

UQÀM



RAOUL DANDURAND CHAIR
OF STRATEGIC AND DIPLOMATIC STUDIES

25 years

Geopolitical Cyber Incidents in Canada

2022 ASSESSMENT

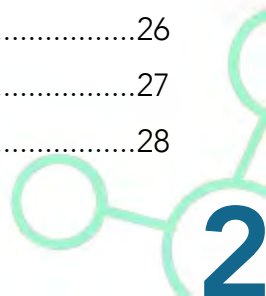
By the Center on Multidimensional Conflicts
(Observatoire des conflits multidimensionnels)



@Joiseyshowaa/Flickr

Summary

Who we are	3
About the authors.....	4
A few recent cyber incidents	5
Canada and geopolitical cyber incidents: a 2022 snapshot	6
Box: what do we mean by cyber incidents?.....	7
Three major trends to watch in the near future	11
Activists, dissenters, and exiles: the exportation of surveillance.....	11
Hackers-for-hire: Canada and the rise of cyber-mercenaries.....	16
Ransomwares: when criminality edges towards geopolitics.....	21
Conclusion: the Ukrainian factor	26
How this report was established	27
Typology and definitions of incidents	28





Who we are

The Center on Multidimensional Conflicts (Observatoire des conflits multidimensionnels or OCM) of the Raoul Dandurand Chair was created in 2019 with the support of the National Bank of Canada. The OCM is led by Frédéric Gagnon, a political science professor at the Université du Québec à Montréal (UQAM) and holder of the Raoul Dandurand Chair. The center brings together Canadian and international researchers studying novel strategies which foreign actors, particularly nation-states, deploy internationally to destabilize states, weaken their societies and institutions, or to undermine their critical systems and infrastructure. Cyber attacks, disinformation, political and electoral interference, and geoeconomics are among phenomena analyzed by the OCM. The OCM contributes to the fostering of Canadian debates on these topics through publications, conferences, and media interventions. It also aims to inform the public and raise awareness on the impact of contemporary security changes, including the malicious use of digital technologies, on states such as Canada, their governments, civil society, the private sector, and citizens.





About the authors

Frédéric Gagnon holds the Raoul Dandurand Chair, is Director of the OCM, and a political science professor at UQAM. He is a recognized expert of U.S. politics, U.S. foreign policy, and Canada–U.S. relations. His recent work at the OCM has focused on Russian interference and disinformation in the 2016 U.S. election, U.S. cyber conflict management, and the impact of geoeconomic competition between China and the U.S. on Canada–U.S. relations.

Alexis Rapin is a scholar-in-residence at the OCM. He holds a degree in international relations from the University of Geneva and a Master's degree in international studies from the Université de Montréal. He studies the transformation of warfare, such as cyber defence and the rise of disinformation strategies, as well as the impacts of new technologies on international security. He has contributed to a number of books in English and French on armed conflicts and foreign policy.

Danny Gagné is a Ph.D. student in political science at UQAM and a scholar-in-residence at the OCM. His research focuses on the use of drone warfare in the US. His recent work at the OCM has been the subject of numerous “Chroniques des nouvelles conflictualités” (published by the Raoul Dandurand Chair) discussing the strategic use of disinformation, such as Russian campaigns targeting Canadian troops stationed in Eastern Europe.

Gabrielle Gendron is a Master's student in political science at UQAM and a scholar-in-residence at the OCM. Her work focuses mainly on the development of the digital economy and new Chinese technologies, cyber security in Southeast Asia, digital initiatives under the Belt and Road Initiative (BRI), and global Chinese digital exports. She also contributes regularly to the “Chroniques des nouvelles conflictualités” (published by the Raoul Dandurand Chair).



A few recent cyber incidents



February 2020

DISINFORMATION ON THE ORIGIN OF COVID-19

Various Russian and Arabic-speaking propaganda websites spread false allegations that COVID-19 was created in Canadian laboratories, and then sent to China. Other versions of the rumors allege that the virus was stolen by Chinese spies infiltrated in Canada.



November 2020

CYBER ESPIONAGE TARGETING COVID-19 RESEARCH

A new wave of pharmaceutical cyber espionage targets 7 companies involved in COVID-19 related research. These activities impacted five countries, including Canada. Microsoft attributes these hacks to three state-sponsored groups located in North Korea and Russia.

February 2021

TAKEDOWN OF INAUTHENTIC RUSSIAN TWITTER ACCOUNTS

Twitter takes down 373 inauthentic accounts suspectedly used by nation-states to spread disinformation. Among these, the Canadian entity DisinfoWatch identified various accounts of Russian origin which have produced Canada-related tweets. The content discussed issues related to the Arctic and NATO, as well as various Canadian political figures, including Justin Trudeau, Stephen Harper, and Chrystia Freeland.

January 2022

CYBER INCIDENT AT GLOBAL AFFAIRS CANADA

Global Affairs Canada is hit by a cyber incident. Various online services of the ministry are temporarily deactivated. As a diplomatic crisis mounts between Russia and Ukraine, some anonymous governmental sources suggest that Russia may bear some responsibility in the incident.

September 2020

IRANIAN ACTIVISTS TARGETED BY A SURVEILLANCE CAMPAIGN

A NGO report exposes a vast campaign of cyber espionage against activists defending human rights in Iran. The campaign targeted several hundred individuals in fifteen countries, including Canada.

October 2020

CYBER ESPIONAGE CAMPAIGN BY "SILENT LIBRARIAN"

A cybersecurity company reveals that an Iranian hacker group, Silent Librarian, attempted to compromise various universities across 8 countries, including Canada. The University of Toronto, Western University, and McGill University are among the targeted entities.

CYBER INCIDENT AT NSIRA

The National Security and Intelligence Review Agency (NSIRA) announces that it has experienced a "cyber incident". Protected, though not classified, data was compromised by a third-party. The culprit's identity is not revealed by the agency.

MARCH 2021

UYGHUR ACTIVISTS TARGETED BY A SURVEILLANCE CAMPAIGN

Facebook exposes a vast Chinese cyber espionage operation that targeted Uyghur journalists and human rights activists in several countries. According to Facebook, about 20 of these individuals reside in Canada.

2020

2021

2022



CANADA AND GEOPOLITICAL CYBER INCIDENTS: A 2022 SNAPSHOT

In 2021, more than ever before, few weeks passed without media revelations of a new cyberattack, an operation of electronic surveillance, or a disinformation campaign somewhere around the world. Among other factors, the prolonged COVID-19 pandemic has contributed to the multiplication of cyber incidents, which have not spared Canada. While the vast majority of such activities remain criminal in nature, state-sponsored cyber incidents with geopolitical implications are still frequent. For instance, in January 2022 Global Affairs Canada revealed it had experienced a major cyber breach, which some unnamed governmental sources tended to associate to the Russian state.

