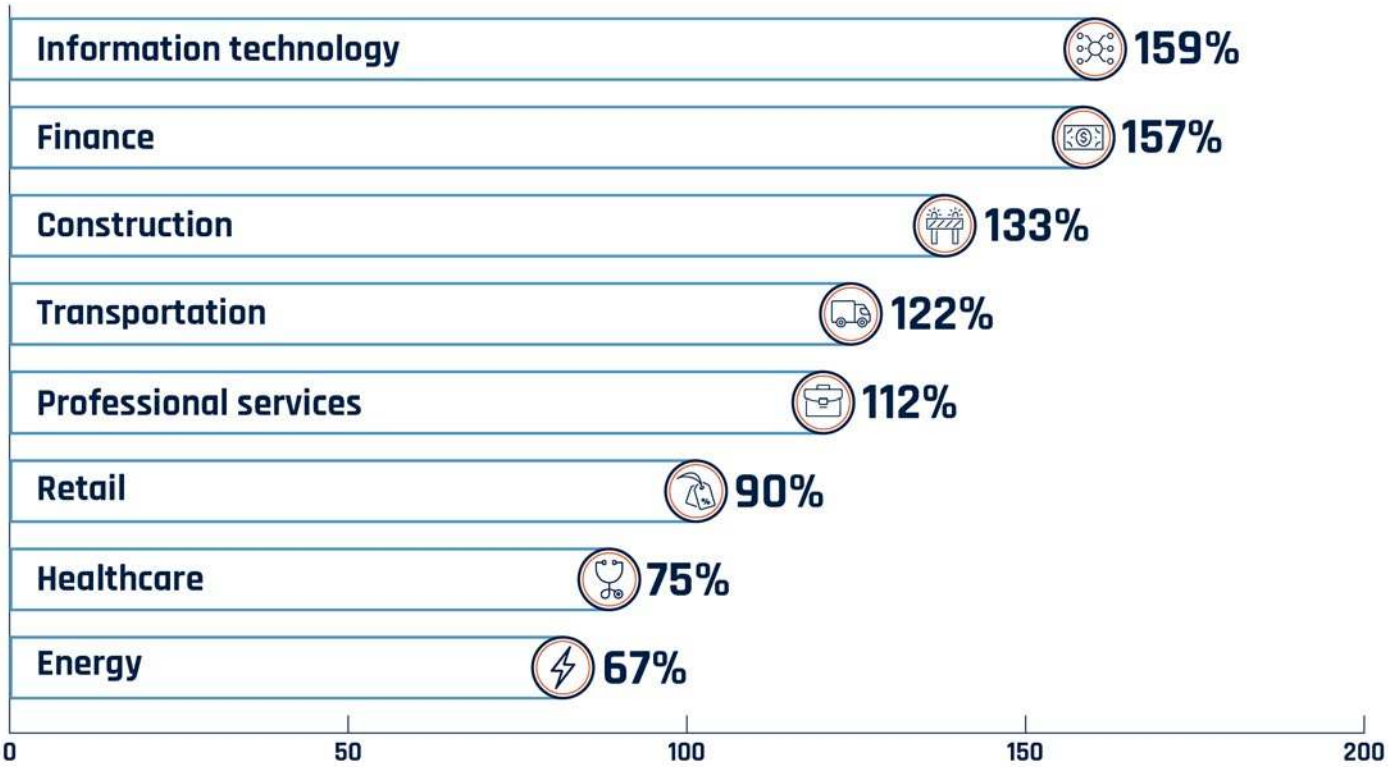
March 2024: The City of Hamilton was subject to a ransomware incident that impacted IT systems that manage various municipal functions, such as city phone lines, for weeks.[100]

Ransomware incidents hitting the healthcare sector are on the rise

Ransomware incidents impacting the healthcare sector have been steadily increasing worldwide.[101] Canada and our allies have collectively experienced high-profile ransomware attacks against the healthcare sector in recent years. In March 2024, Change Healthcare paid a multimillion-dollar ransom for the restoration of sensitive medical data after a ransomware attack disrupted billing processes for prescriptions in pharmacies across the U.S.[102] Soon after, in June 2024, a ransomware incident impacting pathology firm Synnovis caused major delays to several London, UK hospitals and resulted in the theft of sensitive data, which ransomware actors published online.[103]

By one estimate, ransomware incidents impacting the healthcare sector have nearly doubled since 2022.[104] This is concerning since these incidents directly disrupt the healthcare sectors' ability to deliver critical services to patients.[105] However, we judge that ransomware actors will almost certainly continue to choose victims based on opportunity rather than specific targeting in the next two years. Any observed increases in ransomware incidents impacting the healthcare sector will almost certainly reflect an increase in ransomware incidents overall, as well as the continued use of big game hunting by major ransomware groups.

Figure 12: Increase in Canadian ransomware incidents by sector observed by the Cyber Centre from 2022 to 2023



Ransomware actors are evolving their tactics to boost profits and evade detection

Ransomware actors are constantly evolving their strategies and adapting their techniques to maximize their profits and evade law enforcement detection.[106] We judge that these financial incentives combined with the flexibility of the RaaS model have almost certainly bolstered ransomware actors' resiliency in the face of law enforcement disruptions.

Ransomware ecosystem is splintering under law enforcement pressure

Recent major international law enforcement operations to tackle the ransomware ecosystem almost certainly degraded the targeted groups' capabilities and caused chaos in the cybercriminal underground.[107] However, we judge that these disruptions almost certainly will not have an enduring impact on the ransomware environment because, unless members of core RaaS groups are arrested, actors often find ways to adjust, rebrand, and resume their operations.[108]

By that same token, it is almost certain that the CaaS model has made the ransomware ecosystem more resilient to law enforcement action. The complex web of enabling services and cybercriminals interacting in borderless online spaces makes investigating cybercrime difficult.[109] If law enforcement disrupts a popular CaaS provider, the actor behind it will often rebrand and relaunch their service, or another service will quickly take their place. The flexibility of the CaaS model also makes it easy for cybercriminals to use multiple service providers simultaneously so they can pivot to new service providers if one is disrupted.[110]

International law enforcement disruptions against the ransomware ecosystem

The groups below were major players in the ransomware ecosystem. Prior to their disruptions, these groups were linked to over 1,000 compromises around the world and had amassed millions in ransom payments.[111]

- **January 2023:** Hive's networks were infiltrated, decryptor tools were provided to victims to recover their data, and Hive's infrastructure was seized by law enforcement.[112]
- **December 2023:** ALPHV (also known as BlackCat) had their infrastructure seized by law enforcement and a decryptor tool was provided to victims.[113]
- **February 2024:** LockBit's infrastructure was seized by law enforcement and cryptocurrency accounts linked to LockBit were frozen. Some core members were also arrested.[114]

In the next two years, we judge that the ransomware ecosystem will almost certainly become increasingly splintered.[115] Affiliates will almost certainly begin to act independently and create their own ransomware variants to reduce their susceptibility to law enforcement disruptions.[116] Further complicating this threat landscape, we judge that smaller ransomware groups will likely begin collaborating to increase their capabilities, or they will try to attract affiliates from ransomware groups that are subject to disruption operations to take the place of their former competitors and grab a greater share of the ransomware market.[117]

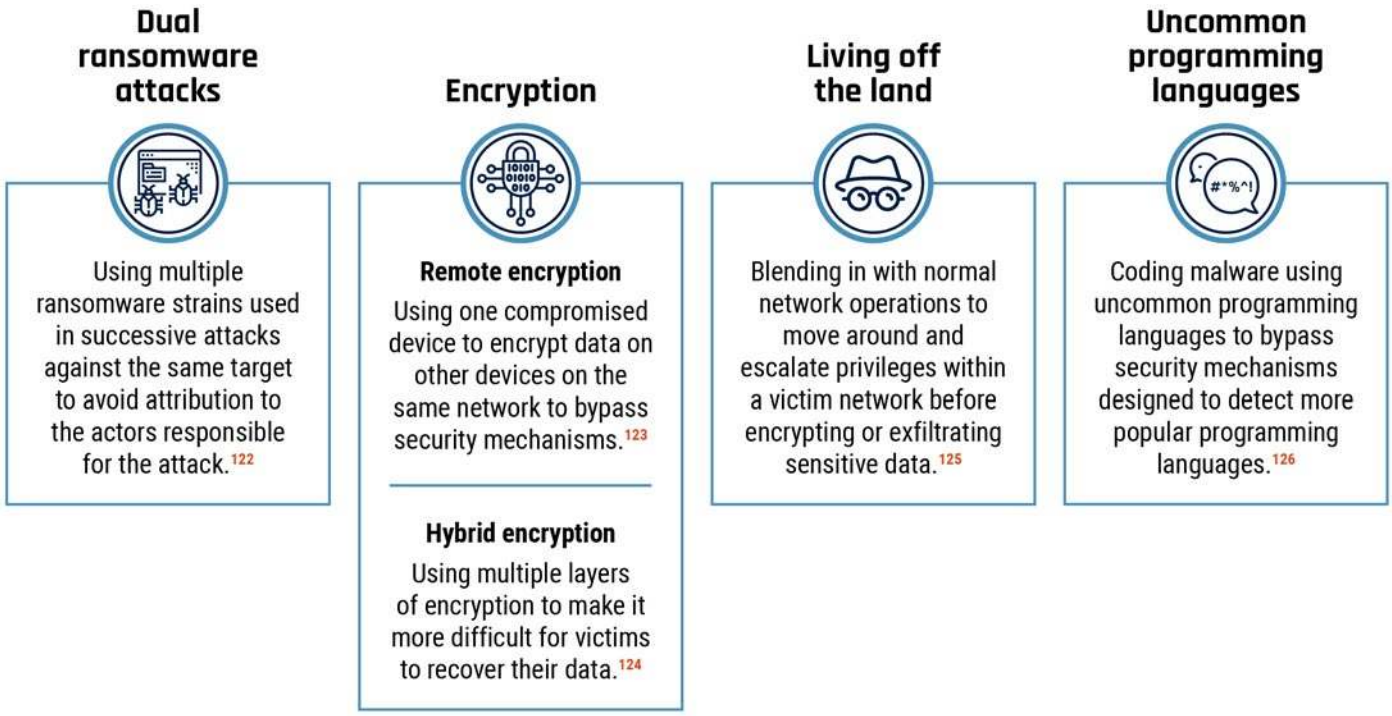
Intensifying extortion methods

Ransomware actors are increasing pressure on victims to pay ransoms by ramping up their extortion methods. Some ransomware groups have started posting count downs on their websites indicating when they plan to leak stolen data, or even directly calling victims or their clients and threatening to release their personal information if they do not pay the demanded ransom.[118] Additionally, ransomware actors have publicly criticized the organizations that have fallen victim to their ransomware to damage their reputation, and have encouraged clients of the victim organizations to file lawsuits against the victims.[119] Ransomware actors have also started to use new legislation that require victims to report ransomware incidents to apply pressure to their victims. For example, ALPHV-affiliated actors claimed that they filed a complaint with the U.S. Securities and Exchange Commission against a victim for failing to report the ransomware incident that ALPHV itself conducted against them.[120] We judge that ransomware actors' extortion methods will continue to evolve in the next two years in an effort to maximize their likelihood of receiving payment from victims.

Ransomware actors are using new tactics to obfuscate their activities

As ransomware actors have come under intense scrutiny from law enforcement, many have started layering obfuscation techniques to camouflage and hide themselves from detection and minimize their digital footprints.[121]

Figure 13: Obfuscation techniques used by ransomware actors



Collaboration is necessary to tackle the evolving ransomware threat

We judge that ransomware actors will continue to diversify their tactics in response to heightened law enforcement attention. Understanding this threat and the CaaS business model and recognizing the dynamic nature of this ecosystem will be critical to tackling it in the future. Collaboration between industry, law enforcement, and all levels of government, as well as bolstering Canadians' awareness about cybercrime, are imperative to building resilience against this evolving threat.[127]

3

TRENDS SHAPING CANADA'S **CYBER THREAT LANDSCAPE**

Background

CSE uses its expertise to help monitor, detect, and investigate threats against Canada's information systems and networks. Based on our observations since NCTA 2023-2024, we have identified five trends that will shape Canada's cyber threat environment until 2026:

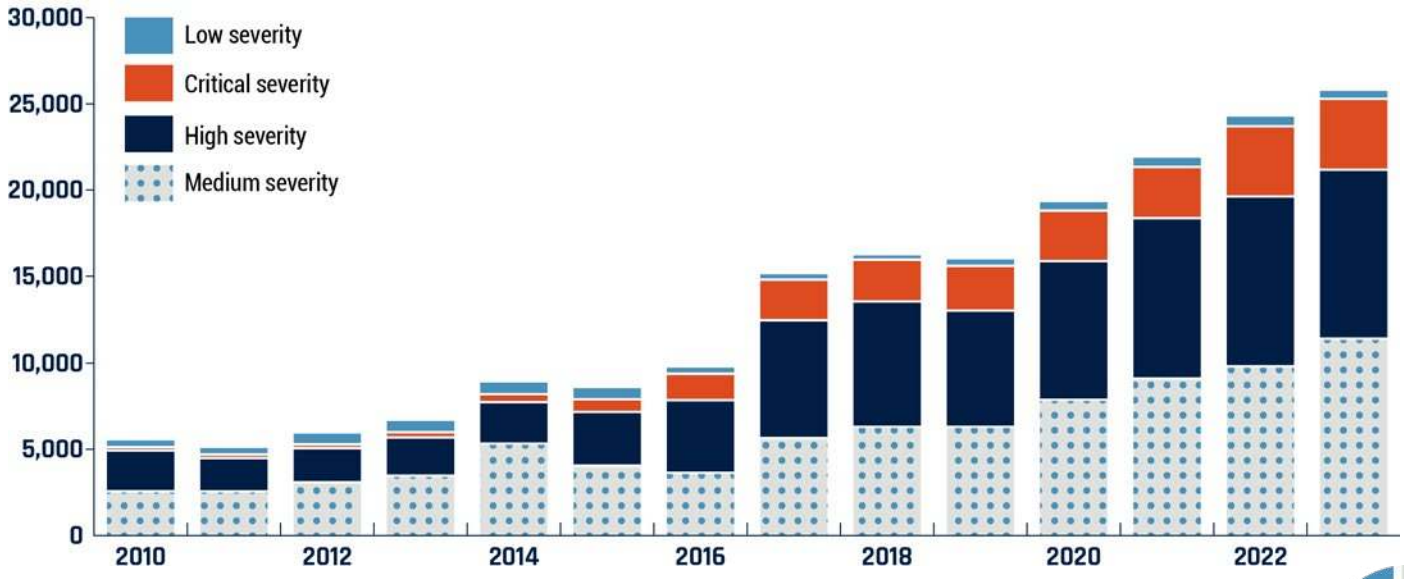
- **Trend 1:** Artificial intelligence (AI) technologies are amplifying cyber space threats
- **Trend 2:** Cyber threat actor tradecraft is evolving to evade detection
- **Trend 3:** Geopolitically inspired non-state actors are creating unpredictability
- **Trend 4:** Vendor concentration is increasing cyber vulnerability
- **Trend 5:** Dual-use commercial services are in the digital crossfire

Trends discussed in past NCTAs are still relevant

Before discussing the five trends above in more detail, it is important to note that trends impacting Canada's cyber threat landscape that we raised in previous NCTAs remain relevant today. These trends continue to evolve over time in light of geopolitical, technological, and threat actor developments. For example:

- **The cyber threat surface keeps expanding:** In addition to the continued adoption and deployment of the Internet of Things (e.g., connected vehicles), the boom in cloud-based AI platforms and services is forecasted to drive demand for supporting infrastructure, such as AI-capable data centres and energy generation, and lead to the transfer of even more data to cloud environments. It is also very likely that AI-focused organizations (including AI labs that conduct AI research and develop AI models) are now more prominent targets for cyber threat actors.[128]
- **Supply chain attacks continue:** Cyber threat actors continue to launch digital supply chain attacks where a threat actor compromises or exploits a software, information technology (IT), or cloud services vendor to enable it to exploit the customers that use the service. This includes double supply chain attacks where one supply chain attack enables another.[129]
- **Publicly known vulnerabilities are still being exploited:** Cyber threat actors are constantly scanning for publicly known security vulnerabilities in software and exploiting unpatched vulnerabilities to gain unauthorized access to private and public networks. The number of common vulnerabilities and exposures (CVE) continues to grow (Figure 14). The time it takes threat actors to exploit these vulnerabilities continues to decrease, with attacks starting within days after their disclosure.[130]

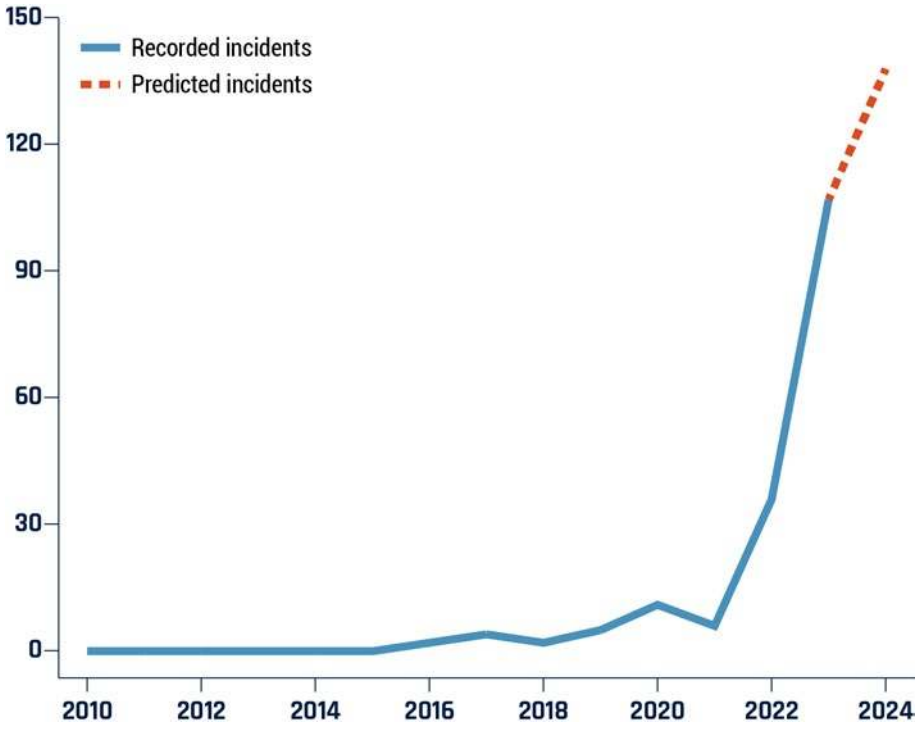
Figure 14: Common vulnerabilities and exposures (CVE) count by severity[131]



Trend 1: Artificial intelligence technologies are amplifying cyberspace threats

AI technologies are almost certainly lowering the barriers to entry and enhancing the quality, scale, and precision of malicious cyber threat activity.[132] Cybercriminals and state-sponsored cyber threat actors are using generative and predictive AI tools (including large language models (LLMs)) to support their work processes, from content generation to big data analysis. We assess that technically skilled cyber threat actors will almost certainly attempt to misuse AI tools in novel ways over the next two years as the technology develops. This includes automating parts of the cyber attack chain to improve productivity.[133]

Figure 15: Publicly reported worldwide generative AI incidents resulting in harm or near harm[134]



AI is improving the personalization and persuasiveness of social engineering attacks

Cybercriminals and state-sponsored cyber threat actors are almost certainly using LLMs to improve social engineering attacks that manipulate targets into doing something that is detrimental to their interests, such as disclosing sensitive information, authorizing fraudulent transactions, or downloading malware.[135] Generative AI tools enable cyber threat actors to create realistic audio and visual content impersonating trusted individuals (i.e., deepfakes). These help to establish legitimacy with and persuade targets.[136] Cyber threat actors are also using AI to craft personalized phishing emails at scale with convincing and grammatically correct language that mimics human writing styles, making it harder for recipients to identify and filter phishing attempts.[137]

AI technologies are enhancing the quality and scale of foreign online influence campaigns

In NCTA 2023-2024, we discussed how state cyber threat actors can create and spread AI-generated disinformation. Since then, a growing number of countries, including the PRC, Russia, Iran, and Israel, have reportedly incorporated fake or deceptive AI-generated articles, images, and videos (deepfakes) in their online influence operations (misinformation, disinformation, and malinformation) to enhance the quality and scale of their campaigns.[138] They are also very likely using AI tools to generate fictitious social media bot accounts and online personas in an effort to amplify engagement.[139] These campaigns are designed to weaken opponents by polluting the online information space, undermining trust in institutions, and sowing doubt and division in the target society.[140]

We assess that AI-enhanced disinformation is more likely to gain traction when it has one or more of these characteristics:[141]

- amplifies polarizing narratives that already exist in the target society
- fills a void in the information space
- is spread by a trusted or official source(s)
- targets time-sensitive situations when there is limited time to debunk fake content

The rise of AI-generated websites

Foreign states are creating fake news websites masquerading as real news outlets as part of their disinformation campaigns. Many of the sites are designed to look like local news outlets that have closed down and rely on AI-generated content.[142]

Predictive AI is improving big data analysis capabilities

Well-resourced states are very likely leveraging AI tools to help process and analyze large volumes of data they collect. We assess that foreign intelligence services are very likely using AI-enabled data analytics to find patterns and trends in bulk data, gain insights on individuals and assets of interest, and inform follow-on cyber operations.[143]

Trend 2: Cyber threat actor tradecraft is evolving to evade detection

As network defences have improved at detecting and responding to security threats, cyber threat actors are evolving their tradecraft in an attempt to minimize detection and stay hidden operating on victim systems longer.

Cyber threat actors are targeting and exploiting edge devices to access networks

Cyber threat actors are exploiting vulnerabilities in security and networking devices that sit at the perimeter of networks—known as "edge" devices (e.g., routers, firewalls, and virtual private network [VPN] solutions). By compromising an edge device, a cyber threat actor can enter a network, monitor, modify, and exfiltrate network traffic flowing through the device, or possibly move deeper into the victim's network.