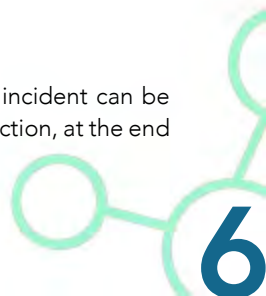
As more and more nation-states now appear entangled in a constant state of international cyber rivalry, such incidents have become quite constant in Canada: the analysis we conducted for this report has identified **at least 75 geopolitical cyber incidents that targeted Canada since 2010**. What specific forms did these activities take? What do we know about their origin? What types of entities were targeted? The present section aims to help answer such questions. The data presented below is based on the [Canadian](#)

[cyber incidents directory](#), an online, free-access database created by the Raoul Dandurand Chair in 2021.

What types of cyber incidents are most frequent?

One specific type of cyber incident remains largely predominant in Canada: cyber espionage, namely, the use of cyber capabilities to obtain confidential information without its holder's consent. This category entails the theft of state secrets and intellectual property, as well as the targeted surveillance of individuals, for instance. **Among the 75 geopolitical cyber incidents accounted for in this report, 49 are categorized as acts of cyber espionage.** The second most frequent type of incident is [information manipulation](#), namely, the intentional, massive and coordinated dissemination of false or biased information in cyberspace for hostile political purposes. We have identified 15 such incidents targeting Canada since 2010. These two most frequent categories are then followed by cyber reconnaissance operations, defacements, and acts of doxing¹.

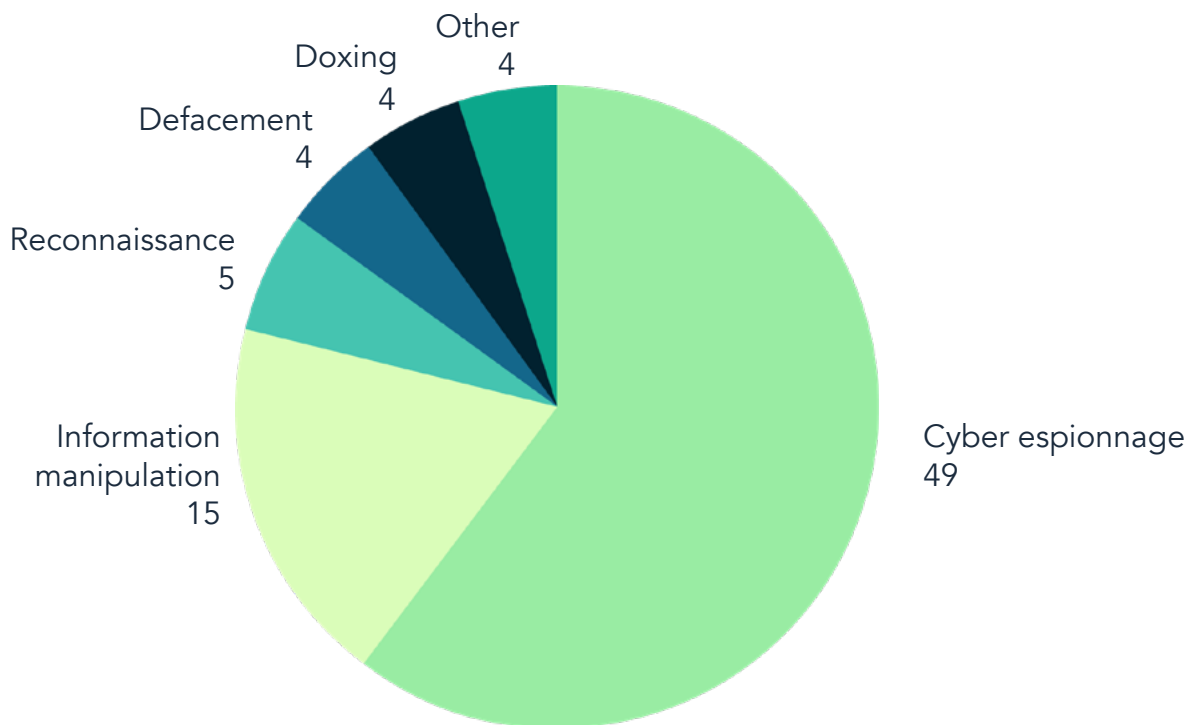
¹ Complete definitions of each type of cyber incident can be found in the "How this report was established" section, at the end of this document.



What do we mean by cyber incidents?

We define “cyber incidents” as intentional, malicious actions, limited in time and carried out at least in part in cyber space. The term cyber incident therefore includes cyber attacks, data theft, and online disinformation, among other things (for more details, see the “Typology” section below). This analysis focuses on geopolitical or strategic cyber incidents. In other words, the incidents analyzed here are not primarily related to criminal or domestic political activity, but rather to international rivalries and strategic competition; they originate most often outside Canada and are mostly orchestrated by foreign governments for military, political, economic, or other purposes. The incidents discussed here have affected Canada, including its public authorities, the general public, research institutions, and companies, individuals or international organizations based in Canada. Some targeted Canada specifically, while others were aimed at multiple countries including Canada. The incidents analyzed in this report date as far back as 2010.

MOST FREQUENT TYPES OF CYBER INCIDENTS



Source : Canadian cyber incidents directory (www.dandurand.uqam.ca/cyberincidents)



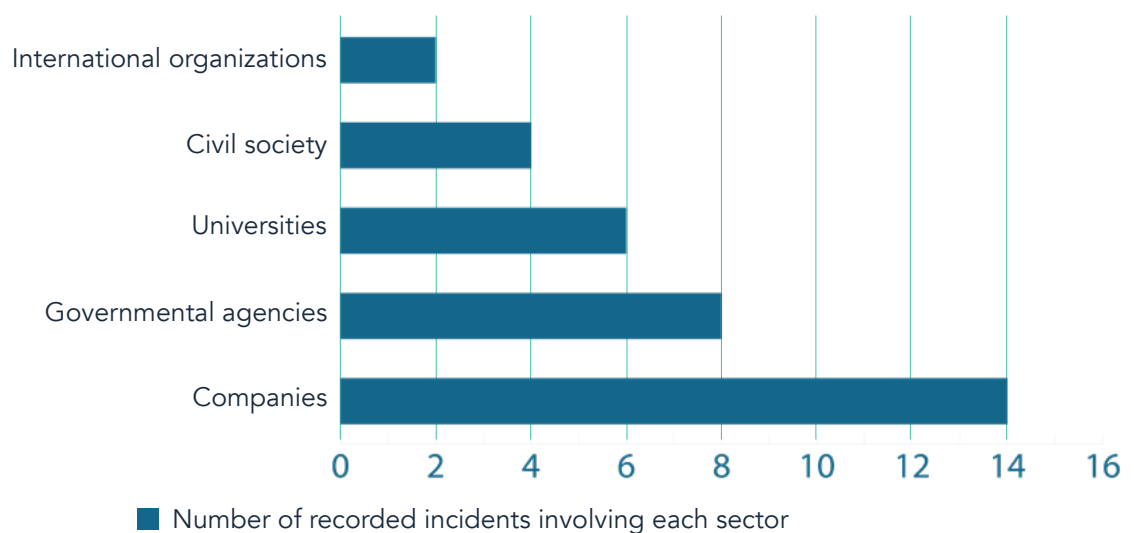
Cyber espionage: what do we know about targeted entities?