Cyber threat actors very likely target edge devices because network defenses may have limited capability to monitor and detect malware activity on them, especially compared to other access vectors, such as phishing emails.[144] For example, in early 2024, Canada and our allies detected that a well-resourced and sophisticated state-sponsored cyber threat actor had collected and exfiltrated data by exploiting 2 newly discovered vulnerabilities in VPN devices used by government and critical national infrastructure networks.[145]

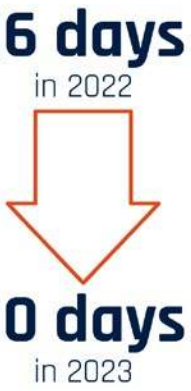
Cyber threat actors are "living off the land" in compromised environments to stay undetected

Cyber threat actors using living-off-the-land (LOTL) techniques repurpose native system tools and processes that are already present in the target's environment to move throughout the network discreetly.[146] They do not deploy malware or custom tools on the compromised network. This makes it challenging for network defences to detect and discover intrusions.[147] PRC, Russian, and Iranian state-sponsored cyber threat actors use LOTL techniques.[148] For example, a Russian cyber threat actor reportedly compromised a Ukrainian electric utility's network in October 2022 and used LOTL techniques to move through the utility's operational technology environment before triggering a power outage.[149]

Attacker dwell time is dropping

The global median dwell time—number of days an attacker is present in a compromised system before detection—continued to drop from 2022 to 2023.

Mandiant[150]



Cyber threat actors are abusing domestic infrastructure to hide their malicious activity

State-sponsored cyber threat actors and cybercriminals are almost certainly conducting malicious activity against Canada using virtual resources and networking infrastructure (e.g., routers) located in North America to limit scrutiny and visibility into their operations.[151] For example, Russian and PRC state-sponsored cyber threat actors have been observed routing their malicious cyber operations through compromised small office and home office (SOHO) network equipment located in Canada and the U.S., such as routers belonging to unsuspecting households and businesses, to blend into normal network activity.[152]

Trend 3: Geopolitically inspired non-state actors are creating unpredictability

Geopolitical conflicts and tensions are inspiring disruptive cyber threat activity from non-state groups, commonly referred to as hacktivists. Geopolitically motivated hacktivists typically conduct attacks to gain attention, such as DDoS attacks, website defacements, and data leaks. Some groups have elevated the impact of their activity by opportunistically targeting and disrupting vulnerable critical infrastructure, such as municipal water systems, risking serious harm to the public.[153]

Geopolitically motivated hacktivism is surging around military conflicts. Hacktivist groups have carried out campaigns related to Russia's invasion of Ukraine in 2022 and the Israel-Hamas war in 2023.[154] Diplomatic tensions are also inspiring hacktivist activity. After Canada accused India of involvement in the killing of a Canadian citizen, a pro-India hacktivist group claimed to have defaced and conducted brief DDoS attacks against websites in Canada, including the public-facing website of the Canadian Armed Forces.[155]

This non-state ecosystem is dynamic and unpredictable. Some hacktivists are genuinely motivated by a mix of patriotism, ideology, or a political cause, but others opportunistically take advantage of conflicts for personal benefit or notoriety. New groups regularly appear and established groups dissolve and re-emerge with new names. Actors shift their focus and motivations. Different groups coordinate and collaborate, including across multiple conflicts.[156] Although hacktivist activities can sometimes align with an adversarial state's interests, the relationship, if any, between a hacktivist and the state can be difficult to discern.

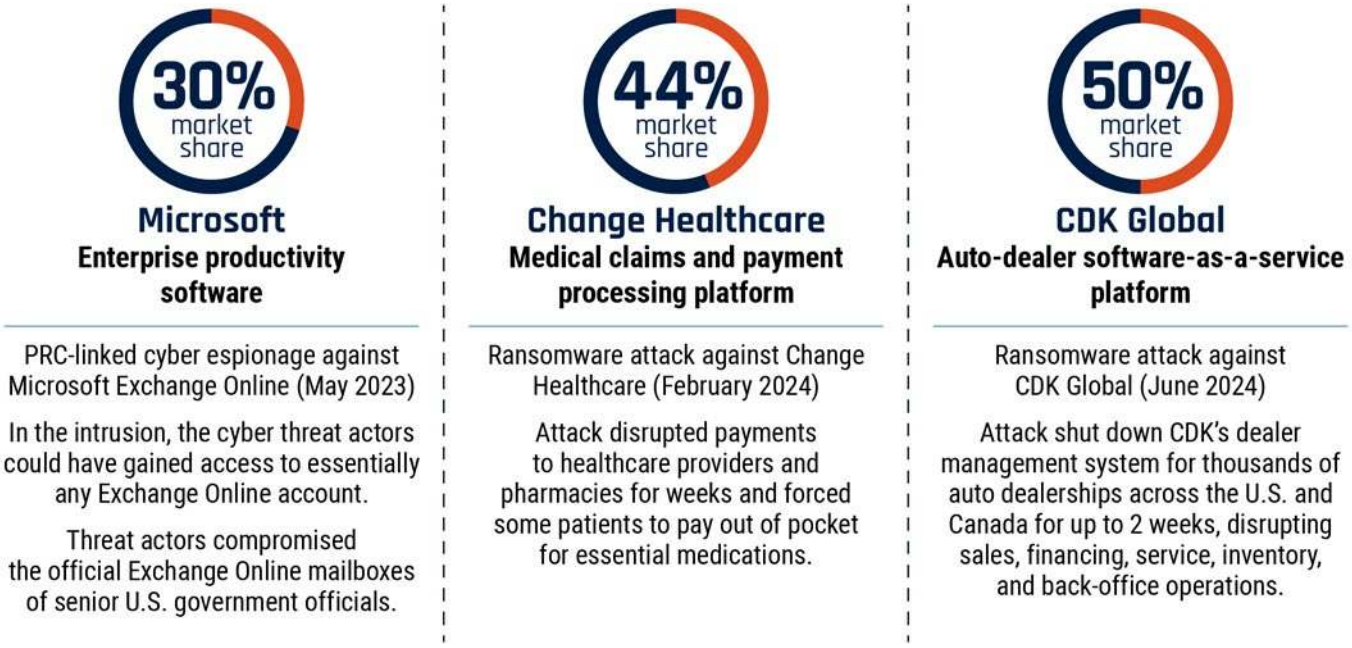
Trend 4: Vendor concentration is increasing cyber vulnerability

The provision of many technology services is concentrated, with only a few large providers of a given digital service, each with a large base of users.[157] Organizations in both the public and private sectors, including banks, airlines, and healthcare providers, rely on these dominant service providers, such as a cloud provider or a specialized Software-as-a-Service platform, to support critical functions and operations.[158] A cyber incident impacting a single dominant service provider can impact an entire sector.

Dominant service providers are magnets for malicious cyber threat activity. Cyber threat actors target dominant vendors seeking to steal customer data or demand ransom payments.[159] For example, state-sponsored cyber threat actors are persistently targeting and developing capabilities to compromise the three major commercial cloud service providers that together make up an estimated 65% of the global cloud market: Amazon, Microsoft, and Google.[160] This includes researching the internal networks of the cloud platforms and improving techniques to covertly bypass security mechanisms and exfiltrate data.

When dominant service providers are compromised, the impact of cyber security incidents are amplified. Cyber threat activity against services that are digital chokepoints—single points of failure within supply chains—can have cascading and system-wide disruptive impacts on the economy and society, including endangering our national security (Figure 16).[161]

Figure 16: Recent cyber attacks against dominant vendors and their market share[162]



Despite the fact that dominant service providers know that they are major targets, the scale and complexity of their operations may limit their ability to discover and fix cyber vulnerabilities.[163] For instance, in May 2023, a threat actor assessed to be affiliated with the PRC compromised Microsoft's cloud-based Exchange email service in a breach that the U.S. Cyber Safety Review Board investigating the incident found was preventable.[164] Less than a year later in November 2023, a Russian state-sponsored cyber threat actor compromised Microsoft's Exchange service and exfiltrated data from Microsoft's own corporate email accounts, including customer data. Then, in July 2024, Microsoft's Azure cloud service failed to withstand a DDoS attack, disrupting global access to some Microsoft services for hours.[165] According to Microsoft, an error in its own defence mechanisms contributed to the outage.[166]

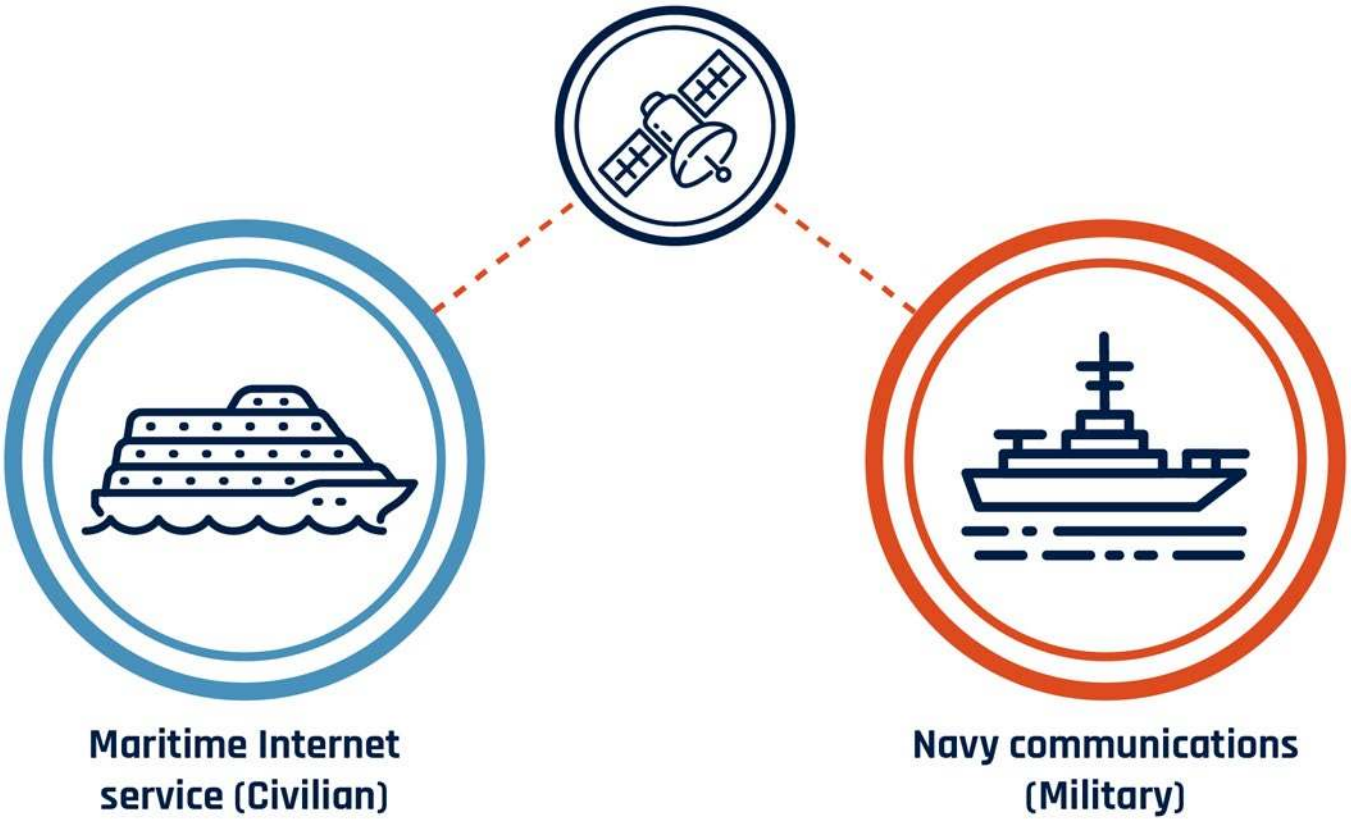
Trend 5: Dual-use commercial services are in the digital crossfire

Governments around the world are turning to services available in the commercial market to gain a competitive edge over their adversaries and ensure resilience during a conflict. Commercial solutions, such as commercial satellite communications systems and advanced computing capabilities, offer militaries and intelligence agencies access to innovative technologies at scale that can be deployed quickly.[167]

We assess that commercial services that provide service to both civilian and military customers (i.e., dual-use services) are almost certainly targets of state-sponsored cyber threat activity.[168] Our adversaries have signaled an intent and demonstrated the capability to use cyber attacks to disrupt, degrade, or deny opponents access to commercial services during an armed conflict.[169] These attacks can have cascading disruptive effects on civilian and critical infrastructure customers that depend on the same services.

For instance, state-sponsored cyber threat actors are very likely targeting dual-use commercial satellite systems that support military or government communications, remote sensing, and navigation capabilities. Since the start of Russia's invasion of Ukraine in February 2022, Russian state-sponsored cyber threat actors have conducted cyber and electronic warfare operations (like jamming and spoofing) against commercial satellite communications services used by the Ukrainian military.[170] At least one of these attacks disrupted satellite Internet service to civilian customers outside of the conflict zone.

Figure 17: Example of a dual-use satellite communications service



Conclusion

Cyber threat actors present a persistent threat to Canada's economic prosperity and national security. As a wealthy country, Canada will remain a valuable target for financially motivated cybercriminals that are supported by a highly adaptable and resilient cybercrime ecosystem. Meanwhile, the threat to Canada from state-sponsored cyber threat activity will be influenced by geopolitical events beyond our borders, the status of Canada's foreign relations, and an international environment defined by economic and technological rivalry.[171] The threats in cyberspace will increasingly reflect a global system where an array of actors are forging networks of varying strength and convenience in pursuit of their own self-interests.[172]

Despite our cyber vulnerabilities and the evolving cyber-threat environment, the intensity and impact of cyber threats to Canada can be mitigated through awareness and best practices in cyber security by both individuals and organizations.

CSE leverages all aspects of its mandate, and its partnerships, to defend federal networks and systems of importance to the Government of Canada. CSE will continue to share important information on the cyber threat landscape with Canadians, the private sector, and critical infrastructure. Canadians can be assured that the Cyber Centre is dedicated to tracking cyber threats to Canada, advancing our cyber security, and protecting the systems that we rely on daily, offering support to critical infrastructure networks as well as to other systems of importance to Canada. We will continue to work with the private sector to drive security and resilience and forge international partnerships to achieve shared cyber security goals.

We encourage readers to consult our cyber security guidance[173] for more information on the cyber threats outlined in this assessment and how to protect against them. Organizations may also consult our Cross-Sector Cyber Security Readiness Goals Toolkit[174] to learn how to increase their cyber security posture.

Endnotes

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

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

3 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

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

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

6 Statistics Canada, *Canadian Internet Use Survey, 2022*, 20 July 2023. https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm; Chris Dixon, *Read Write Own: Building the Next Era of the Internet*, (New York: Random House, 2024).

7 Federal Trade Commission, *FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens,* 19 September 2024. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance; Reva Goujon, "Shut Out: Data Security and Cybersecurity Converge in Next Wave of US Tech Controls," *Rhodium Group*, 5 March 2024. https://rhg.com/research/shut-out-data-security-and-cybersecurity-converge-in-next-wave-of-us-tech-controls/.

8 Brian Klaas, "The CrowdStrike Failure Was a Warning," *The Atlantic*, 21 July 2024. https://www.theatlantic.com/ideas/archive/2024/07/crowdstrike-failure-warning-solutions/679174/.

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

10 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

11 https://www.cyber.gc.ca/en/guidance/threat-large-language-model-text-generators

12 Jonathan Rauch, "The World is Realigning," *The Atlantic*, 1 July 2024. https://www.theatlantic.com/ideas/archive/2024/07/russia-china-nato-axis-resistance/678831/; Chun Han Wong, "China's Xi Jinping Takes Rare Direct Aim at U.S. in Speech," The *Wall Street Journal*, 6 March 2023. https://www.wsj.com/articles/chinas-xi-jinping-takes-rare-direct-aim-at-u-s-in-speech-5d8fde1a.

13 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, (Oxford: Oxford University Press, 2022); Rajat Pandit, "Armed forces formulate new doctrine for cyberspace operations," *The Times of India*, 18 June 2024. https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms.

14 Google Threat Analysis Group, "Buying Spying: Insights into Commercial Surveillance Vendors," *Google*, February 2024. https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/; Jen Roberts et. al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights," *DFRLab*, 4 September 2024. https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/.

15 Redacted Indictment, *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), filed 25 March 2024. https://www.justice.gov/usao-edny/media/1345131/dl; United States Department of the Treasury, *Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies*, 23 April 2024. https://home.treasury.gov/news/press-releases/jy2292; Christian Sepherd et al., "Leaked files from Chinese firm show vast international hacking effort," *The Washington Post*, 22 February 2024. https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/; United States Department of Justice, *Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guards Corps*, 23 March 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary; Google Threat Analysis Group, "Buying Spying: Insights into Commercial Surveillance Vendors," *Google*, February 2024. https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/; Wahlstrom et al., "Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan," *Mandiant*, 30 March 2023. https://cloud.google.com/blog/topics/threat-intelligence/cyber-operations-russian-vulkan; United States Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, 3 November 2021. https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list; Max Smeets, "Hack Global, Buy Local: The Inefficiencies of the Zero-Day Exploit Market," *Lawfare*, 6 June 2022. https://www.lawfaremedia.org/article/hack-global-buy-local-inefficiencies-zero-day-exploit-market.

16 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity*, 3 June, 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity.

17 Redacted Indictment, *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), filed 25 March 2024. https://www.justice.gov/usao-edny/media/1345131/dl.

18 Robert Fife and Steve Chase, "Canadian spy agency says it shared details of Chinese hacking with Parliamentary officials" *The Globe and Mail*, 30 April, 2024. https://www.theglobeandmail.com/politics/article-canadian-spy-agency-says-it-shared-details-of-chinese-hacking-with.

19 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity*, 3 June, 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity

20 United States Department of State, *Global Engagement Center Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment,* 28 September 2023. https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/; Redacted Complaint and Affidavit in Support of Application for Arrest Warrants, *United States v. Bai*, 1:23-mj-00334, (E.D.N.Y), filed 6 April 2023. https://www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf. United States House Select Committee on the CCP, HEARING: CCP Transnational Repression: The Party's Effort to Silence and Coerce Critics Overseas, 13 December 2023. https://selectcommitteeontheccp.house.gov/media/witness-testimony/hearing-ccp-transnational-repression-partys-effort-silence-and-coerce.

21 Mike Dvilyanski, "Taking Action Against Hackers in China," *Meta*, 24 March 2021. https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/; Redacted Indictment, *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), filed 25 March 2024. https://www.justice.gov/usao-edny/media/1345131/dl; Kristina Balaam et al., "BadBazaar: iOS and Android Surveillanceware by China's APT15 Used to Target Tibetans and Uyghurs," *Lookout*, 22 January 2024. https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15.

22 Congressional-Executive Commission on China, *The Human Rights Situation in Tibet and the International Response, One Hundred Sixteenth Congress*, Second Session, 30 September 2020. https://www.congress.gov/event/116th-congress/joint-event/LC68497/text; The Honourable Mari-Josée Hogue, Commissioner, "Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions - initial report", *Privy Council Office*, 3 May 2024. https://publications.gc.ca/site/eng/9.935030/publication.html; Amnesty International, *China: Overseas students face harassment and surveillance in campaign of transnational repression*, 13 May 2024. https://www.amnesty.org/en/latest/news/2024/05/china-overseas-students-face-harassment-and-surveillance-in-campaign-of-transnational-repression/.

23 Dakota Cary and Aleksandar Milenkoski, "Unmasking I-Soon | The Leak That Revealed China's Cyber Operations," *SentinalLabs*, 21 February, 2024. https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/; Christian Sepherd et al., "Leaked files from Chinese firm show vast international hacking effort," *The Washington Post*, 22 February 2024. https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon.

24 Redacted Indictment, *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), filed 25 March 2024. https://www.justice.gov/usao-edny/media/1345131/dl.

25 Center for Security and Emerging Technology, *Translation: Implementation Opinions of Seven Ministries Including the Ministry of Industry and Information Technology on Promoting the Innovative Development of Future Industries*, 12 February 2024. https://cset.georgetown.edu/publication/future-industry-implementation-opinions/.

26 Cybersecurity and Infrastructure Security Agency, *Opening Statement by CISA Director Jen Easterly*, 31 January 2024. https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly; Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity*, 3 June, 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity.

27 Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Alert AA24-038A, 7 February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; The Economist, "The new front in China's cyber campaign against America," *The Economist*, 13 June 2024. https://www.economist.com/international/2024/06/13/the-new-front-in-chinas-cyber-campaign-against-america.

28 Canadian Centre for Cyber Security, C*yber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity*, 3 June, 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity.

29 United States Department of Justice, *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*, 13 July 2018. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election; Microsoft Threat Intelligence Report, *Iran steps into US election 2024 with cyber-enabled influence operations*, 9 August 2024. https://blogs.microsoft.com/on-the-issues/2024/08/iran-targeting-2024-us-election/; United States Department of Justice, *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*, 4 September 2024. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; Canadian Centre for Cyber Security, *Russian military cyber actors target U.S. and global critical infrastructure*, 5 September 2024. https://www.cyber.gc.ca/en/news-events/russian-military-cyber-actors-target-us-global-critical-infrastructure.

30 Canadian Centre for Cyber Security, *CSE urges the Canadian cyber security community to be vigilant on two-year mark of Russia's full-scale invasion of Ukraine*, 19 February 2024. https://www.cyber.gc.ca/en/news-events/cse-urges-canadian-cyber-security-community-be-vigilant-two-year-mark-russias-full-scale-invasion-ukraine

31 Tom Balmforth, "Exclusive: Russia hackers were inside Ukraine telecom giant for months," *Reuters*, 5 January 2024. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

32 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*, 14 July 2022. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine.

33 Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023-2024*, 28 October 2022. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

34 Cybersecurity and Infrastructure Security Agency, *Cybersecurity Advisory: SVR Cyber Actors Adapt Tactics for Initial Cloud Access*, 26 February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a.

35 Cybersecurity and Infrastructure Security Agency, *Emergency Directives ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*, 2 April 2024. https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system; Alexander Martin, "Exclusive: Russian spies hacked UK government data and emails earlier this year," *The Record*, 8 August, 2024. https://therecord.media/russia-hack-uk-government-home-office-microsoft.

36 Microsoft, *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*, 19 January 2024. https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard.

37 Anne Keast-Butler, Director GCHQ, *CYBERUK 2024: Anne Keast-Butler keynote speech*, 14 May 2024. https://www.ncsc.gov.uk/speech/cyberuk-2024-gchq-director-keynote-speech.

38 Catharine Tunney, "Trudeau shrugs off reports pro-Russia hackers brought down PMO website," *CBC News*, 11 April 2023. https://www.cbc.ca/news/politics/cse-cyber-attack-ukrainian-visit-1.6806709

39 Canadian Centre for Cyber Security, *Alert – Risk of malicious cyber activity against Ukraine-aligned nations*, 24 February 2023. https://www.cyber.gc.ca/en/alerts-advisories/risk-malicious-cyber-activity-against-ukraine-aligned-nations; Ellen Nakashima, "Tex. Hack may be first disruption of U.S. water system by Russia," *The Washington Post*, 17 April 2024. https://www.washingtonpost.com/politics/2024/04/17/tex-hack-may-be-first-disruption-us-water-system-by-russia/; Cybersecurity and Infrastructure Security Agency, *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity*, 1 May 2024. https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity.