While the exact nature of cyber espionage campaigns is not always known, our analysis suggests that about half of the espionage operations we studied for this report were first and foremost economic or industrial espionage campaigns. These operations targeted major companies, universities, and other R&D-dedicated entities, most noticeably involved in the information technology, energy, finance and aerospace industries. Nearly another quarter of these incidents were rather acts of “conventional” espionage, targeting Canadian governmental agencies. In most cases, however, the nature of the impacted entities remains unknown.

How often is Canada impacted by cyber incidents?

Our data shows that on average, since 2017, **Canada experiences ten geopolitical cyber incidents each year**. The year 2020 marked a peak, with thirteen incidents, while 2021 proved rather calm, with eight incidents. It is important to note, however, that many cyber incidents are not identified or publicly disclosed until months after they occur. It is therefore to be expected that other events will soon be added to the 2021 total in the near future.

PUBLICLY RECORDED VICTIMS OF CYBER ESPIONAGE IN CANADA



Source : Canadian cyber incidents directory (www.dandurand.uqam.ca/cyberincidents)

Where do most of these incidents originate from?

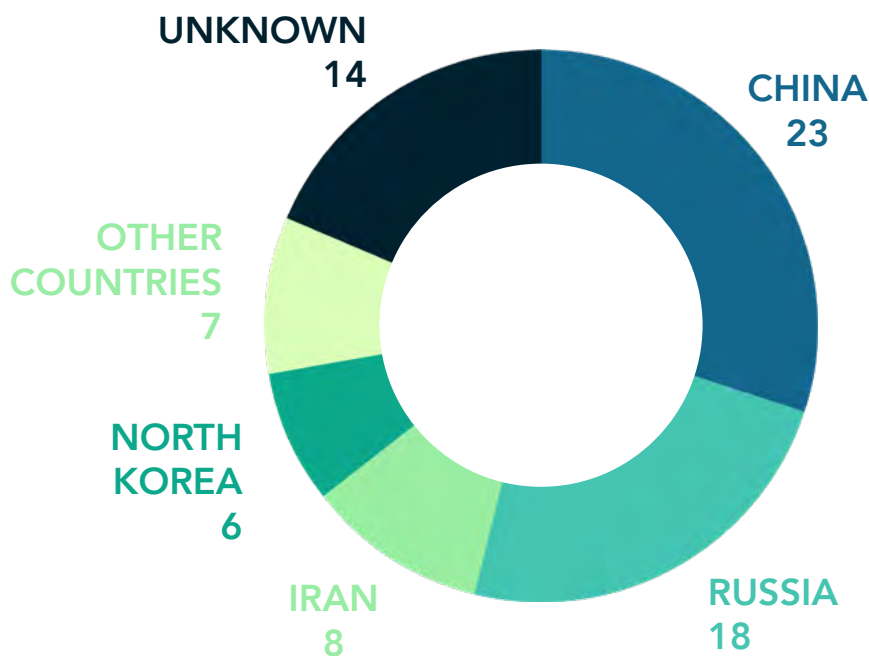
According to our data, **the vast majority of geopolitical cyber incidents recorded in Canada since 2010 can be traced back to just four countries** : China (23 of 75 incidents), Russia (18), Iran (8) and North Korea (6). It must be stressed, however, that these data relate to the geographic origin of cyber incidents that have affected Canada and do not necessarily imply responsibility of the governments of the countries mentioned. Some incidents, for instance, may have been operated by non-state actors located in these countries and acting on their own. Furthermore, establishing the

origin of an incident often requires significant time and resources. As a result, fourteen of the incidents recorded since 2010 have no known origin for the moment.

Which hacker groups proved especially active against Canada?

Although the attribution of a cyber incident is often a long and complex endeavour, several groups of state-sponsored hackers are well-known in the cybersecurity community. Specific intrusion methods, for instance, can be recognized and compared, providing precious clues on which incidents may be linked to which groups. These cumulated

GEOGRAPHICAL ORIGIN OF CYBER INCIDENTS (since 2010)



Source : Canadian cyber incidents directory (www.dandurand.uqam.ca/cyberincidents)

investigative efforts demonstrate that a handful of hacker groups can be held responsible for a significant number of cyber incidents targeting Canada in recent years: Cozy Bear (originating from Russia), Silent Librarian (Iran), APT 10 (China) and Lazarus Group (North Korea). Taken together, these groups are responsible for at least eleven incidents since 2017. For instance, Cozy Bear and Lazarus Group have taken part in the 2020 cyber espionage campaign targeting medical research on COVID-19 in Canada. Members of Silent Librarian have launched three consecutive campaigns of intellectual

property theft against universities, including several Canadian institutions. The chart below presents Canadian incidents that have been formally attributed to each of these actors².

² The classification of hacker groups is a complex and confusing endeavour for various reasons. First, each major cybersecurity company uses its own designation system, thus generating a variety of names representing the same actor. Furthermore, hacker groups may evolve and change in their composition from one campaign to another. It is thus difficult to decide whether to establish a distinction or an association between certain groups and incidents. Our chart presents actors whose composition seem to have remained stable throughout the designated campaigns. We present the most frequently-used designations.

COZY BEAR	SILENT LIBRARIAN	LAZARUS GROUP	APT 10
<ul style="list-style-type: none"> Espionage of Canadian medical research on COVID-19 (2020) Solar Winds incident (2020); approximately a hundred Canadian entities targeted Phishing campaign against companies and governmental agencies in various countries (2021) 	<ul style="list-style-type: none"> Espionage campaign against various universities (2013-2017) Espionage campaign against various universities (2019) Phishing campaign (2020); at least three Canadian universities targeted 	<ul style="list-style-type: none"> WannaCry ransomware attack (2017) Espionage campaign "Operation GhostSecret" (2018) Espionage of Canadian medical research on COVID-19 (2020) 	<ul style="list-style-type: none"> Hacking of Equifax (2017), data of 19000 Canadian customers compromised "Cloud Hopper" espionage campaign (2018)
			



THREE MAJOR TRENDS TO WATCH IN

Three major trends to watch in the near future

While cyber insecurity and digital threats are not a new phenomenon in Canada, the 2020-2021 period has contributed to the emergence or acceleration of specific dynamics in the cyber domain. This section aims to highlight three major trends that should command particular attention in the coming years, namely: the growing digital surveillance of activists living in Canada by foreign powers, the expansion of the cyber-mercenary industry, and the massive growth of ransomware attacks.