40 United States Department of Treasury, *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn*, 19 July 2024. https://home.treasury.gov/news/press-releases/jy2473.

41 The Canadian Press Staff, "Quebec government says data not compromised after websites hit by cyberattack," *CTV News*, 13 September 2023. https://montreal.ctvnews.ca/quebec-government-sites-under-cyber-attack-1.6560005?cache=hhhufcdil; Michelle Allan, "Websites for PMO's office, NCC among those crashed by hackers," *CBC News*, 15 April 2023. https://www.cbc.ca/news/canada/ottawa/websites-for-pmo-s-office-ncc-among-those-crashed-by-hackers-1.6810684.

42 Gil Baram, "How the cyberwar between Iran and Israel has intensified," *The Washington Post*, 25 July 2022. https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war; Sharon Wrobel, "Cyberattacks by Iran, Hezbollah have tripled during the war, says Israel cyber czar," *The Times of Israel*, 4 July 2024. https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-czar/.

43 United States Department of the Treasury, *Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities*, 9 September 2022. https://home.treasury.gov/news/press-releases/jy0941; United States Department of the Treasury, *Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure*, 2 February 2024. https://home.treasury.gov/news/press-releases/jy2072.

44 Cybersecurity and Infrastructure Security Agency. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*, 28 November 2023. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems; Jim Walter, "Iran-Backed Cyber Av3ngers Escalates Campaigns Against U.S. Critical Infrastructure," *Sentinel One*, 30 November 2023. https://www.sentinelone.com/blog/iran-backed-cyber-av3ngers-escalates-campaigns-against-u-s-critical-infrastructure/.

45 Figure 5 is derived from data in Microsoft Threat Intelligence, *Iran surges cyber-enabled influence operations in support of Hamas*, 26 February 2024. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas; Cybersecurity and Infrastructure Security Agency, *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*, 28 November 2023. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems; Jim Walter, "Iran-Backed Cyber Av3ngers Escalates Campaigns Against U.S. Critical Infrastructure," *Sentinel One*, 30 November 2023. https://www.sentinelone.com/blog/iran-backed-cyber-av3ngers-escalates-campaigns-against-u-s-critical-infrastructure/; Cybersecurity and Infrastructure Security Agency. *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, 23 September 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a; The Federal Bureau of Investigations and the Cybersecurity and Infrastructure Security Agency, *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, 21 September 2022. https://www.cisa.gov/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf; Global Affairs Canada, *Statement on Iran's malicious cyber activity affecting Albania*, 22 September 2022. https://www.canada.ca/en/global-affairs/news/2022/09/statement-on-irans-malicious-cyber-activity-affecting-albania.html; Clearsky Cyber Security, *No Justice Wiper. Wiper attack on Albania by Iranian APT*, 4 January 2024. https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf; Daryna Antoniuk, "Wiper malware found in analysis of Iran-linked attacks on Albanian institutions," *The Record*, 8 January 2024. https://therecord.media/albania-parliament-telecoms-airline-cyberattacks-wiper-malware; Associated Press Staff, "Albanian authorities accuse Iranian-backed hackers of cyberattack on Institute of Statistics," *Associated Press News*, 14 February 2024. https://apnews.com/article/albania-iran-hackers-cyberattack-statistics-e80780e2d927394589c3d8903e36d066; Microsoft Threat Intelligence, *Iran turning to cyber-enabled influence operations for greater effect*, 5 February 2023. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-turning-to-cyber-enabled-influence-operations-for-greater-effect; Associated Press Staff, "Hackers target Bahrain airport, news sites to mark uprising," *CTV News*, 14 February 2023. https://www.ctvnews.ca/hackers-target-bahrain-airport-news-sites-to-mark-uprising-1.6273145.

46 Google Threat Analysis Group, *Iranian backed group steps up phishing campaigns against Israel*, U.S., 14 August 2024. https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/; Rozmann et al., "Uncharmed: Untangling Iran's APT42 Operations," *Mandiant*, 1 May 2024. https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations; INSIKT Group, "Social Engineering Remains Key Tradecraft for Iranian APTs," *Recorded Future*, 30 March 2022. https://www.recordedfuture.com/research/social-engineering-remains-key-tradecraft-for-iranian-apts.

47 Borzou Daraghi, "Iran is using its cyber capabilities to kidnap its foes in the real world," *The Atlantic Council*, 24 May 2023. https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/; United States Department of Justice, *One Iranian and Two Canadian Nationals Indicted in Murder-for-Hire Scheme*, 29 January 2024. https://justice.gov/opa/pr/one-iranian-and-two-canadian-nationals-indicted-murder-hire-scheme; United States Department of Justice, *Members of Iran's Islamic Revolutionary Guards Corps (IRGC) Charged with Plot to Murder the Former National Security Advisor*, 10 August 2022; Arash Azizi, "Iran's Deadly Message to Journalists Abroad," *The Atlantic*, 12 April 2024. https://www.theatlantic.com/international/archive/2024/04/iran-journalism-west-violence/678038; Greg Miller, Souad Mekhennet, and Cate Brown, "Iran turns to Hells Angels and other criminal gangs to target critics," *The Washington Post*, 12 September 2024. https://www.washingtonpost.com/world/2024/09/12/iran-criminal-gangs-target-dissidents/.

48 United States Department of the Treasury, *Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies*, 23 April 2024. https://home.treasury.gov/news/press-releases/jy2292.

49 United States Department of Justice, *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Healthcare Providers*, 25 July 2024. https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

50 Cybersecurity and Infrastructure Security Agency, *Guidance on the North Korean Cyber Threat*, 23 June 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a; Sean Lyngass, "North Korean hackers extorted health care organizations to fund further cyberattacks, US and South Korea say," *CNN*, 9 February 2023. https://www.cnn.com/2023/02/09/politics/north-korea-cyber-health-care-ransom/index.html.

51 Alex O'Neill, "Countering North Korean Cybercrime and Its Enablers," *Lawfare,* 2 May 2024. https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers

52 Rajat Pandit, "Armed forces formulate new doctrine for cyberspace operations," *The Times of India,* 18 June 2024. https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms.

53 Mehul Srivastava and Kaye Wiggins, "India hunts for spyware that rivals controversial Pegasus system," *Financial Times,* 31 March 2023. https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9; Jen Roberts et. al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights," *DFRLab,* 4 September 2024. https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/.

54 Bleeping Computer, *Ransomware as a Service and the Strange Economics of the Dark Web,* 27 March 2024. https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/; Field Effect, *The rise of cybercrime-as-a-service,* 19 April 2023. https://fieldeffect.com/blog/cybercrime-as-a-service; National Cyber Security Centre, *Ransomware, extortion and the cyber crime ecosystem,* 11 September 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6.

55 Alexander Martin, "Ransomware ecosystem fragmenting under law enforcement pressure and distrust," *The Record*, 23 July 2024. https://therecord.media/ransomware-ecosystem-changing-under-law-enforcement-pressure-distrust; Bleeping Computer, *Ransomware as a Service and the Strange Economics of the Dark Web,* 27 March 2024. https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/; Courtney Shea, "Why Canada has so many cyberattacks—and why we're all at risk," *Macleans*, 18 March 2024. https://macleans.ca/society/technology/cyberattacks-canada/; National Cyber Security Centre, *Ransomware, extortion and the cyber crime ecosystem,* 11 September 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6.

56 Sophos, *Sophos 2023 Threat Report: Maturing Criminal Marketplaces Present New Challenges to Defenders*, 17 November 2023. https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf.

57 Intel471, *How Threat Actors Use Underground Marketplaces,* 22 September 2022. https://intel471.com/blog/how-threat-actors-use-underground-marketplaces.

58 Flare, *Top Cybercrime Forums to Monitor in 2023*, 16 May 2023. https://flare.io/learn/resources/blog/top-cybercrime-forums/.

59 Kela, *Telegram: How a Messenger Turned into a Cybercrime Ecosystem by 2023*. https://www.kelacyber.com/wp-content/uploads/2024/01/KELA_Telegram_CEBIN_24.pdf.

60 Alexander Martin, "Genesis Market, one of world's largest platforms for cyber fraud, seized by police," *The Record*, 4 April 2023. https://therecord.media/genesis-market-takedown-cybercrime.

61 United States Department of Justice, *Criminal Marketplace Disrupted in International Cyber Operation,* 5 April 2023. https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.

62 Canadian Centre for Cyber Security, *Baseline cyber threat assessment: Cybercrime,* 28 August 2023. https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime.

63 Royal Canadian Mounted Police, *Fraud Prevention Month 2024: Fighting fraud in the digital era*, 29 February 2024. https://www.rcmp-grc.gc.ca/en/news/2024/fraud-prevention-month-2024-fighting-fraud-the-digital-era.

64 IBM, *What is business email compromise (BEC)?,* https://www.ibm.com/topics/business-email-compromise.

65 Canadian Anti-Fraud Centre, A*nnual Report 2022*. https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-eng.pdf; Royal Canadian Mounted Police, *Fraud Prevention Month 2024: Fighting fraud in the digital era*, 29 February 2024. https://www.rcmp-grc.gc.ca/en/news/2024/fraud-prevention-month-2024-fighting-fraud-the-digital-era.

66 Europol, *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 July 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024; Recorded Future, *2023 Annual Report*, 21 March 2024. https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf.

67 Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,* 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/; Cyber Threat Intelligence Integration Center, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 February 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

68 Alexander Martin, "Ransomware ecosystem fragmenting under law enforcement pressure and distrust," *The Record*, 23 July 2024. https://therecord.media/ransomware-ecosystem-changing-under-law-enforcement-pressure-distrust.

69 Cyber Threat Intelligence Integration Center, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 February 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

70 Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/.

71 Nathaniel Dove, "Canadian firms paying 'significantly' more in ransomware attacks: data," *Global News*, 7 December 2023. http://www.globalnews.ca/news/10155151/companies-1-million-ransomware-attacks/.

72 Chainalysis, *2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder*, 15 August 2024. https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/; Jonathan Grieg, "Ransomware gangs rake in more than $450 million in first half of 2024," *The Record*, 15 August 2024. https://therecord.media/ransomware-gangs-set-record-for-money-extorted; Jordan Pearson, "Ransomware Is 'More Brutal' Than Ever in 2024," *Wired*, 10 June 2024. https://www.wired.com/story/state-of-ransomware-2024/.

73 Karina Zapata, "It's time for companies to double down on cybersecurity measures as ransomware attacks rise, say experts," *CBC*, 11 August 2023. https://www.cbc.ca/news/canada/calgary/cybersecurity-measures-ransomware-attacks-1.6934486.

74 Canadian Centre for Cyber Security, *CSE and international partners publish a cyber security advisory on LockBit ransomware*. https://www.cyber.gc.ca/en/news-events/cse-and-international-partners-publish-cyber-security-advisory-lockbit-ransomware.

75 Canadian Centre for Cyber Security, *Alert - ALPHV/BlackCat Ransomware Targeting of Canadian Industries,* 25 July 2023. https://www.cyber.gc.ca/en/alerts-advisories/alphvblackcat-ransomware-targeting-canadian-industries.

76 Canadian Centre for Cyber Security, *Profile: TA505 / CL0P ransomware*, 11 July 2023, https://www.cyber.gc.ca/en/guidance/profile-ta505-cl0p-ransomware; Sentenniel One, *What is Cl0p ransomware?* https://www.sentinelone.com/anthology/clop/.