ACTIVISTS, & DISSENTERS, EXILES

THE EXPORTATION OF SURVEILLANCE

In recent years, the acquisition of new cyber capabilities by a growing number of states has significantly transformed the global landscape of intelligence collection. Cyberspace now provides nation-states with countless new avenues of espionage and surveillance everywhere in the world, without much risk of retaliation. The type of information now coveted by states not only includes traditional state secrets, but also intellectual property or personal information on foreign high-ranking decision makers, to name just a few. In recent

years, however, another trend has been of increasing concern: the digital surveillance of civil society actors, human rights activists, or members of oppressed minority groups.

Cyberspace now provides nation-states with countless new avenues of espionage and surveillance everywhere in the world, without much risk of retaliation.

While the development of information technology and cyberspace has for many years raised hopes for a global wave of democratization and was expected to unequivocally enhance freedom of speech, these same technologies are now also used by states (especially authoritarian ones) to harass political opponents, whistleblowers, and other dissenting voices. Sociopolitical struggles and oppressions in the real world now largely extend to



cyberspace, and it has become rather unclear whether information technology provides more means of emancipation than potential tools of repression. What is more, the global rise of digital authoritarianism now transcends borders and poses significant challenges to democratic countries such as Canada.

Oppressed in China, harassed overseas: the case of Uyghurs

Surveillance of activists and digital repression of minority groups has increased massively around the world over the past decade. This phenomenon is especially visible in China, where the Uyghur community is now subjected to relentless state surveillance and its members deprived of their basic human rights. In China itself, the Communist party has developed a state-of-the-art, Orwellian surveillance machine, with the help of China's Big Tech companies. Meanwhile, the Chinese regime also increasingly deploys an arsenal of espionage outside of its own territory: the Uyghur diaspora in different countries is increasingly targeted by cyberattacks and malicious activities aimed at collecting intelligence and harassing critics of the Communist party.

In September 2019, the cybersecurity company Volexity **identified eleven websites** dedicated to Uyghur-related issues that had been compromised for surveillance purposes. According to Volexity, these websites had

been fraudulently exploited since 2013 to spy and launch cyberattacks against the Uyghur community throughout the world. As these websites were blocked by China's "Great Firewall"¹, the company emphasized that the operation was most certainly not targeting Uyghurs on Chinese soil, but rather, members of the community living overseas.

In China itself, the Communist party has developed a state-of-the-art, Orwellian surveillance machine (...)

More recently, the cybersecurity companies Check Point and Kaspersky exposed **another Chinese hacking campaign** that targeted influential figures among the Uyghur community based in China and Pakistan. Hackers fraudulently emulated UN agencies and a human rights organization called Turkic Culture and Heritage Foundation. Using these false identities, they tricked their targets into downloading a purported vulnerability scanner², which actually allowed the deployment of a malware and gave them access to the victims' computers.

1 The Great Firewall of China describes a wide range of technology and systems deployed by the Chinese state to block and prevent access to various websites and social media platforms in China. Automated systems also track the use of keywords on the internet, in order to control the flows of information in the country and prevent outside influence.

2 A vulnerability scanner is a security software designed to search and detect vulnerabilities in an application or computer system.

Not the first, probably not the last

Such campaigns now represent an important tool in Beijing's repressive arsenal, at home and overseas. Uyghurs, however, are not the only group subjected to the Communist party's aggressive surveillance. Other communities, deemed problematic by the regime, are also targeted by cyber espionage campaigns or online harassment by China's security apparatus.

Uyghurs, however, are not the only group subjected to the Communist party's aggressive surveillance.

In Canada, members of **the Tibetan community** or organizations defending the cause of Tibet have been targeted by cyber operations. In 2013, University of Toronto's Citizen Lab exposed **an espionage campaign** orchestrated by the Chinese hacker group **APT 1** (Unit 61398 of the People's Liberation Army), that targeted several Canadian-Tibetan organizations.

Since 2010, practitioners of Falun Gong³ living in Canada have also reported **various acts** of online intimidation and disparagement, allegedly orchestrated by the Chinese

³ Falun Gong, or Falun Dafa, is a spiritual movement inspired by the Buddhist tradition. It has been banned in China since 1999. Its practitioners are persecuted by the Chinese Communist party, which considers the ideas promoted by Falun Gong as a challenge to its political hegemony.

state. For example, in 2015, 2018 and 2019, **insulting and threatening emails** were sent to several Canadian ministers or members of the Canadian Parliament. The perpetrators falsely claimed to be affiliated with Falun Gong. However, tracking the IP addresses of some of these emails showed that they originated in China. Some observers have therefore suggested that the whole scheme was an attempt by Chinese authorities to discredit Falun Gong practitioners in Canadian political circles.

A growing list of "surveillance-states"

China is not the only foreign power deploying surveillance campaigns against human rights activists in Canada. In 2018, the Citizen Lab revealed that **Omar Abdulaziz**, a Saudi dissident living in Quebec, had been targeted by a digital surveillance operation. His phone had been infected by the infamous **Pegasus** spyware, designed by the Israeli company NSO. The Citizen Lab attributed the incident to a cyber actor called KINGDOM, which was strongly suspected of being affiliated to Saudi security services.

More recently, in September 2020, **a report** published by the NGO Miaan Group exposed an espionage campaign which targeted several hundred individuals involved in the promotion of human rights in Iran. The victims included journalists, lawyers or student activists, most of them members of Iranian ethnic or religious minorities. They were



residing in about fifteen countries, including Canada. The cybersecurity company Check Point, which also investigated the campaign, **concluded** that the Iranian state was most certainly behind these activities.

The victims included journalists, lawyers or student activists, most of them members of Iranian ethnic or religious minorities.

Because these cyber incidents become more frequent, they obviously raise serious questions about the protection of human rights

and privacy on Canadian soil. There is also growing concern that Canada, home to many exiled NGOs and human rights activists, is becoming a new hunting ground for unscrupulous authoritarian foreign powers. As China now tries to export its model of digital authoritarianism to various developing countries, and expands its technological industry client list accordingly, there is little reason to think that this phenomenon will go away anytime soon.



A Canadian case: a phishing campaign targeting Uyghur activists (2021)

In March 2021, Facebook announced that it had taken measures against a group of hackers that used its platform to spy on Uyghur activists in various countries. The company declared that it had identified about 500 victims, mostly originating from the Chinese province of Xinjiang but living abroad, in countries such as Turkey, Kazakhstan, the United States, Syria, Australia and Canada. According to the report, about 20 of the targeted individuals were established in Canada.

Facebook attributed this campaign to a hacking group named Earth Empusa (also known as Evil Eye, or Poison Carp). This China-based group is largely suspected to be connected to security services of the People's Republic of China. Previous campaigns of cyber espionage against the Uyghur community publicized in 2019 and 2021 (see above) were also attributed to Earth Empusa.

According to Facebook, the hackers used various tactics to spy on their victims. They created fraudulent Facebook profiles impersonating journalists, students, human rights activists or members of the Uyghur community, in order to trump their targets' vigilance. The group also created websites purported to provide news about Uighur-related issues, as well as fake online shops and apps, which were all infected with a spyware named *Insomnia*.

This recent cyber espionage campaign appears to be an extension of the Chinese surveillance machine deployed in Xinjiang to prevent and suppress criticism within the Uyghur community, in the name of the fight against "terrorism" and "extremism". Since 2014, the "[Strike Hard Campaign against Violent Terrorism](#)", in particular, has generated a sharp rise in the development of malwares used in such surveillance campaigns.

However, as Canada is home to a Uyghur community of about 2000 people, espionage is not the only form of malicious activity experienced by this population. Many Uyghurs have reported frequent acts of harassment and intimidation on Canadian soil: anonymous phone calls involving death threats, among others. Some people also reported that local authorities in Xinjiang were persecuting their relatives living in China in order to pressure them to stop their activism in Canada.



HACKERS- FOR-HIRE

CANADA AND THE RISE OF CYBER-MERCENARIES

If Canada was already known to be a frequent target of cybercriminals or state-sponsored hackers, it is now increasingly destabilized by a new type of actor: private groups of hackers-for-hire, selling their cyber capabilities to anyone who can afford them. Sometimes formally organized as private companies or structured like clandestine organizations, these groups of **cyber-mercenaries** often possess high-end hacking abilities. Their customers may include, for instance, unscrupulous companies in search of commercial secrets or governments eager to boost their security apparatus capabilities.

Over the past few years, the phenomenon of cyber-mercenaries has grown from a small, niche industry to a flourishing transnational market, which now commercializes hacking

services comparable to those of well-resourced nation-state intelligence services. In fact, the latter proves to be an important recruiting ground for this industry. In 2019, Reuters journalists revealed the existence of a company named **DarkMatter**, which employed former NSA operatives to conduct cyber-espionage campaigns for the UAE government. More recently, the private security firm **Global Risk Advisors**, which employs former CIA agents, was accused of a vast hacking campaign mandated by the Qatari government.

Over the past few years, the phenomenon of cyber-mercenaries has grown from a small, niche industry to a flourishing transnational market (...)

Between proliferation and plausible deniability

The services offered by the cyber-mercenary industry is now wide-ranging and continuously diversifying: **training** of foreign security services, assistance in the creation of intrusion techniques, and in many cases, direct execution of highly sophisticated cyberoperations. Hackers-for-hire vary in their **organizational structure**. Some groups essentially work clandestinely, using cybercriminal networks to market informal, on-demand services. Other, more professionalized entities may be formally




registered as private companies working on a contractual basis.

This quiet outsourcing of cyber-warfare, which supplements the now well-known market of spyware technology (exemplified by the Israeli company [NSO Group](#)), poses major challenges of its own. By commoditizing intelligence agencies or military-grade cyber know-how, it contributes significantly to the global proliferation of advanced and offensive cyber capabilities. Such outsourcing also adds uncertainty to an already shadowy cyber-warfare global landscape: when acting as intermediaries for nation-states, these cyber-mercenaries help provide plausible deniability, further complicating the [problem of attribution](#). In other words, the rise of cyber-mercenaries is far from contributing to international stability in cyberspace.

Illaudable causes

These problems, however, are hardly the most controversial aspects of the cyber-mercenary industry. A growing number of observers, for instance, accuses hackers-for-hire to regularly work against their own country's best interest. For instance, former NSA operatives employed by DarkMatter were ordered to hack US citizens and even ended up intercepting emails exchanged between [Michelle Obama](#) and a member of Qatar's royal family. Other voices blame Global Risk Advisors' ex-CIA agents for spying on FIFA's officials on behalf





of Qatar, thus helping the Gulf monarchy win the 2022 soccer World Cup bid, for which the United States was also in the running.

A growing number of observers, for instance, accuses hackers-for-hire to regularly work against their own country's best interest.

More generally, frequent revelations surrounding the cyber-mercenary industry also demonstrate that its actors are **not always serving noble causes**, to say the least. Hackers-for-hire are often employed by authoritarian states to track political opponents, spy on NGOs and journalists or steal personal information destined to blackmail and harass dissenters. Although this industry strives to present itself as a benevolent purveyor of security for its clients, it is clear that, in the absence of appropriate regulation and oversight, it also represents a serious source of insecurity for many people around the world.

First documented cases in Canada

The cyber-mercenary phenomenon is now beginning to impact Canada as well. In June 2020, the company NortonLifeLock and the University of Toronto's Citizen Lab exposed a vast cyber-espionage campaign operated by a shadowy Indian hackers-for-hire organization, whose targets included several Canadian entities (see below). More recently, in November

2021, the cybersecurity company Trend Micro published **a report** documenting the activities of a Russian-speaking cyber-mercenary group called Void Balaur (or Rockethack). The report identified various hacking campaigns dating back to 2015, targeting institutions in at least 30 countries, including Canada.

Hackers-for-hire are often employed by authoritarian states to track political opponents, spy on NGOs and journalists or steal personal information destined to blackmail and harass dissenters.

Although the number and nature of Void Balaur's Canadian targets were not specified, Trend Micro indicated that the group's victims were very diverse: human rights activists, journalists, politicians, diplomats, and company executives from various sectors. The hackers' missions therefore consisted as much in monitoring political opponents as in spying on private companies. The identity of Void Balaur's patrons, as well as the group's location, however, remain unknown.

Proven target and potential hub

The impacts of the cyber-mercenary industry now extends to social media platforms: in late 2021, Meta announced that it had taken down **1500 fraudulent Facebook profiles**, which



where used by several hacking companies to trick their victims. These fake personas served to establish contact with targeted individuals and lure them into clicking on infected links, thus enabling the clandestine surveillance of their computer or smartphone. As Meta indicated, it had identified more than 50,000 victims in over a hundred countries, and it seems very likely that Canadian residents are among the total.

While Canada is thus a proven target of cyber-mercenaries, it may also soon become a territory in which such actors base their operations. In March 2017, at the request of the US Justice Department, a [Canadian citizen](#) was arrested in the Greater Toronto Area, after being hired by Russian intelligence services to

take part in a massive data breach targeting Yahoo. The 22-year-old man did not maintain any specific relations with Russian intelligence but had simply been [mandated for the occasion](#), after he advertised his hacking abilities on a cyber-criminal online platform. What seems to be a small first may well not be the last; as Canada is home to both a large IT workforce and to many cybersecurity companies, it presents a rather high potential for becoming a hub of the cyber-mercenary industry, with all the issues such a development may raise in the future.