77 Internet Crime Complaint Centre, *Joint Cybersecurity Advisory: #StopRansomware: Play Ransomware*, 18 December 2023. https://www.ic3.gov/Media/News/2023/231218.pdf.

78 Cybersecurity Infrastructure & Security Agency, *CISA and Partners Release Advisory on Black Basta Ransomware*, 10 May 2024. https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware.

79 The bar for 2024 represents a projection for what we expect the total number of incidents reported to the Cyber Centre to be, based on the first 6 months of 2024. Since many ransomware incidents go unreported, it is almost certain that the true number of ransomware incidents impacting Canada is higher than what this graph displays.

80 Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,* 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/; Jenna McLaughlin, "The rise in ransomware attacks this year may be related to Russia's war in Ukraine," NPR, 13 July 2023. https://www.npr.org/2023/07/13/1187573935/the-rise-in-ransomware-attacks-this-year-may-be-related-to-russias-war-in-ukrain.

81 Bavi Sadayappan, Zach Riddle, Jordan Nuce, Joshua Shilko, & Jeremy Kennelly, "Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools," *Google Cloud*, 3 June 2024. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools.

82 Laura Hiserodt, "Third-Party Breaches: Risk in the Supply Chain," *Resilience*, 18 October 2023. https://www.cyberresilience.com/threatonomics/third-party-breaches-risk-in-the-supply-chain/.

83 Canadian Centre for Cyber Security, *Profile: TA505 / CL0P ransomware*, 11 July 2023, https://www.cyber.gc.ca/en/guidance/profile-ta505-cl0p-ransomware.

84 Recorded Future, *2023 Annual Report*, 21 March 2024. https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf.

85 Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,* 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/; Recorded Future, *2023 Annual Report*, 21 March 2024. https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf.

86 National Cyber Security Centre, *Ransomware, extortion and the cyber crime ecosystem,* 11 September 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6.

87 Arctic Wolf, *Ransomware-as-a-Service Will Continue to Grow in 2024*, 19 January 2024. https://arcticwolf.com/resources/blog/ransomware-as-a-service-will-continue-to-grow-in-2024/; Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,* 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/; Mandiant, *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, 3 June 2024. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools.

88 Abdulrahman H. Alamri, "Dragos Industrial Ransomware Analysis: Q4 2023," *Dragos*, 25 January 2024. https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/; Canadian Centre for Cyber Security, *Baseline cyber threat assessment: Cybercrime,* 28 August 2023. https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime; Canadian Centre for Cyber Security, *The cyber threat to Canada's oil and gas sector,* https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector.

89 Alexander Martin, "Ransomware attacks leave small business owners feeling suicidal, report says," *The Record*, 17 January 2024. https://therecord.media/small-business-ransomware-attacks-mental-health-rusi-study.

90 Andy Greenberg, "Change Healthcare Finally Admits it Paid Ransomware Hackers $22 Million – and Still Faces a Patient Data Leak," *Wired*, 22 April 2024. https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/; Dee-ann Durbin, "Meat company JBS Foods confirms it paid US$11M ransom in cyberattack," *Global News*, 9 June 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*, 9 June 2021. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

91 Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/.

92 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Threat to operational technology*, 16 December 2021. http://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology.

93 Canadian Centre for Cyber Security, *Baseline cyber threat assessment: Cybercrime,* 28 August 2023. https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime.

94 Paula Duhatschek, "Suncor swaps out laptops after cybersecurity incident as energy sector takes stock of risks," *CBC*, 6 July 2023. https://www.cbc.ca/news/canada/calgary/suncor-cybersecurity-incident-energy-sector-1.6898118; Suncor, *Update on Suncor Energy response to cybersecurity incident*, 6 July 2023. https://www.suncor.com/-/media/project/suncor/files/news-releases/2023/2023-07-06-nr-su-update-cybersecurity-incident-en.pdf?modified=20230706200434&_ga=2.177511533.959371021.1688674862-1934455315.1687893565.

95 Canadian Centre for Cyber Security, *Baseline cyber threat assessment: Cybercrime,* 28 August 2023. https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime; SickKids, *SickKids lifts Code Grey with 80 per cent of priority systems restored,* 5 January 2023. https://www.sickkids.ca/en/news/archive/2023/sickkids-lifts-code-grey-with-80-per-cent-of-priority-systems-restored/.

96 Chatham-Kent Health Alliance, *Update on Cyber Attacks at Regional Hospitals*, 31 October 2023. https://www.ckha.on.ca/update-on-cyber-attacks-at-regional-hospitals-2/; David Musyj, *CYBER ATTACK STATEMENT*, 3 April 2024. https://windsor.bluelemonmedia.com/uploads/Common/News/Cyberattack_Statement_Apr_3_2024.pdf; Rich Garton, "Notorious ransomware group claims responsibility for local hospitals cyberattack," *CTV News*, 3 November 2023. https://windsor.ctvnews.ca/notorious-ransomware-group-claims-responsibility-for-local-hospitals-cyberattack-1.6630237.

97 Akshay Kulkarni, "London Drugs confirms it was victim of ransomware attack," *CBC News*, 21 May 2024. https://www.cbc.ca/news/canada/british-columbia/london-drugs-ransomware-attack-1.7210754; Sergiu Gatlan, "LockBit says they stole data in London Drugs ransomware attack," *Bleeping Computer,* 21 May 2024. https://www.bleepingcomputer.com/news/security/lockbit-says-they-stole-data-in-london-drugs-ransomware-attack/.

98 Government of Nova Scotia, *Update on MOVEit Global Security Breach,* 6 June 2023. https://news.novascotia.ca/en/2023/06/06/update-moveit-global-security-breach.

99 Department of National Defence, *Update: Incident affecting Brookfield Global Relocation Services (BGRS) systems,* 20 October 2023. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2023/10/update-incident-affecting-brookfield-global-relocation-services-systems.html; Kailee Hilt, "As We Enter 2024, Cyberthreats to Canada Are Growing," *Centre for International Governance Innovation*, 28 December 2023. https://www.cigionline.org/articles/as-we-enter-2024-cyberthreats-to-canada-are-growing/.

100 City of Hamilton, *City Confirms Cyber Incident is a Ransomware Attack*, 5 March 2024. https://www.hamilton.ca/city-council/news-notices/news-releases/city-confirms-cyber-incident-ransomware-attack.

101 Cyber Threat Intelligence Integration Center, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 February 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

102 Zack Whittaker, "How the ransomware attack at Change Healthcare went down: A timeline," *Tech Crunch*, 17 August 2024. https://techcrunch.com/2024/08/17/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/.

103 BBC, *Hospitals cyber attack impacts 800 operations*, 14 June 2024. https://www.bbc.com/news/articles/cd11v377eywo; Joe Tidy, "Stolen test data and NHS numbers published by hospital hackers," *BBC*, 21 June 2024. https://www.bbc.com/news/articles/c9ww90j9dj8o.

104 Cyber Threat Intelligence Integration Center, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 February 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

105 Abdulrahman H. Alamri, "Dragos Industrial Ransomware Analysis: Q4 2023," *Dragos,* 25 January 2024. https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/.

106 Chainalysis, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,* 7 February 2024. https://www.chainalysis.com/blog/ransomware-2024/.

107 Chainalysis, *Examining the Impact of Ransomware Disruptions: Qakbot, LockBit, and BlackCat,* 6 May 2024. https://www.chainalysis.com/blog/ransomware-disruptions-impact/.

108 Europol, *Internet Organized Crime Threat Assessment (IOCTA) 2024,* 26 July 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

109 Bleeping Computer, *Ransomware as a Service and the Strange Economics of the Dark Web,* 27 March 2024. https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/; National Cyber Security Centre, *Ransomware, extortion and the cyber crime ecosystem,* 11 September 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6.

110 Europol, *Internet Organized Crime Threat Assessment (IOCTA)2024,* 26 July 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

111 Matt Burgess & Lily Hay Newman, "The Unrelenting Menace of the LockBit Ransomware Gang," *Wired*, 24 January 2023. https://www.wired.com/story/lockbit-ransomware-attacks/; Sergiu Gatlan, "FBI: ALPHV ransomware raked in $300 million from over 1,000 victims," *Bleeping Computer*, 19 December 2023. https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/; United States Department of Justice, *U.S. Department of Justice Disrupts Hive Ransomware Variant*, 26 January 2023. https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

112 United States Department of Justice, *U.S. Department of Justice Disrupts Hive Ransomware Variant*, 26 January 2023. https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

113 United States Department of Justice, *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant,* 19 December 2023. https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

114 Europol, *Law enforcement disrupt world's biggest ransomware operation*, 20 February 2024. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

115 Europol, *Internet Organized Crime Threat Assessment (IOCTA)2024,* 26 July 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

116 Europol, *Internet Organized Crime Threat Assessment (IOCTA)2024,* 26 July 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.; Mathew J. Schwartz, "Ever More Toxic Ransomware Brands Breed Lone Wolf Operators," *BankInfoSecurity*, 1 August 2024. https://www.bankinfosecurity.com/blogs/ever-more-toxic-ransomware-brands-breed-lone-wolf-operators-p-3682.

117 Abdulrahman H. Alamri, "Dragos Industrial Ransomware Analysis: Q4 2023," *Dragos,* 25 January 2024. https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/; Lucian Constantin, "Emerging ransomware groups on the rise: Who they are, how they operate," *CSO*, 24 May 2024. https://www.csoonline.com/article/2121702/emerging-ransomware-groups-on-the-rise-who-they-are-how-they-operate.html.

118 Jordan Pearson, "Ransomware Is 'More Brutal' Than Ever in 2024," *Wired*, 10 June 2024. https://www.wired.com/story/state-of-ransomware-2024/; Matt Kapko, "Ransomware gangs incite fear in victims to fuel attacks," *Cybersecurity Dive*, 21 March 2023. https://www.cybersecuritydive.com/news/ransomware-gangs-extortion-unit42/645544/.

119 Jordan Pearson, "Ransomware Is 'More Brutal' Than Ever in 2024," *Wired*, 10 June 2024. https://www.wired.com/story/state-of-ransomware-2024/; Sophos, *Turning the screws: The pressure tactics of ransomware gangs*, 6 August 2024. https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/.

120 Mandiant, *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, 3 June 2024. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools; Sophos, *Turning the screws: The pressure tactics of ransomware gangs*, 6 August 2024. https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/.

121 Abdulrahman H. Alamri, "Dragos Industrial Ransomware Analysis: Q4 2023," *Dragos,* 25 January 2024. https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/.

122 Federal Bureau of Investigation, *Private Industry Notification*, 27 September 2023. https://www.ic3.gov/Media/News/2023/230928.pdf.

123 SC Media, *Remote ransomware: What is and how to stop it*, 12 January 2024. https://www.scmagazine.com/resource/remote-ransomware-what-is-and-how-to-stop-it.

124 Alexander Culafi, "CISA: Akira ransomware extorted $42M from 250+ victims," *TechTarget*, 19 April 2024. https://www.techtarget.com/searchsecurity/news/366581522/CISA-Akira-ransomware-extorted-42M-from-250-plus-victims; Recorded Future, *Ransomware Examples*. https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-examples; Trend Micro, *What is Ransomware?*, https://www.trendmicro.com/en_us/what-is/ransomware.html.

125 ThreatDown, *Threat Brief: Ransomware Gangs & Living Off the Land Attacks*, 1 November 2023. https://www.threatdown.com/wp-content/uploads/2024/05/TD_ThreatBrief_Ransomware_LOTL_Ebook_EN_11142023.pdf.