A Canadian case: The “Mercenary.Amanda” hacking campaign (2020)

In June 2020, the cybersecurity company NortonLifeLock and the University of Toronto’s Citizen Lab simultaneously published reports concluding a coordinated investigation of several months. Both documents shed light on a major hacking campaign that took place between 2017 and 2020, orchestrated by a shadowy hackers-for-hire company based in India. This actor, nicknamed “Mercenary.Amanda” by NortonLifeLock (and “Dark Basin” by the Citizen Lab), was deemed to have targeted 220 organizations and more than 1800 email accounts in approximately fifteen countries, including Canada. A Reuters investigation, published at the same moment, estimated the grand total of compromised email accounts to [more than 10,000](#) since 2013.

The respective reports revealed that the hackers had successively performed political, industrial and financial espionage, targeting a wide variety of actors: politicians, journalists, environmental organizations, judges, government officials, hedge funds, law firms as well as political consulting companies, among others. In particular, the Citizen Lab has documented various malicious activities against environmental groups involved in the [#ExxonKnew](#) campaign, including Greenpeace and Public Citizen.

The University of Toronto’s researchers also indicated that they had identified with “high confidence” the specific organization behind this hacking campaign: BellTroX InfoTech Services, a hackers-for-hire company based in New Delhi and founded in 2013. Interestingly enough, BellTroX would be one of the companies [sanctioned by Meta](#) in 2021 for using fraudulent Facebook profiles to trick and hack its victims (see above).

Even though details on the Canadian organizations targeted by Mercenary.Amanda were scarce, the NortonLifeLock’s report still delivered interesting numbers: about 4% of attacked entities were Canadian, making Canada the fifth country most impacted by the campaign (more than half of the victims were based in the US). Globally, the most targeted sectors were the financial industry (32% of targeted entities), law firms (14%), non-profits (9%), consulting firms (8%), the manufacturing sector (6%) and media outlets (4%).

Meanwhile, the instigators of the BellTroX operations remain unknown. The Reuters investigation, quoting former employees, suggested that the company was often hired by politicians to spy on rival parties or opponents. Another ex-employee, later quoted in an article by the Indian newspaper The Economic Times, stated that BellTroX counted at least four or five [foreign clients](#) among its regulars. Involving a private company based abroad, itself probably mandated by mysterious actors based in yet another country, the Mercenary.Amanda case thus demonstrates with acuity the complex and multifaceted nature of the cyber-mercenary phenomenon.



RANSOMWARES

WHEN

CRIMINALITY

EDGES TOWARDS

GEOPOLITICS

At first glance, the ransomware issue appears to be primarily a cyber criminality issue with few national security or geopolitical ramifications. As the frequency and impact of ransomware attacks continue to grow each year, however, so do the limits of this perspective; ransomwares now generate more and more financial damage, may significantly disrupt global supply chains, and may even threaten the availability of essential human services. What is more, such attacks are often launched by hackers operating from foreign countries, where they are not always kept in check by local authorities. Managing the ransomware problem may thus entail diplomatic and international cooperation challenges.

(...) ransomwares now generate more and more financial damage, may significantly disrupt global supply chains, and may even threaten the availability of essential human services.

As their name suggests, ransomwares are a type of malware used by malicious actors for online extortion purposes. Cybercriminals fraudulently access the computer systems of companies or other institutions and deprive them of their own data by using an encryption mechanism. The hackers then demand a ransom in exchange for the decryption key, and thus for the return of the said data. Ransoms are often proportional to the financial capacity of the targeted entity, and an increasing number of criminals ask to be paid in crypto-currency, in order to minimize traceability.

Taken separately, ransomware attacks appear more as a nuisance than as an existential threat. However, by any relevant metrics, they have skyrocketed in recent years. According to [a study](#) published by the British cybersecurity company CybSafe, there has been a 900 % increase of ransomware attacks between the first half of 2020 and the same period in 2021. Ransoms themselves are also ballooning: from 5000 USD in 2018, the average ransom asked by hackers had jumped to **200,000 USD** in 2020. Last year, the US Department of the




Treasury estimated that in only the first half of 2021, at least **590 million USD** (in cryptocurrency) was extorted through the use of ransomwares.

The risk of systemic disruption: the Colonial Pipeline case

Few cases of ransomware attacks better illustrate their potential impact than the Colonial Pipeline incident. On May 7th, 2021, an employee of this major American pipeline operator receives a ransom demand on his computer. The amount, requested in cryptocurrency, is estimated to be around 5 million USD. The **Colonial Pipeline** Company, worried that the firm's servers may be infiltrated, decides to shut down its whole systems for the time being. The same goes for its pipeline, which normally carries 2.5 million barrels of crude oil along the US East coast every day.

As the company's systems would remain shut down until May 12th, some gas stations in the neighboring major cities start **running out of fuel**; not because the supply has actually stopped at this point, but because news regarding the hack has spread like wildfire and created a panic: customers rushed to their nearest gas station to buy unusually large quantities of gas and stockpile it, in case the situation persists. Although these fears might appear unfounded, the results are nonetheless very tangible: 43 % of gas stations in Georgia and South Carolina, as well as 65 % in North Carolina, eventually ran dry. The attack (which





meanwhile has been attributed to the Russian cybercriminal gang DarkSide) generated an 8 % increase in gas prices throughout the US.

Needless to say, such attacks may also have consequences for other countries as well. While Canada, for instance, only experienced a very **small increase** in gas prices in more eastern provinces due to the incident, the attack still raised fears that national supply may significantly **slow down** if it lasted any longer. Globally, such attacks may also disrupt international supply chains and stock markets in the future, and potentially influence investors behaviors, thus generating systemic aftershocks. Meanwhile, it now appears that the Colonial Pipeline incident was probably caused by **a single compromised password**.

When lives are at stake


Other ransomware attacks are even more worrying, as they directly endanger human lives. On May 13th and 14th, 2021, **two such incidents** targeted Ireland's Department of Health. At the height of the COVID-19 pandemic, the Health Service Executive (HSE), which manages online services for various hospitals and clinics, had its computer systems compromised by ransomware. A 20 million USD ransom was demanded in exchange for the decryption key.

Other ransomware attacks are even more worrying, as they directly endanger human lives.

The attack's consequences proved quite dramatic: many appointments were cancelled (up to 80 % in some areas), HSE employees were forced to rely on paper and pens for their work, as emails were temporarily unavailable, and the medical information of more than 500 patients were compromised. Once again, the comparison between the incident's impact and its origin revealed rather unsettling: an employee had simply clicked on an infected link from his workspace computer. The attack, which was later attributed to the Russia-based criminal group **Wizard Spider**, is hardly an isolated case, as **many other** ransomware attacks targeted health institutions throughout the world during the COVID-19 pandemic.

The geopolitics of ransomware

The HSE and Colonial Pipeline incidents are far from being the only major disruptions caused by foreign-based criminal groups. Studies published by cybersecurity companies such as **Chainalysis** or **Kaspersky** suggest that the vast majority of hacking groups deploying ransoms are based in Russia, and a smaller fraction in **Eastern European** countries, North Korea, **Iran** or China. Although it remains uncertain whether this state of affair is the result of deliberate state policies or rather reflects mere judicial ineffectiveness, there are many indications that these groups are hardly threatened by the local authorities in their respective countries.



(...) it remains uncertain whether this state of affair is the result of deliberate state policies or rather reflects mere judicial ineffectiveness (...)

Considering that states such as Russia, Iran, North Korea or China maintain a rather firm control on their national cyberspace, it is very plausible that ransomware groups are in most cases well-known by local authorities but left undisturbed so long as they only cause disturbance in rival countries. This implicit or explicit agreement is in many cases well understood by cybercriminals: cybersecurity researchers have shown, for instance, that the Russian-based ransomware group REvil used to program its malwares so as not to target computers **which language-settings were in Russian** (and other languages spoken in former soviet countries).

Nation-states also find many benefits in accommodating cybercriminals. Indeed, such groups regularly prove to be a precious **recruiting ground** for national intelligence services and also show readiness to occasionally pause their criminal activities to perform cyber espionage campaigns for their host country. While often subtle or informal, such instances of cooperation nevertheless show that it becomes more and more difficult to establish clear boundaries between cyber criminality and interstate competition in cyberspace.

Canada looking for solutions

One thing is certain, Canada is not done dealing with ransomware. According to a **recent report** published by the Communication Security Establishment (CSE), there has been at least 235 reported ransomware attacks against Canadian entities in 2021. The real total, however, is undoubtedly much higher. Although the CSE hasn't revealed the specific identity of targeted entities, it made clear that critical infrastructures were affected, including in the healthcare, manufacturing, and energy sectors.

Accordingly, Canadian authorities display growing efforts to try to anticipate and mitigate threats posed by ransomware attacks. In late 2021, the Canadian Center for Cybersecurity published its first "**ransomware playbook**" destined to help small and large organizations to better understand the problem and adjust to the ransomware threat. At the legislative level, the *Security Information Act* was also amended in 2019 in order to bolster Canada's cyber defence policy. And it now appears that the Canadian national security apparatus is willing and able to make use of its new prerogatives; in December 2021, the CSE announced for the first time that it had launched a **cyberattack** against foreign-based cybercriminals, thus demonstrating how ransoms are increasingly perceived and treated as a national security matter.

A Canadian case: the hacking of the Royal Military College in Kingston (2020)

Canada is not spared by the proliferation of ransomware attacks. In July 2020, for instance, the Royal Military College in Kingston (RMC) was the target of such [an incident](#), which temporarily paralyzed the institution's activities. The email and intranet systems used by the College's employees and students, among others, were affected and intentionally shut down in order to prevent further compromise. The damages were apparently significant enough to prevent the College's systems to be fully available when teaching activities resumed [at the end of August](#).

At first, the Department of National Defence (which administers the RMC) stated that the incident was the result of a "mass phishing campaign"¹ that did not lead to the compromise of classified information. The ministry added that the data most likely to have been compromised were academic research papers, destined to be published anyway. A month after the incident, however, it was established that [financial information and personal data](#) had actually been compromised and published on the Dark Web. This heavily suggested that a ransomware, rather than a mere phishing attempt, was actually at play. Among the leaked documents were some cadet progress reports and acceptance letters, which contained information including their names and addresses.

The publication of such information by hackers is generally intended to personalize and give more credibility to a ransom demand, as well as to put more public pressure on the victim, thus maximizing the chances of payment. In addition to these tactical considerations, however, some observers stressed that in the case of the Military College such data presented [sensitive implications](#). For example, an adversarial state could use this leaked information to know which individuals may climb the ladder of Canada's defence apparatus in the near future, and accumulate personal information on them.

According to several observers, the hacking of RMC Kingston was attributable to a cybercriminal group called [DoppelPaymer](#) that didn't seem to be connected to a nation-state actor. Stolen data, however, were published on the Dark Web and it is impossible to determine who may have accessed them or how they could be used in the future (potentially in conjunction with other information gleaned from other sources). The case of RMC Kingston therefore demonstrates the critical ambiguity associated with ransomware attacks; although they might be first and foremost criminal acts based on financial motives, they may also inconspicuously entail geopolitical issues.

¹ "Phishing", or spear phishing, is an intrusion method used by hackers to deceitfully access a target's computer. It often consists in sending a fraudulent email which contains an infected URL link, that the receiver is invited to open. Clicking on the link may then give the hackers undue access or the opportunity to upload a malware on the victim's device.



CONCLUSION: the Ukrainian factor

The present report aimed at providing a general assessment of geopolitical cyber incidents in Canada, as well as highlighting several major trends in the domain to watch for in the near future. As such, the conflict recently initiated in Ukraine generates significant upheavals and may not remain without consequence for Canada. As the Canadian government has joined various multinational diplomatic, economical and military efforts in order to support Ukraine and sanction Russia, cyberspace represents an important channel through which the Russian state or other actors may try to retaliate for these actions.

Fears of such retribution are already displayed; in March 2022, a ransomware attack targeting the [Alouette aluminum smelter](#) in Sept-Îles (QC), launched by the Russian cybercriminal group Conti, quickly raised suspicion in the media – especially as Conti is one of several hacker gangs [proclaiming its support](#) for the Russian state in its war against Ukraine. There are, however, several pieces of evidence suggesting that the attack was not related to the war in Ukraine, most notably the fact that the first breach occurred several days before the Russian invasion. Although the Alouette hacking was likely not ideological or geopolitical in nature, the coming months may nevertheless bring more ambiguous incidents. The challenge for Canadian authorities and organizations will then be to clearly identify what should be perceived as geopolitically-oriented incidents, and respond accordingly.

Although Canada does not appear as a primary target for the time being, multiple scenarios may occur. At a minimum, Russia could indeed encourage its cybercriminal networks to bolster their attacks – especially ransomware attacks – against Canadian entities, especially [those who took specific actions](#) against Russia (boycotts, for instance). Despite present efforts by NATO states to prevent any escalation, it is also conceivable that Russia might eventually try to target Western critical infrastructure. As Canadian electrical infrastructures are very much interconnected with the US electrical grid, Canada may for instance be targeted to inflict damage on American systems.

As stated by many Western observers, the war in Ukraine [does not seem](#) to have brought about major, destructive cyberattacks so far. Nevertheless, we should keep in mind that the stealthy, clandestine nature of cyber capabilities make them a potentially precious tool in the rather indirect interstate rivalries surrounding the conflict, to which Canada is not immune. The potential for disruption thus supplements the other trends highlighted in this report, and should not be minimized, much less ignored.