126 Sophos, *Sophos 2023 Threat Report: Maturing Criminal Marketplaces Present New Challenges to Defenders*, 17 November 2023. https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf.

127 Daniel Sergile, "The Evolving Threat of Ransomware – A Call to Action for Cybersecurity," *Palo Alto*, 17 April 2024. http://www.paloaltonetworks.com/blog/2024/04/the-evolving-threat-of-ransomware/.

128 Karen Weise, "In Race to Build A.I., Tech Plans a Big Plumbing Upgrade," *The New York Times,* 27 April 2024. https://www.nytimes.com/2024/04/27/technology/ai-big-tech-spending.html; Jordan Jacobs, "Canadian AI Sovereign Compute Strategy," *Radical Ventures,* 7 April 2024. https://radical.vc/canadian-ai-sovereign-compute-strategy/; Dylan Patel et. al., "AI Datacenter Energy Dilemma – Race for AI Datacenter Space," *Semianalysis,* 13 March 2024. https://www.semianalysis.com/p/ai-datacenter-energy-dilemma-race; Brookfield Renewable Partners, *Brookfield and Microsoft Collaborating to Deliver Over 10.5 GW of New Renewable Power Capacity Globally,* 1 May 2024. https://bep.brookfield.com/press-releases/bep/brookfield-and-microsoft-collaborating-deliver-over-105-gw-new-renewable-power; Cade Metz, "A Hacker Stole OpenAI Secrets, Raising Fears that China Could, Too," *The New York Times,* 4 July 2024. https://www.nytimes.com/2024/07/04/technology/openai-hack.html?smid=nytcore-ios-share&referringSource=articleShare; Chris Miller, "The global chip war could turn into a cloud war," *Financial Times,* 30 July 2024. https://www.ft.com/content/202c3240-fa20-4081-a2a7-8470b7f12110; CTIA, *2024 Annual Survey Highlights,* 10 September 2024. https://www.ctia.org/news/2024-annual-survey-highlights.

129 KrebsonSecurity, *3CX Breach Was a Double Supply Chain Compromise,* 20 April 2023. https://krebsonsecurity.com/2023/04/3cx-breach-was-a-double-supply-chain-compromise/.

130 Mandiant, *M-Trends 2024 Special Report,* https://cloud.google.com/security/resources/m-trends; Mandiant, *Analysis of Time-to-Exploit Trends: 2021-2022,* 28 September 2023. https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2021-2022/.

131 National Institute of Standards and Technology, *National Vulnerability Database.* https://nvd.nist.gov/vuln/data-feeds.

132 Eric Schmidt, "AI, Great Power Competition & National Security," *Daedalus* (2022) 151 (2): 288-298. https://direct.mit.edu/daed/article/151/2/288/110603/AI-Great-Power-Competition-amp-National-Security

133 Rachel Metz, "OpenAI Scale Ranks Progress Toward 'Human-Level' Problem Solving, *Bloomberg,* 11 July 2024. https://www.bloomberg.com/news/articles/2024-07-11/openai-sets-levels-to-track-progress-toward-superintelligent-ai; Aaron Holmes, "To Unlock AI Spending, Microsoft, OpenAI and Google Prep 'Agents'," *The Information,* 18 April 2024. https://www.theinformation.com/articles/to-unlock-ai-spending-microsoft-openai-and-google-prep-agents; Cade Metz, "OpenAI Unveils New ChatGPT That Can Reason Through Math and Science," *The New York Times,* 12 September 2024. https://www.nytimes.com/2024/09/12/technology/openai-chatgpt-math.html.

134 Responsible AI Collaborative. *AI Incident Database*. https://incidentdatabase.ai/. Further annotation of incidents in the database was performed by Canadian Centre for Cyber Security staff.

135 FBI, *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence,* 8 May 2024. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence; Check Point Team, *Generative AI is the Pride of Cybercrime Services,* 1 February 2024. https://blog.checkpoint.com/research/generative-ai-is-the-pride-of-cybercrime-services/; Vincenzo Ciancaglini and David Sancho, "Back to the Hype. An update on How Cybercriminals Are Using GenAI," *Trend Micro,* 8 May 2024. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai.

136 Cybersecurity and Infrastructure Security Agency, *NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats,* 12 September 2023. https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats; Heather Chen and Kathleen Magramo, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'," *CNN,* 4 February 2024. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html; Matt Burgess, "The Real-Time Deepfake Romance Scams Have Arrived," *Wired,* 18 April 2024. https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/; Benj Edwards, "Deep-Live-Cam goes viral, allowing anyone to become a digital doppelganger," *arsTechnica,* 13 August 2024. https://arstechnica.com/information-technology/2024/08/new-ai-tool-enables-real-time-face-swapping-on-webcams-raising-fraud-concerns/.

137 Dena De Angelo, "The Dark Side of AI in Cybersecurity – AI-Generated Malware," *Paloalto Networks,* 15 May 2024. https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/; Matz, S.C., Teeny, J.D., Vaid, S.S. *et al.* The potential of generative AI for personalized persuasion at scale. *Sci Rep* 14, 4692 (2024). https://www.nature.com/articles/s41598-024-53755-0.

138 Meta, *Adversarial Threats,* First Quarter, May 2024. https://transparency.meta.com/metasecurity/threat-reporting; OpenAI, *AI and Covert Influence Operations: Latest Trends,* May 2024. https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/; Jeff Stone and Daniel Zuidijk, "Russian Bots Use Fake Tom Cruise for Olympic Disinformation," *Bloomberg,* 3 June 2024. https://www.bloomberg.com/news/articles/2024-06-03/russian-bots-use-fake-tom-cruise-for-olympic-disinformation; Nicholas Dufour et al., *AMMEBA : A Large-Scale Survey and Dataset of Media-Based Misinformation In-The-Wild,* 19 May 2024. https://arxiv.org/abs/2405.11697; Sheera Frenkel, "Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War," *The New York Times,* 5 June 2024. https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html; Omer Benjakob, "Israel Secretly Targeted American Lawmakers with Gaza War Influence Campaign," *Haaretz,* 5 June 2024. https://www.haaretz.com/israel-news/security-aviation/2024-06-05/ty-article-magazine/.premium/israel-secretly-targeted-american-lawmakers-with-gaza-war-influence-campaign/0000018f-e7c8-d11f-a5cf-e7cb62af0000; Stephanie Levitz, Alex Ballingall, and Mark Ramzy, "Trudeau government raises concerns with Israel about 'Islamophobic' misinformation campaign that is 'targeting Canadians'," *The Toronto Star,* 11 June 2024. https://www.thestar.com/politics/federal/trudeau-government-raises-concerns-with-israel-about-islamophobic-misinformation-campaign-that-is-targeting-canadians/article_3c854d48-274f-11ef-865d-a3f2559953b0.html; DFRLab, *Inauthentic campaign amplifying Islamophobic content targeting Canadians,* 28 March 2024. https://dfrlab.org/2024/03/28/inauthentic-campaign-amplifying-islamophobic-content-targeting-canadians/; U.S. Department of Justice, *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere,* 4 September 2024. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

139 Canadian Centre for Cyber Security, *Russian state-sponsored media organization leverages AI-enhanced "Meliorator" software for foreign influence activity,* 9 July 2024. https://www.cyber.gc.ca/en/news-events/russian-state-sponsored-media-organization-leverages-ai-enhanced-meliorator-software-foreign-malign-influence-activity

140 Canadian Centre for Cyber Security, *The threat from large language model text generators,* 17 January 2024. https://www.cyber.gc.ca/en/guidance/threat-large-language-model-text-generators; Canadian Centre for Cyber Security, *Cyber Threats to Canada's Democratic Process: 2023 update,* 6 December 2023. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update; Global Affairs Canada, *Russia's use of disinformation and information manipulation,* 28 February 2024. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng; Dustin Volz, "China is Targeting U.S. Voters and Taiwan with AI-Powered Disinformation," *The Wall Street Journal,* 5 April 2024. https://www.wsj.com/politics/national-security/china-is-targeting-u-s-voters-and-taiwan-with-ai-powered-disinformation-34f59e21.

141 Jelena Vicic and Richard Harknett, "The mechanisms of cyber-enabled information campaigning," *Binding Hook,* 21 June 2024. https://bindinghook.com/articles-binding-edge/the-mechanisms-of-cyber-enabled-information-campaigning/; Brandy Zadrozny, "Disinformation poses an unprecedented threat in 2024 – and the U.S. is less ready than ever," *NBC News,* 18 January 2024. https://www.nbcnews.com/tech/misinformation/disinformation-unprecedented-threat-2024-election-rcna134290; Olga Belogolova, Lee Foster, Thomas Rid, and Gavin Wilde. "Don't Hype the Disinformation Threat," *Foreign Affairs,* 3 May 2024. https://www.foreignaffairs.com/russian-federation/dont-hype-disinformation-threat; Josh A. Goldstein and Renée DiResta, "Propagandists are using AI too – and companies need to be open about it," *MIT Technology Review,* 8 June 2024. https://www.technologyreview.com/2024/06/08/1093356/propagandists-are-using-ai-too-and-companies-need-to-be-open-about-it/; Cat Zakrzewski and Joseph Menn, "Russia and China Pounce on Trump Rally Shooting to Undermine U.S.," *The Washington Post,* 17 July 2024. https://www.washingtonpost.com/technology/2024/07/17/trump-shooting-china-russia-disinformation-campaign/; Matt Honeycombe-Foster and Andrew Mcdonald, "UK probes whether 'state actors' stoked far-right riots," *Politico,* 5 August 2024. https://www.politico.eu/article/uk-probes-whether-state-actors-stoked-far-right-riots/; Will Bedingfield, "Generative AI is Playing a Surprising Role in Israel-Hamas Disinformation," *Wired,* 30 October 2023. https://www.wired.com/story/israel-hamas-war-generative-artificial-intelligence-disinformation/; Andrew Ross Sorkin et. al., "An A.I.-Generated Spoof Rattles the Markets," *The New York Times,* 23 May 2023. https://www.nytimes.com/2023/05/23/business/ai-picture-stock-market.html.

142 Eric Berger, "Deluge of 'pink slime' websites threaten to drown out truth with fake news in US election," *The Guardian,* 20 June 2024. https://www.theguardian.com/us-news/article/2024/jun/20/fake-news-websites-us-election; Dan Patterson, "Black Hat 2024: Foreign Influence Operations Evolve as Narrative Attacks Become Sophisticated," Blackbird.AI *RAV3N Blog,* 7 August 2024. https://blackbird.ai/blog/foreign-influence-operations-evolve-as-narrative-attacks-grow-more-sophisticated/; Steven Lee Myers, Tiffany Hsu, and Farnaz Fassihi, "Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race," *The New York Times,* 4 September 2024. https://www.nytimes.com/2024/09/04/business/media/iran-disinformation-us-presidential-race.html.

143 Paul Scharre, *Four Battlegrounds. Power in the Age of Artificial Intelligence*, (New York: W.W. Norton & Company, Inc., 2023); *UAE's Edge Group and G42 get into natural language processing,* Intelligence Online, 22 March 2023. https://www.intelligenceonline.com/surveillance--interception/2023/03/22/uae-s-edge-group-and-g42-get-into-natural-language-processing,109926405-art; Palantir Technologies Inc., Form 10-K Annual Report for the fiscal year ended December 31, 2023. https://www.sec.gov/ix?doc=/Archives/edgar/data/1321655/000132165524000022/pltr-20231231.htm.

144 Mandiant, *M-Trends 2024 Special Report,* https://cloud.google.com/security/resources/m-trends?hl=en; Cisco Talos, *ArcaneDoor – New espionage-focused campaign found targeting perimeter network devices,* 24 April 2024. https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/; Andy Greenberg, "Russia's New Cyberwarfare in Ukraine is Fast, Dirty, and Relentless, 10 November 2022. https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

145 Canadian Centre for Cyber Security, *Cyber Activity Impacting CISCO ASA VPNs,* 24 April 2024. https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns

146 Canadian Centre for Cyber Security, *Joint advisory on PRC state-sponsored actors compromising and maintaining persistent access to U.S. critical infrastructure and joint guidance on identifying and mitigating living off the land,* 7 February 2024. https://www.cyber.gc.ca/en/news-events/joint-advisory-prc-state-sponsored-actors-compromising-and-maintaining-persistent-access-us-critical-infrastructure-and-joint-guidance-identifying-and-mitigating-living-land-0; Australian Cyber Security Centre, *Identifying and Mitigating Living Off the Land Techniques,* 8 February 2024. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques.

147 Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity,* 3 June 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity.

148 Cybersecurity and Infrastructure Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,* 7 February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; Gabby Roncone et. al.,"APT44: Unearthing Sandworm," *Mandiant,* 17 April 2024. https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.

149 Ken Proska et. al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology," *Mandiant,* 9 November 2023. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/; Andy Greenberg, "Sandworm Hackers Caused Another Blackout in Ukraine – During a Missile Strike," *Wired,* 9 November 2023. https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.

150 Mandiant, *M-Trends 2024 Special Report,* https://cloud.google.com/security/resources/m-trends?hl=en

151 The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President. Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors,* 26 September 2023. https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee/presidents-nstac-publications

152 United States Department of Justice, *Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU),* 15 February 2024. https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian; Canadian Centre for Cyber Security, *Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity,* 3 June 2024. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity.

153 Andy Greenberg, "Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities," *Wired,* 17 April 2024. https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/; United States Department of the Treasury, *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn,* 19 July 2024. https://home.treasury.gov/news/press-releases/jy2473; National Cyber Security Centre, *Heightened threat of state-aligned groups against western critical national infrastructure,* 1 May 2024. https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups; Cybersecurity and Infrastructure Security Agency, *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity,* 1 May 2024. https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity; Mauro Vignati, "Civilian hackers blur the lines of modern conflict," *Binding Hook,* 13 December 2023. https://bindinghook.com/articles-hooked-on-trends/civilian-hackers-blur-the-lines-of-modern-conflict/.

154 Daniel Kapellmann Zafra et al., "Global Revival of Hacktivism Requires Increased Vigilance from Defenders," *Mandiant,* 27 June 2024. https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism; Akinobu Iwasawa, "Israel-Hamas war draws Russian, Indian 'hacktivists' into shadow conflict," *Nikkei Asia,* 27 October 2023. https://asia.nikkei.com/Politics/Middle-East-crisis/Israel-Hamas-war-draws-Russian-Indian-hacktivists-into-shadow-conflict; Canadian Centre for Cyber Security, *Alert – Risk of malicious cyber activity against Ukraine-aligned nations,* 24 February 2023. https://www.cyber.gc.ca/en/alerts-advisories/risk-malicious-cyber-activity-against-ukraine-aligned-nations; Canadian Centre for Cyber Security, *Alert – Distributed Denial of Service campaign targeting multiple Canadian Sectors,* 15 September 2023. https://www.cyber.gc.ca/en/alerts-advisories/distributed-denial-service-campaign-targeting-multiple-canadian-sectors.

155 Dylan Robertson, "Cyberattacks hit military, Parliament websites as India-based group targets Canada," *CBC News,* 28 September 2023. https://www.cbc.ca/news/politics/cyberattacks-parliament-india-1.6981399

156 Radware, *Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists,* 21 April 2023. https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/

157 Eric Schmidt, "AI, Great Power Competition & National Security," *Daedalus* (2022) 151 (2): 288-298. https://direct.mit.edu/daed/article/151/2/288/110603/AI-Great-Power-Competition-amp-National-Security; Peter Brennan and Chris Hudgins, "Market-leading US companies consolidate power in era of 'superstar' firms," *S&P Global,* 17 January 2023. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/market-leading-us-companies-consolidate-power-in-era-of-superstar-firms-73773141;

158 Belle Lin, "CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry," *Wall Street Journal,* 29 June 2024. https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d; Bastian Benrath, "AI Risks to Financial Stability Are Already a Central Bank Worry," *Bloomberg,* 7 May 2024; Drew Bagley, "Achieving Ecosystem-level Cybersecurity: A U.S. Policy Perspective," *Crowdstrike Blog,* 11 June 2024. https://www.crowdstrike.com/blog/next-steps-for-ecosystem-level-cybersecurity/; Jeanette MAnfra and Charley Snyder, "CSRB report highlights the need for new approaches to securing the public sector," *Google,* 20 May 2024. https://blog.google/technology/safety-security/csrb-report-google-recommendations/; Office of the Superintendent of Financial Institutions, *Third-Party Risk Management Guideline,* https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/third-party-risk-management-guideline.

159 Tianjiu Zuo, Justin Sherman, Maia Hamin, and Stewart Scott, "Critical Infrastructure and the Cloud: Policy for Emerging Risk," *DFRLab,* 10 July 2023. https://dfrlab.org/2023/07/10/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/. Microsoft Corporation, Form 10-Q for the Quarterly period ended December 31, 2023. https://www.sec.gov/Archives/edgar/data/789019/000095017024008814/msft-20231231.htm#item_1a_risk_factors; Cybersecurity and Infrastructure Security Agency, *SVR Cyber Actors Adapt Tactics for Initial Cloud Access,* 26 February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a.

160 Microsoft Threat Intelligence, *Midnight Blizzard: Guidance for responders on nation-state attack,* 25 January 2024. https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/; Microsoft Corporation, Form 10-K For the Fiscal Year Ended June 30, 2023. https://microsoft.gcs-web.com/static-files/e2931fdb-9823-4130-b2a8-f6b8db0b15a9; Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2023. https://www.sec.gov/Archives/edgar/data/1652044/000165204424000022/goog-20231231.htm; Felix Richter, "Amazon Maintains Cloud Lead as Microsoft Edges Closer," *Statista,* 2 May 2024. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

161 Eric Geller, "The US Government Has a Microsoft Problem," *Wired,* 15 April 2024. https://www.wired.com/story/the-us-government-has-a-microsoft-problem/; Cybersecurity and Infrastructure Security Agency, *Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System,* 2 April 2024. https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

162 Cyber Safety Review Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion,* 20 March 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf; Lionel Sujay Vailshery, "Market share of major office productivity software worldwide in 2024", *Statista,* 9 February 2024. https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/; UnitedHealth Group Incorporated, Form 8-K (Amendment No. 1), 21 February 2024, https://www.sec.gov/ix?doc=/Archives/edgar/data/0000731766/000073176624000085/unh-20240221.htm; Belle Lin, "CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry," *Wall Street Journal,* 29 June 2024. https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d; Jonathan Greig, "Multiple car dealers report disruptions to SEC due to cyberattack on software company," *The Record,* 24 June 2024. https://therecord.media/car-dealerships-reports-sec-cdk-software-ransomware; Brookfield Business Partners, *Corporate Profile,* February 2024. https://bbu.brookfield.com/sites/bbu-brookfield-ir/files/2024-02/bbu-q4-2023-corporate-profile-feb-6.pdf; AutoCanada, *AUTOCANADA PROVIDES UPDATE ON CDK CYBER SECURITY INCIDENT,* 4 July 2024. https://investors.autocan.ca/2024/07/autocanada-provides-update-on-cdk-cyber-security-incident/.

163 Dan Geer, Eric Jardine & Eireann Leverett, "On market concentration and cybersecurity risk," *Journal of Cyber Policy,* (2020), 5:1, 9-29. https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1728355.

164 Cyber Safety Review Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion,* 20 March 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

165 Matthew Schwartz, "Microsoft Azure Cloud Service Fails to Withstand DDoS Attack," *Gov Info Security,* 31 July 2024. https://www.govinfosecurity.com/microsoft-azure-cloud-service-fails-to-withstand-ddos-attack-a-25893.

166 Microsoft, *Mitigation Statement – Azure Front Door – Issues accessing a subset of Microsoft services,* Tracking ID: KTY1-HW8, 30 July 2024. https://azure.status.microsoft/en-us/status/history/; Eduard Kovacs, "Microsoft Says Azure Outage Caused by DDoS Attack Response," *SecurityWeek,* 31 July 2024. https://www.securityweek.com/microsoft-says-azure-outage-caused-by-ddos-attack-response/.

167 United States Department of Defence, *Deputy Secretary of Defence Kathleen Hicks Keynote Address: 'The Urgency to Innovate' (As Delivered),* 28 August 2023. https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/; Amy B. Zegart, "American Spy Agencies are Struggling in the Age of Data," *Wired,* 2 February 2022. https://www.wired.com/story/spies-algorithms-artificial-intelligence-cybersecurity-data/; Audrey Kurth Cronin, "How Private Tech Companies are Reshaping Great Power Competition," *The Kissinger Center Papers,* August 2023. https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition; United States Space Force, *U.S. Space Force Commercial Space Strategy: Accelerating the Purposeful Pursuit of Hybrid Space Architectures,* 8 April 2024. https://www.spaceforce.mil/News/Article-Display/Article/3736616/ussf-releases-commercial-space-strategy-to-increase-competitive-advantage/; Jonathan Horowitz, "One click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict," *Chicago Journal of International Law,* Vol. 24, No. 2, Winter 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4470988

168 National Counterintelligence and Security Center, *Safeguarding the US Space Industry,* 18 August 2023. https://www.dni.gov/index.php/ncsc-features/2762-safeguarding-our-future; Palantir Technologies Inc., Form 10-K Annual Report for the fiscal year ended December 31, 2023. https://www.sec.gov/ix?doc=/Archives/edgar/data/1321655/000132165524000022/pltr-20231231.htm.

169 Reuters, *Russia warns West: We can target your commercial satellites,* 27 October 2022. https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/; Paul Mozur and Adam Satariano, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service," *The New York Times,* 24 May 2024. https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

170 Global Affairs Canada. *Statement on Russia's malicious cyber activity affecting Europe and Ukraine,* 10 May 2022. https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html; Paul Mozur and Adam Satariano, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service," *The New York Times,* 24 May 2024. https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

171 Sam Fleming, Demetri Sevastopulo, and Clair Jones, "How national security has transformed economic policy," *Financial Times,* 4 September 2024. https://www.ft.com/content/6068310d-4e01-42df-8b10-ef6952804604; Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order,* (New York: Oxford University Press, 2021). Elias X. Huber, "Technology Controls to Contain China's Quantum Ambitions Are Here," *Lawfare,* 22 August 2024. https://www.lawfaremedia.org/article/technology-controls-to-contain-china-s-quantum-ambitions-are-here

172 Parag Khanna, "The Coming Entropy of Our World Order," *NOEMA,* 7 May 2024. https://www.noemamag.com/the-coming-entropy-of-our-world-order/.

173 https://www.cyber.gc.ca/en/guidance

174 https://www.cyber.gc.ca/en/cyber-security-readiness-goals/cross-sector-cyber-security-readiness-goals-toolkit