How this report was established

The data and cases presented in this report are taken directly from the Canadian cyber incidents directory produced by the Center on Multidimensional Conflicts (Observatoire des conflits multidimensionnels or OCM) of the Raoul Dandurand Chair. The directory is an online database launched in March 2021 and freely accessible to the public. It is accessible at:

www.dandurand.uqam.ca/cyberincidents

The purpose of the Canadian cyber incidents directory is to identify and classify geopolitical cyber incidents that have affected various actors and targets in Canada, including the general public, public authorities, businesses, civil society, and infrastructure, as well as entities based in Canada. It is intended as a reference source to be updated regularly but which does not claim to be exhaustive. It currently catalogues incidents dating back to 2010. Is an incident missing? You can let us know at chaire.strat@uqam.ca.

WHAT THIS REPORT DOES AND DOES NOT COVER

In keeping with the mission of the Raoul Dandurand Chair, this report lists cyber incidents with geopolitical or strategic implications for Canada. In other words, the incidents essentially relate to international rivalries and strategic competition. They most often originate from outside Canada and are mainly orchestrated by foreign governments for military, political, economic, or other purposes.

This report **does not address cyber incidents that are strictly domestic and/or strictly criminal in nature** (even if such activities originate from abroad). Because this distinction can sometimes be difficult to make, we have chosen an inclusive approach whereby the directory may include ambiguous cases. Readers are encouraged to consult the online directory for more information on the nuances or cautions regarding such cases.

Typology and definitions of incidents

The Canadian cyber incidents directory, on which this report is based, identifies eight categories of geopolitical cyber incidents. This typology focuses more on the strategic nature of incidents (their goals) than their technical aspects (or *modus operandi*). It is loosely inspired by the [Cyber Operations Tracker](#) produced by the Council on Foreign Relations, an American think tank, and on other sources listed below. The following are specific definitions for each type of incident

CYBER ESPIONNAGE: The act of obtaining information through digital means without the information holder's prior consent. This category includes the theft of state secrets, theft of intellectual property, and covert surveillance of individuals.

RECONNAISSANCE: The act of fraudulently entering a computer system in order to map it or assess its defenses or vulnerabilities, in anticipation of future actions.

INFORMATION MANIPULATION: The intentional, massive and coordinated dissemination of false or biased news in cyberspace for hostile political purposes (or what [Jeangène Vilmer et al., 2018](#), call "manipulation of information").

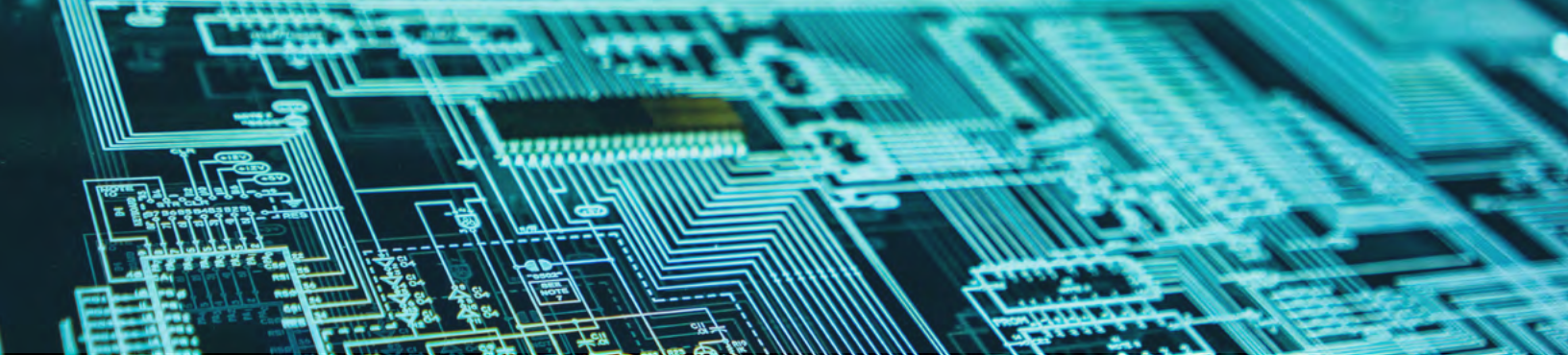
DEFACEMENT: The act of impersonating, taking over or altering the appearance of a website, account, or page in an unauthorized manner for hostile political purposes.

DOXING: "The intentional public release onto the Internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual" ([Douglas, 2016](#)). We extend this definition to organizations ("organizational doxing"). This category includes activities such as "hack and leak" operations.

DATA DEPRIVATION: The act of permanently destroying or temporarily depriving a user or an organization of their data. This category includes the use of ransomware.

DENIAL OF SERVICE: "Any attack intended to compromise the availability of networks and systems (...) resulting in performance degradation or interruption of service" ([Verizon, 2019](#)). This includes distributed denial of service (DDoS) cyber attacks.

CYBER SABOTAGE: The act of using a virus or malicious software to cause physical damage to a computer, machine, or infrastructure. Cyber sabotage can also be used to interrupt the operation of a computer-controlled system for an extended period.



DATES AND ORIGIN OF INCIDENTS

The information in this report is based on open sources, and the details of many cyber incidents, or the manner in which certain conclusions were drawn by the actors involved in the process, are often unknown or confidential.

The date we assign to a cyber incident may refer to when the incident actually took place or when it was publicized. We prefer the first approach, but the exact starting date of an incident often cannot be determined. This is particularly true of waves of cyber espionage, which are stealthy by nature, and disinformation campaigns extending over long periods of time. In such cases, we use as our reference point the date when the incident was identified or publicized.

In terms of origin, we distinguish between the (geographic) source of an incident and the (political) responsibility for it. We give pre-eminence to geographic data in this report because they are technically easier to establish and because it is quite rare that responsibility for a cyber incident is publicly attributed. In both cases, the origins cited in the report are based on the public findings of the organizations that investigated a given incident, such as reports from cyber security firms, press releases from national security agencies, and the like. Readers are encouraged to browse our [online directory](#) for more details on the origin of each incident.

ON WHAT SOURCES ARE THE INVENTORY AND REPORT BASED?

Data in the Canadian cyber incidents directory, on which this report is based, are taken from the following types of sources: content produced by professional media in accordance with the principles set out in the Munich Charter; studies and reports from government, academic, or private institutions (cyber security companies, think tanks, NGOs, etc.); press releases from Canadian and foreign government official bodies; and scientific publications and other databases subject to peer review. Such sources are, as much as possible, cross-checked. In addition to hyperlinks provided in this report, readers are invited to visit our [online directory](#) to directly access the sources for each case.

Raoul Dandurand Chair
of Strategic and Diplomatic Studies

Université du Québec à Montréal

dandurand.uqam.ca



Review:
Yvana Michelant-Pauthex
Louis Collerette

Graphism:
Françoise Conea

With the support of:

