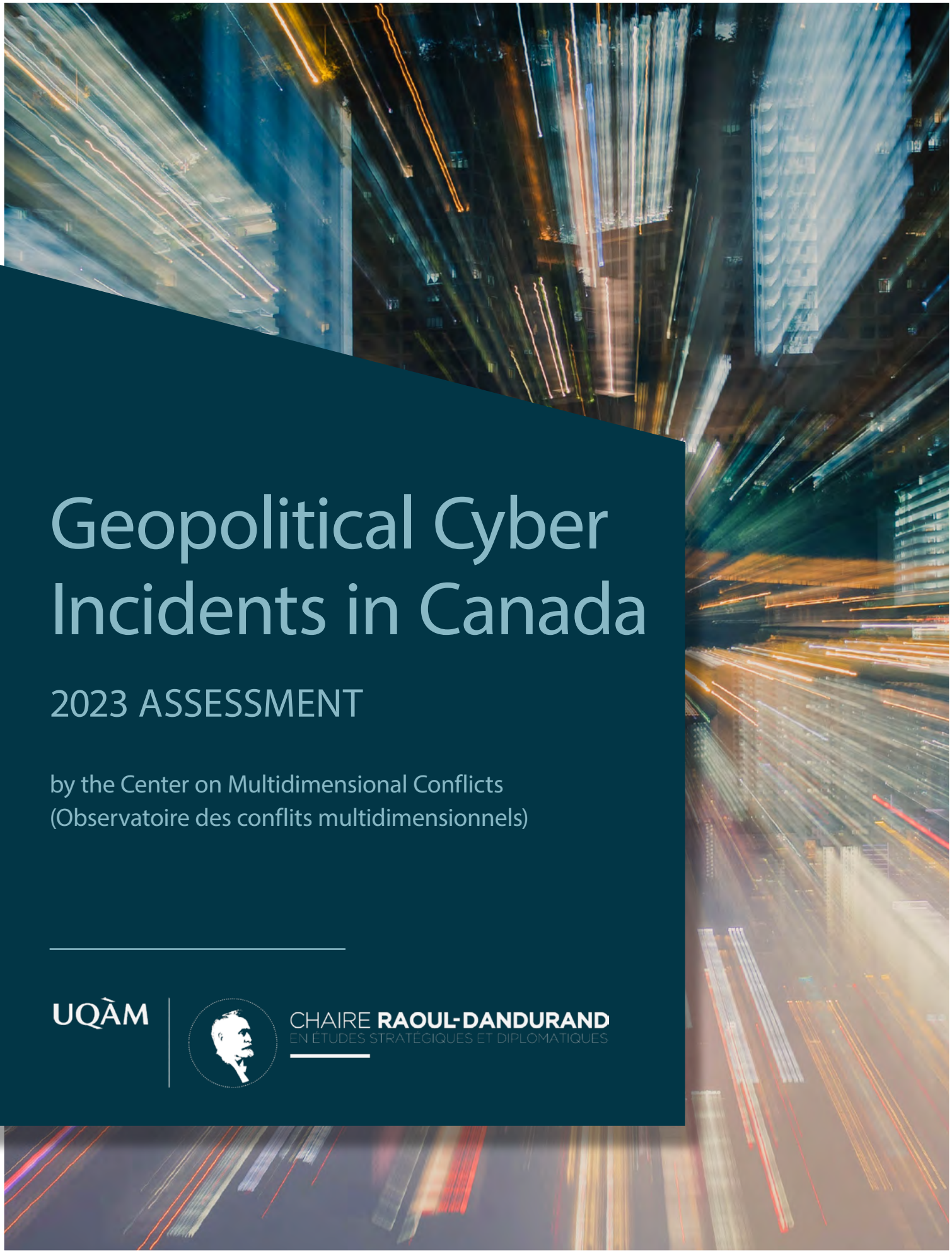


Geopolitical Cyber Incidents in Canada

2023 ASSESSMENT

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

UQÀM

CHAIRE RAOUL-DANDURAND
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

Table of contents

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 Frédérick Gagnon, a political science professor at Université du Québec à Montréal (UQAM) and holder of the Raoul Dandurand Chair. The center brings together Canadian and international scholars studying novel strategies which foreign actors, particularly nation-states, deploy internationally to destabilize states, weaken their societies and institutions, or undermine their critical systems and infrastructure. Cyber attacks, disinformation, political and electoral interference, and geo-economics are among the phenomena studied 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

Frédérick Gagnon holds the Raoul Dandurand Chair, is Director of the Center on Multidimensional Conflicts (OCM), and a political science professor at Université du Québec à Montréal (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 the geo-economic competition between China and the U.S. on Canada–U.S. relations.

Alexis Rapin is research fellow at the OCM. He studies the transformation of warfare, such as cyber strategy and disinformation, as well as the impacts of new technologies on international security. He has contributed to numerous scholarly and non-scholarly publications in French and English. In early 2023, he testified in Ottawa before the House of Commons Standing Committee on National Defence, on issues related to Canada's cyber defence.

Danny Gagné is a Ph.D. candidate in political science at UQAM and a research fellow at the OCM. His research focuses on the use of drone warfare in the United States. His recent work at the OCM has been the subject of numerous "Chroniques des nouvelles conflictualités" (published by the Raoul Dandurand Chair), noticeably discussing the strategic use of disinformation.

Fanny Tan is research fellow at the OCM and a student in political science at UQAM. She holds a bachelor's degree in digital media (UQAM) and a certificate in video game design (UQAT). As a freelance journalist, Fanny Tan regularly writes in the Canadian media about social issues surrounding new technologies. She is a tech contributor on the radio show *Moteur de recherche* (ICI Première) and a member of the privacy advocacy organization Lab 2038.

EIGHT SIGNIFICANT INCIDENTS

2022

JANUARY

CYBER INCIDENT AT GLOBAL AFFAIRS CANADA

Global Affairs Canada is hit by a cyber attack, which anonymous government sources believe originated from Russia. Some of the department's online services are rendered temporarily unavailable due to mitigation measures. While Russia has been massing troops on its border with Ukraine in recent months, the incident occurred while the Minister of Foreign Affairs Mélanie Joly was visiting Kiev.

APRIL

IRANIAN HACKERS TARGET ENERGY COMPANIES

Meta announces that it has cracked down on an Iranian-based group that has been conducting hacking attacks against various companies in a dozen countries. The group's targets include at least one Canadian energy company. One of the malwares deployed made possible to access and exfiltrate files, or take screenshots without the victims' knowledge.

MAY

RANSOMWARE ATTACK AGAINST CMC ELECTRONICS

CMC Electronics, a Canadian aerospace company active in the defense sector, is hit by a ransomware attack. The hack is claimed by the Russian-speaking cybercriminal group ALPHV. CMC is among the companies selected to participate in the modernization of the Canadian Armed Forces' CH-146 Griffon helicopter fleet.

JUNE

INFLUENCE OPERATION AGAINST APPIA RARE EARTHS

The cybersecurity firm Mandiant exposes an information operation that targeted three major mining companies, including Canada-based Appia Rare Earths & Uranium Corp. According to Mandiant, this disinformation campaign was orchestrated by the China-based group DRAGONBRIDGE and was intended to disseminate narratives aligned with the interests of the People's Republic of China.

JULY

ESPIONAGE OF ENERGY COMPANIES BY LAZARUS GROUP

The cybersecurity firm Talos (Cisco) reveals that the North Korean hacker group Lazarus conducted a major cyberespionage campaign between February and July 2022 against Canadian, American and Japanese energy companies. According to Talos, the campaign was focused on the theft of intellectual property.

SEPTEMBER

IRGC-MANDATED EXTORTION CAMPAIGN

In a joint statement, American, Canadian, Australian and British cybersecurity agencies attribute a cyber extortion campaign to Iran's Islamic Revolutionary Guard Corps (IRGC). The Iranian hackers have allegedly sought to conduct ransomware attacks against various organizations in the four countries they targeted.

OCTOBER

CYBER INCIDENT AT THE CANADIAN PARLIAMENT

The Toronto Star reveals that a cyber incident of unspecified origin has struck the Canadian Parliament. Members of Parliament were asked to change their email passwords and some of the Parliamen's online services were interrupted. No details are provided about the actors responsible for the incident.

DECEMBER

AMNESTY CANADA HACKED BY CHINESE GROUP

Amnesty Canada announces that it has been the target of a sophisticated hack, which forced the NGO to take its systems offline for nearly three weeks. According to the cybersecurity firm Secureworks, this cyber attack can be attributed to a hacker group affiliated with the Chinese state. The hackers seemingly tried to obtain information about the organization's contacts and projects.

Canada and geopolitical cyber incidents: a data snapshot

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 most often come from 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. Some of the data included in this report date back to 2010.

Marked by various geopolitical earthquakes, such as the all-out invasion of Ukraine, the intensification of the Sino-American geo-economic rivalry, or the rise of a massive protest movement in Iran, 2022 saw many of these upheavals spill over into the global digital space, including in Canada. Cyberespionage operations, ransomware attacks and online influence campaigns have haunted the Canadian public debate on multiple occasions in 2022. In fact, probably more so than any previous year. While the last edition of this report concluded that there had been an average of 10 geopolitical cyber incidents in Canada per year since 2017, the current analysis found no less than 14 such incidents in 2022. In total, the Raoul Dandurand Chair's directory of Canadian cyber incidents, from which the data in this report is derived, now lists 97 geopolitical cyber incidents that have affected Canada since 2010.

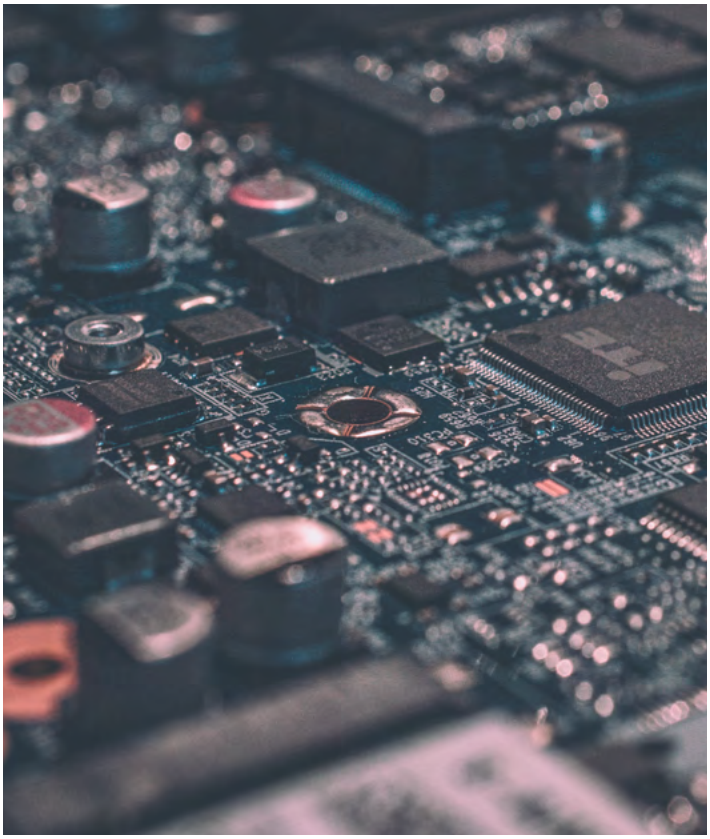
What major conclusions can we draw from the cyber incidents observed in 2022? Of course, it must be reiterated that geopolitical incidents in cyberspace are a complex object of study: identifying attackers, their motives and the consequences of their actions is often a lengthy process, and the results are not always indisputable. Based solely on open sources, this report is the result of a monitoring and compilation process, designed to serve as a barometer of cyber (in)security in Canada. This section highlights some of the key data for 2022 and illustrates how this year may or may not have differed from previous years, with regards to the types of incidents recorded, sectors most targeted, or countries and hacker groups most frequently involved in cyber incidents in Canada.

What are the known targets?

The private sector represented half of the victims, and was the most frequent focus of geopolitical cyber incidents in 2022. Canadian companies operating in strategic sectors, such as energy, mining, or the aerospace industry, proved to be prime targets. In July 2022, the North Korean hacker group Lazarus infiltrated the systems of Canadian energy companies (whose names have not been disclosed), with the aim of stealing intellectual property. China, which has been particularly active on the strategic minerals market in recent years, has also taken an interest in the Canadian mining sector and orchestrated an influence campaign targeting Appia

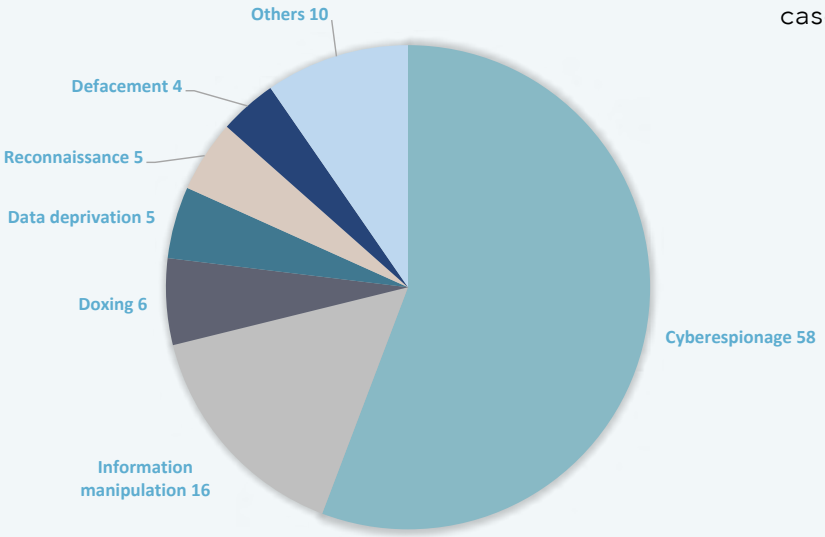
Rare Earths & Uranium Corp. in June 2022. Canada's favorable position in various critical sectors seems to be attracting the attention of foreign powers.

The Canadian public sector also suffered its share of cyber incidents in 2022, perhaps more so than in previous years. In March, the National Research Council Canada was the victim of an undisclosed cyber incident. A cyber attack targeted Global Affairs Canada in January, while another cyber incident affected the Canadian Parliament in October. In April, reports of a Russian-led disinformation campaign targeting the Canadian Armed Forces emerged in the context of the conflict in Ukraine. As for the allegations of Chinese interference in the 2021 federal election, it is important to note that the investigation is ongoing and that the information made public so far does not allow to conclude that these acts included a major cyber component per se.



What are the most common types of cyber incidents?

Recorded cyber incidents by type (since 2010)



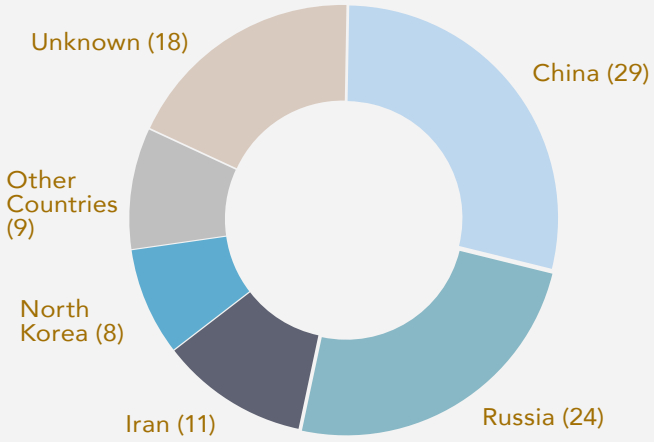
* Some cases may combine several types of incidents simultaneously
Source: Canadian Cyber Incidents Directory

Between 2010 and 2022, the most frequent type of geopolitical cyber incident in Canada remains cyberespionage, which accounts for approximately 60% of our recorded cases. Data for 2022 prove rather consistent with this trend, as cyberespionage represented 40% of recorded cases[1]. Other types of incidents registered last year also included two cases of data deprivation (in this case, ransomware attacks), two instances of threats of data leakage (doxing), and two cases of information manipulation (see chart). And, although the cause has not yet been made public, an intrusion into the computer systems of the National Research Council of Canada is believed to have taken place in March 2022; this organization is a prime target for cyber spies wishing to Canadian scientific research activities.

[1] 4 out of 10 cases where there is a clear pattern.

Where do most of these incidents originate from?

Geographical origin of cyber incidents (since 2010)



Our data indicate that the vast majority of geopolitical cyber incidents recorded in Canada since 2010 can be traced back to just four countries: China (29 out of 97 incidents), Russia (24), Iran (11) and North Korea (8). These data refer to the geographic origin of the cyber incidents that affected Canada and do not necessarily imply the responsibility of the governments of the countries mentioned (for more details, see the methodology section). The distribution of incidents reported in 2022 is consistent with this overall picture, although the ranking somewhat differs: Russia led the way in 2022, with 5 cyber incidents, while China and Iran are both considered responsible for 3 incidents. One case has been attributed to North Korea. One can observe a modest uptick with regards to Iranian activities against Canada: while 8 Canadian cyber incidents were attributed to Iran during the entire 2011-2021 period, the Islamic Republic cumulated three in 2022 only.

Source: Canadian Cyber Incidents Directory

Which hacker groups targeted Canada in 2022?

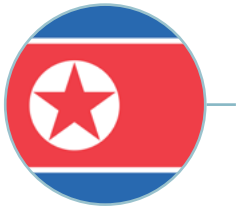
Several geopolitical cyber incidents recorded in 2022 were attributed to hacker groups already well known in Canada, such as Lazarus (a North Korean group active since at least 2009) or the Russian-speaking cybercriminal group Lockbit (likely founded in 2019). Other groups, however, seem to have targeted Canada for the first time last year. This includes DRAGONBRIDGE, a Chinese actor conducting online influence campaigns in various countries since 2019, who is believed to have orchestrated a recent information manipulation campaign against the Canadian mining company Appia Rare Earths. The Russian state-sponsored hacker group Sandworm, active since the late-2000s and already well known internationally, is also believed to have conducted its first operation in Canada in March 2022.

State-sponsored hacker groups most active against Canada

Based on attribution efforts by cybersecurity firms or governments, it can be observed that a small number of state-sponsored hacker groups are responsible for a significant portion of cyber incidents affecting Canada. The infographic below presents these different actors, their presumed affiliation, as well as the Canadian incidents that have been formally attributed to them since 2010.

SILENT LIBRARIANS

Alledge affiliation: Mabna Institute (Iranian government contractor)
Operations in Canada: Phishing campaign (2020), Espionage campaign against universities (2019), Espionage campaign against universities (2018)



LAZARUS GROUP

Alledge affiliation: Reconnaissance General Bureau (Korean People's Army)
Operations in Canada: Espionage of energy companies (2022), "AppleJeus" cryptocurrency theft campaign (2021), Espionage of COVID-19 research (2020), GhostSecret espionage campaign (2018), WannaCry ransomware attack (2017)

APT 1

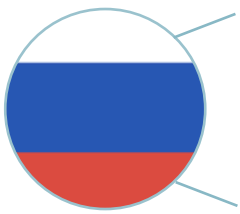
Alledge affiliation: Unit 61398 of China's People's Liberation Army
Operations in Canada: Operation OceanSalt (2018), Surtr campaign (2013), Hacking of the Immigration and Refugee Board of Canada (2011)

APT 10

Alledge affiliation: China's Ministry of State Security (Tianjin State Security Bureau)
Operations in Canada: Operation Cloud Hopper (2018), Equifax breach (2017)

HAFNIUM

Alledge affiliation: China's Ministry of State Security (Hainan State Security Department)
Operations in Canada: Microsoft Exchange vulnerability exploit (2021), Leviathan campaign (2019)



COZY BEAR

Alledge affiliation: Russia's Foreign Intelligence Service (SVR)
Operations in Canada: Chishing campaign (2021), SolarWinds hack (2020), Espionage of COVID-19 research (2020)

FANCY BEAR

Alledge affiliation: Russia's GRU Unit 26165 (military intelligence)
Operations in Canada: Espionage of COVID-19 research (2020), Hacking of the World Anti-Doping Agency (2019)

SEVERAL FEARS CONFIRMED: A 2022 RETROSPECTIVE

In the previous edition of this report, published in the spring of 2022, we presented three major trends to watch closely in the coming year: the increasing cyberespionage of members of Canadian civil society by foreign powers, the growing use of cyber mercenaries, and the rise of ransomware cyber attacks in Canada and their potential geopolitical impacts. One year later, it turns out that several cyber incidents in 2022 have confirmed these previsions and the perils they entail. As these trends are likely to persist into 2023 and beyond, it seems important to underline how they continue to materialize and affect Canadian society.

Activists, exiles and NGOs: prime targets

Activities of cyberespionage and electronic surveillance by foreign powers against members of civil society have been periodically observed in Canada since at least 2013, but are unfortunately becoming more frequent. At least two cyber incidents of this type were observed in 2022.

First, in November 2022, the Canadian Security Intelligence Service (CSIS) announced that it had opened an investigation into various threats against Iranian activists based in Canada. According to CSIS, the Iranian regime is seeking to monitor and intimidate members of the diaspora who have been involved in the protest movement shaking the Islamic Republic since September 2022. In its statement, CSIS said that the tactics and tools used for this purpose include cyberespionage. Meanwhile, a CBC investigation revealed that Iranian activists in the Toronto area have received intimidating anonymous calls on private numbers. Some of these threats referred to posts they had shared on private social media accounts, suggesting the use of electronic surveillance.

Second, in December 2022, Amnesty International Canada announced that it had been the target of a sophisticated hack, detected a few weeks earlier. According to the cybersecurity firm Secureworks, hired by the NGO, this cyber attack was carried out by a group of hackers affiliated with the Chinese state. They seemed to be trying to obtain confidential information on the organization's contacts and projects, and allegedly managed to access some work files. The Canadian branch of Amnesty is one of several organizations that have publicly denounced China's harassment of human rights activists in Canada for several years. It was later revealed that the breach had forced the NGO to take

certain systems offline for nearly three weeks, significantly affecting its operations and fundraising efforts.

As demonstrated by numerous investigations and publications, cyber incidents against civil society organizations are clearly not a phenomenon limited to Canada. However, there are a number of factors that make Canada a major target of such activities. As an important host country guaranteeing freedom of expression, Canada is home to large diaspora or exile communities, whose states of origin (such as China, Iran or Saudi Arabia) fear their ability to criticize, mobilize and protest from abroad. As Canada is very active in the diplomatic arena to promote human rights worldwide, it is also seen as an important symbol of the liberal international order that various illiberal states wish to erode. Such factors are important to consider in order to better understand the root causes of cyber campaigns against Canadian civil society.

“As an important host country guaranteeing freedom of expression, Canada is home to large diaspora or exile communities, whose states of origin (such as China, Iran or Saudi Arabia) fear their ability to criticize, mobilize and protest from abroad.”

The rise of cyber mercenaries

The rise of the cyber mercenary industry, a transnational gray market providing hacking services to anyone who can afford them, was a second trend to watch among those listed in our previous annual assessment. While malicious actions by cyber mercenaries against Canadian entities have been observed since at least 2020, two additional cases of this type occurred more recently (see also box below). In February 2023, for instance, a consortium of investigative journalists revealed the existence of a mysterious Israeli firm, nicknamed Team Jorge, which markets hacking and influence operations services. Among various clandestine capabilities, the company is believed to maintain a network of 30,000 fake profiles on various social media, used for the coordinated inauthentic dissemination of false or biased narratives.

Investigations surrounding Team Jorge also revealed that the company, although primarily hired to sway electoral campaigns in Africa and Latin America, has also conducted online disinformation operations to influence trade disputes in nearly 20 countries, including Canada. However, it is not known at this time which issue(s) of interest in Canada the firm was responsible for influencing, let alone on behalf of which actor. For this reason, and by virtue of our methodology, the case is not yet included in our directory.

Ransomware: when crime meets geopolitics

Finally, a third important trend discussed in our 2022 assessment was the spectacular proliferation of ransomware cyber attacks, and the potential geopolitical implications of these activities. We then pointed out that, while generally criminal in nature and motivated by greed, ransomware attacks can also have strategic ramifications and play a role in international rivalries. Several cyber incidents recorded in 2022 highlighted this phenomenon (see also box below).

In May 2022, for instance, two Canadian defense firms (based in Montreal) were victims of ransomware attacks: Top Aces, a company that provides training services for fighter pilots (including for the Royal Canadian Air Force), and CMC Electronics, an aerospace company involved in a helicopter modernization program for the Canadian Armed Forces. In both cases, observers pointed out that the compromised data could contain information of high strategic value. It was therefore conceivable that the cybercriminals, in addition to their extortion operations, could attempt to sell the data to foreign powers. In fact, the Canadian Department of National Defence subsequently announced that it was undertaking an in-depth analysis of the possible impacts of the attack on CMC Electronics.

These two cases illustrate the synergies that may exist in some countries between cybercriminals and state actors, with the former frequently suspected of providing occasional services to the latter in order to "buy" their impunity. While many of the gangs conducting ransomware attacks are based in Russia, much research suggests that a system of collusion – informal at the very least – exists between Russian intelligence and cybercriminal groups. While both Top Aces and CMC Electronics have been targeted by Russian-speaking criminal groups, it is impossible to conclude with certainty that the compromised data was not quietly offered to foreign powers.

> **"While generally criminal in nature and motivated by greed, ransomware attacks can also have strategic ramifications and play a role in international rivalries."**

A Canadian case: an Iranian-sponsored extortion campaign (September 2022)

In September 2022, several cybersecurity agencies from the United States, Canada, Australia and the United Kingdom issued a joint statement declaring they had identified a major cyber intrusion campaign that targeted organizations in the four aforementioned countries. Noticeably, the statement said that the hackers exploited the Fortinet, Microsoft Exchange and Log4j vulnerabilities in order to conduct a cyber extortion campaign, that included the use of ransomware.

At first glance, this campaign looked like many other criminal operations that had been observed throughout 2022. However, Canada and its three allies had good reasons to publish a joint statement in this case: after extensive analysis, the agencies involved had concluded that this cyber extortion campaign was orchestrated by the Iranian government. More specifically, there were clear indications that the Islamic Revolutionary Guard Corps (IRGC), a paramilitary organization serving the Iranian regime, was behind the campaign. Nevertheless, the IRGC had deployed serious efforts to cover its tracks: according to the Western agencies, the execution of this campaign had been subcontracted to two Iranian technology companies, Najee Technology Hooshmand Fater LLC and Afkar System Yazd Company.

Still, the purpose of the operation itself remains a mystery. According to the press release, the hackers attempted to both encrypt their targets' data (in order to demand a ransom) and to exfiltrate it (probably for intelligence gathering purposes) when it seemed to present a strategic value. The number and nature of the targeted entities, in Canada and elsewhere, have not been specified.

The terms of the arrangement between the IRGC and these two mysterious companies can only be guessed at. It is conceivable, for instance, that the IRGC was seeking to spy on Western organizations holding strategic information, and decided to use private actors to maintain plausible deniability and avoid drawing the attention of Western intelligence services. The two companies, for their part, likely were motivated by the promise of significant financial gains (through the extorted money) and by the perspective of winning the good graces of the Iranian regime. The whole operation's degree of success, on the intelligence as much as on the financial side, however, remains unknown.

In any case, this cyber-extortion campaign illustrates two of the trends discussed earlier in this report. On the one hand, it demonstrates how some states (and particularly Iran) are now exploiting the rise of ransomware attacks to camouflage their foreign intelligence gathering activities. On the other hand, it reveals how private cyber-mercenary entities can contribute to such subterfuge, making it more difficult to identify the true sponsors of cyber attacks and their motives. These are two troubling trends that Canada will likely have to pay good attention to in the near future.

Ukraine, war and cyber: is Canada dodging the digital bullets?

This was one of the major fears expressed in the early months of the all-out invasion of Ukraine: that Western countries that support Ukraine diplomatically or militarily, such as Canada, would become the targets of "punitive" cyber attacks orchestrated or encouraged by Russia. The use of ransomware, denial of service attacks or hack and leak operations against Canadian organizations, among others, were then considered very likely. After more than a year of conflict, have these fears materialized in Canada? Partly, at least. In April 2023, for instance, several denial of service attacks carried out by pro-Russian hacktivist groups targeted some twenty websites belonging to various Canadian public or private organizations. Among these were the sites of the Prime Minister, the Senate and the Canadian Association of Defence and Security Industries. While such cyber attacks are spectacular but remain rather inconsequential, the cases below demonstrate that other, stealthier and more elaborate cyber incidents related to the conflict in Ukraine have also affected Canada throughout 2022.

A mostly indirect target

In March 2022, for instance, the cybersecurity firm Trend Micro revealed that the hacker group Sandworm (affiliated with Russian military intelligence services, the GRU) had infected more than 150 routers and servers in Canada and several other countries, with a sophisticated malware. While the attack made it possible to remotely control these devices, Trend Micro concluded that the Canadian entities operating them were not Sandworm's primary targets, as they presented little strategic interest. The operation was more likely aimed at quietly establishing control over these infrastructures, with the intent of using them as vectors for a future, larger-scale attack – potentially against Ukrainian systems. Indeed, Sandworm is known as one of the most active Russian groups in Ukraine: its members are credited with the 2015 and 2016 cyber sabotage of the Ukrainian power grid, as well as the NotPetya ransomware attack in 2017. Therefore, Canada was probably more of an intermediate target in this case.

It is also on the information battlefield that the conflict in Ukraine has quietly affected Canada. In April 2022, the Communications Security Establishment (CSE) announced that it had observed several Russian disinformation operations, some of which targeting Canadian interests. According to CSE, coordinated efforts by various Russian agents of influence resulted in the online dissemination of false content claiming, for example, that Canadian soldiers were deployed in Donbas, and that some of them were responsible for instances of war crimes[1]. These fraudulent publications were supplemented by doctored images that purportedly showed Canadian soldiers deployed on the frontline. Some were disseminated through deceptive websites that sought to visually mimic those of established Western media. Again, Canada was a rather indirect target in this operation: while the content was not aimed at the Canadian public in order to influence domestic views, it was clearly intended to damage Canada's image abroad.

Government agencies among the victims?

In addition to these two relatively well-documented cyber incidents, two other (and more ambiguous) cases suggest that Canada has been targeted for its role in the conflict in Ukraine: the hacking of Global Affairs Canada in late January 2022 (see box below) and a cyber incident of unspecified origin that affected the Canadian Parliament later in October. While neither has been officially attributed to a foreign actor so far, Russia is among the potential suspects in both instances.

"Canada was a rather indirect target in this operation: while the content was not aimed at the Canadian public in order to influence domestic views, it was clearly intended to damage Canada's image abroad."

Indeed, in June 2022, a report published by Microsoft revealed that 128 organizations in 42 countries had been targeted by Russian cyberespionage operations in the wake of the Ukrainian conflict. While Canada was among the countries listed by Microsoft, it remains unclear which Canadian entity or entities were targeted, and whether Global Affairs was one of them. The October 2022 cyber incident that affected Canada's Parliament remains shrouded in even deeper mystery, as very few details have been disclosed by Canadian authorities thus far. However, it is worth noting that at the time of the incident, the House of Commons was reviewing various reports on Canadian Forces vehicle inventories that could potentially be delivered to Ukraine.

Risks may yet increase

All things considered; however, the fact remains that in comparative terms, Canada has been far from a top target of Russian cyber activity to date. According to another Microsoft report published in March 2023, the

1 Similar false rumors had already been disseminated by Russian state-actors several times in the past, including in 2017 and 2018.

United States, Poland, the United Kingdom and the Baltic States have been the ones most targeted by cyberespionage operations attributed to Russia since February 2022. In another report, published at the beginning of 2023 by the CyberPeace Institute, Canada ranked only 14th in the list of countries most affected by Russian cyber attacks surrounding the Russo-Ukrainian conflict. In other terms, although Canada has not been entirely spared by malicious cyber activities stemming from the conflict in Ukraine, it is nonetheless far from being the most affected Western country. Yet, as the conflict hardly seems to come to an end, at least three factors could contribute to change this state of affairs in the short or medium term:

- First, large or highly publicized military equipment deliveries could attract the attention of pro-Russian cyber actors and motivate one-off cyber actions. This is demonstrated, for example, by the denial of service attacks that targeted Germany in January 2023, following the announcement of Leopard 2 tanks deliveries. It should also be noted that the denial of service attacks that targeted Canadian sites in April 2023 followed the announcement of a new Canadian shipment of munitions to Ukraine. Such incidents, although likely, are nonetheless not very elaborate and usually cause limited damage.

- Second, as the conflict risks edging towards a stalemate, foreign military assistance is seen by a growing number of experts as Ukraine's main vulnerability. As such, Russia deploys growing informational efforts to try to erode Western public support for Ukraine. Canada's position in the top-10 military aid donors list thus makes it a prime target for Russian influence campaigns. While Russian information operations have recently sought to exacerbate fears surrounding the arrival of Ukrainian refugees in various European countries, it is conceivable that such campaigns may eventually be aimed at influencing the Canadian public.

- Finally, various indicators suggest that technological sanctions imposed on Russia are beginning to take their toll on some of its industries. As this pressure increases, Moscow may decide to amplify its industrial cyberespionage efforts, in order to acquire the knowledge that could increase its technological self-reliance. The aerospace sector, for instance, is one in which Russia is currently experiencing great difficulty, and in which Canada's advanced expertise could be of interest to Russian cyber spies.

A Canadian case: the cyber incident at Global Affairs Canada (January 2022)

On January 24, 2022, a troubling story surfaces in the Canadian news cycle: Global Affairs Canada has been the victim of a cyber incident, described by anonymous government sources as "a cyber attack." Reportedly spotted on January 19, the incident leads to the temporary closure of some of the department's online services, to allow the Canadian government to undertake remediating measures. Meanwhile, some news outlets also report that Canadian embassies abroad are experiencing problems with their electronic communications. Anonymous sources reveal that Russia is strongly suspected of being behind the incident.

To be sure, the context of this attack is geopolitically charged to say the least: as the Russian government has massed more than 100,000 troops near the borders of Ukraine over the course of 2021, Western diplomats are busy trying to reason with (and dissuade) Moscow. Canada is among the states heavily involved in these efforts. Mélanie Joly, the Canadian Minister of Foreign Affairs, is in fact visiting Kiev precisely when the cyber incident occurs. Of course, no one yet knows that Russia is just one month away from launching an all-out offensive against Ukraine.

On February 15, new elements emerge in the media. It is revealed, among other things, that some of the ministry's online services are still not restored, and that the Communications Security Establishment (the federal intelligence agency in charge of cybersecurity matters) is assisting Global Affairs in its remediation efforts. No further comment is made with regards to the source of the cyber attack. Meanwhile, on February 8, the international press reveals that the British Foreign Office also suffered a similar cyber incident a few weeks earlier. Yet, as war suddenly erupts on Europe's doorstep a few days later, the Global Affairs cyber incident logically fades from the news cycle.

In June 2022, however, a Microsoft report brings about some interesting news; the US tech company alleges that, in previous months, Russian intelligence-affiliated hackers have been observed conducting cyberespionage operations in 42 countries, including Canada (and almost all other NATO member-states). Nearly half of the targeted entities have been government agencies, with the goal, according to Microsoft, of "obtaining information from inside the governments that are playing critical roles in the West's response to the war." In February 2023, another report published by the French cybersecurity firm Sekoia.IO concludes that the hacker group APT29 (or Fancy Bear), affiliated with Russia's Foreign Intelligence Service (SVR), has been specifically tasked with spying on Western diplomatic circles throughout 2022. Noticeably, Fancy Bear is said to have conducted "long-term and covert operations in embassies networks."

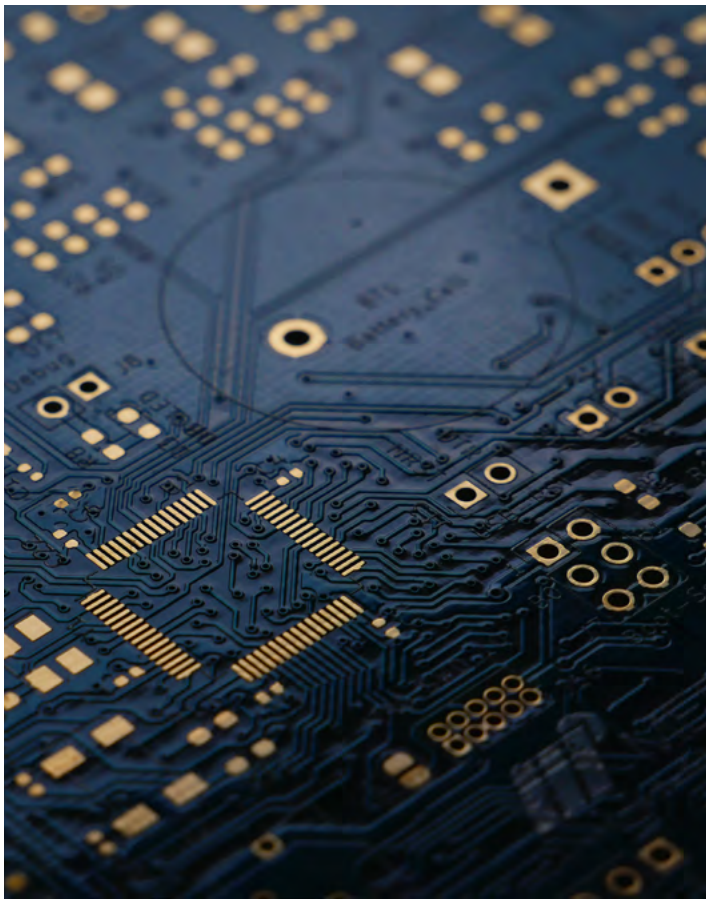
Was the cyber attack on Global Affairs part of this massive Russian cyberespionage campaign? Although various elements cited above suggest this hypothesis is highly likely, it has not yet been officially confirmed. Without further details (or official attribution) from the Canadian government to date, it is also unclear whether the attack was successful and, if so, what information was compromised in the process. Incidentally, it is worth noting that, as the June 2022 Microsoft report did not reveal the number of Canadian entities targeted, it must be assumed that some other strategic Canadian organizations may have been targeted by Russia in the context of the Ukrainian conflict.

Critical minerals and semiconductors: navigating a new geopolitical minefield?

The COVID-19 pandemic has undoubtedly affected Canadian strategic thinking in several ways. Noticeably, serious concerns have emerged in Ottawa in light of how the virus has disrupted global supply chains in two sectors critical to Canada's future: critical minerals/rare earths and semiconductors. It comes as no surprise that Prime Minister Justin Trudeau and President Joe Biden made this issue a focal point of their meeting in Ottawa in March 2023, where they mutually agreed to repatriate some of this global industry to North America.

By all accounts, the strategic importance of critical minerals and semiconductors could surpass that of oil in the decades to come. Essential to the manufacture of military equipment such as communications and missile guidance systems, they are also one of the keys to the transition to renewable energy promised by Ottawa, Washington and their allies. Supplies of lithium, cobalt, copper, dysprosium, neodymium and lanthanum are crucial for the development of electric cars batteries and engines, solar panels and wind turbines. The same is true for semiconductors: these chips and microchips are found in many items that allow Canadians to reduce their environmental footprint, such as electric vehicles, computers and other energy-efficient appliances.

However, Canada, the United States and their allies are heavily dependent on China and East Asia in these sectors. China is the world's largest producer of rare earths, holding 36 per cent of known reserves and controlling 70 per cent of the world's mining capacity and 90 per cent of its processing capacity. In his book *Chip War: The Fight for the World's Most Critical Technology*, Professor Chris Miller also points out that China aspires to be a leader in semiconductor



production (it currently accounts for 15 per cent of global production). More importantly, it is investing heavily in research and development to increase its production of the most sophisticated chips and microchips, 90 percent of which are currently sourced from Taiwan, a neighboring island that Beijing considers its own and whose sovereignty it does not recognize.

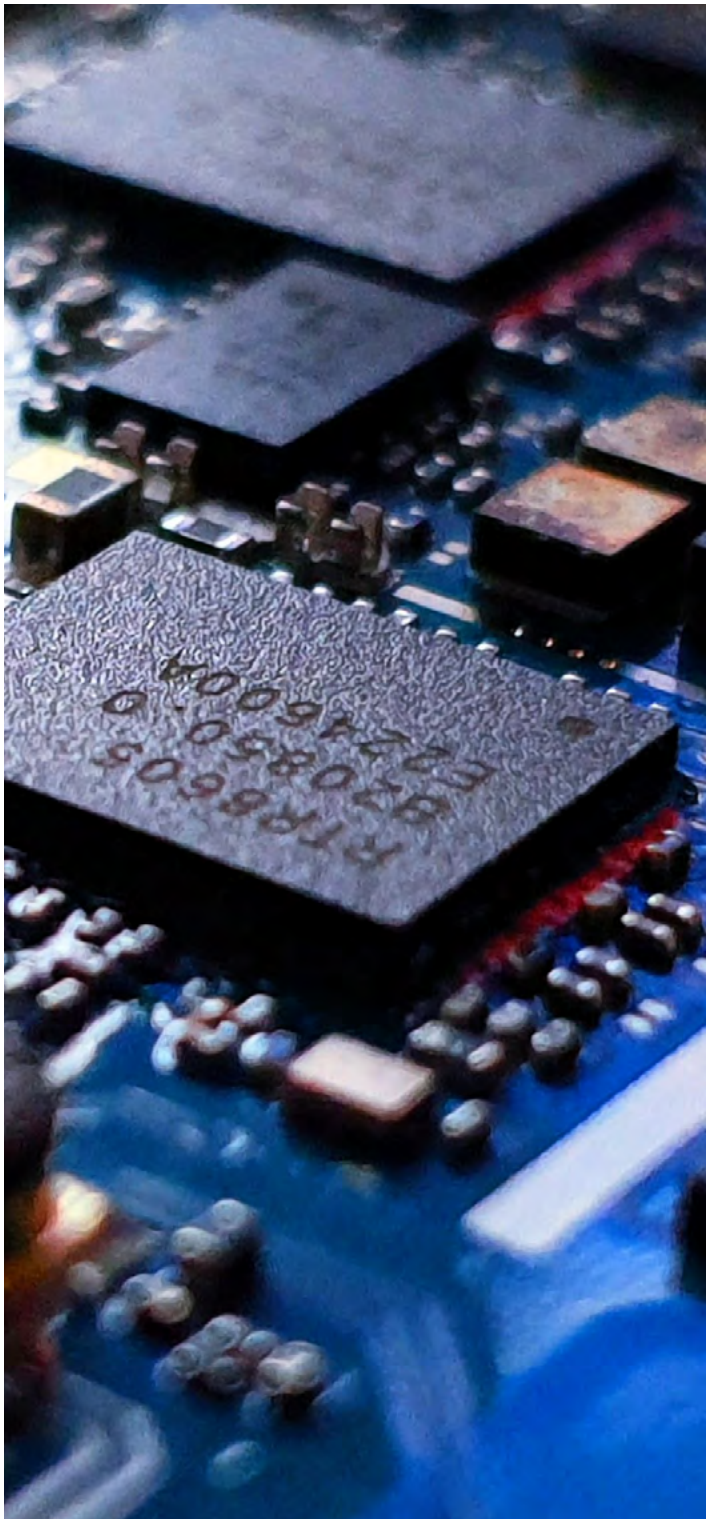
Continued threats of Chinese military action against Taiwan provide further incentive for Canada and the United States to try to reduce their dependence on semiconductors from that region. During their meeting in Ottawa in March 2023, Trudeau and Biden reiterated the importance of preserving stability in

the Taiwan Strait, but also of increasing government investment to accelerate the production and assembly of critical semiconductors in North America.

Ottawa and Washington are also increasingly using sanctions and economic barriers to curb Chinese advances in these sectors. In November 2022, for instance, Ottawa ordered three Chinese firms to divest their holdings in Canadian companies active in the critical minerals sector for national security reasons. A month earlier, Washington had announced a series of measures to isolate Chinese semiconductor production from the rest of the world, including a ban on U.S. companies selling highly sophisticated chips and microchips to China, to prevent theft of intellectual property and reverse engineering.

> **"Continued threats of Chinese military action against Taiwan provide further incentive for Canada and the United States to try to reduce their dependence on semiconductors from that region."**

These developments could well make critical minerals/rare earths and semiconductors a new epicenter of Ottawa-Beijing rivalries, and prompt China to target Canada to damage its international reputation, cripple its businesses or slow the repatriation of critical production lines on North American soil. Our directory of geopolitical cyber incidents targeting Canada already shows that China is using a variety of means, including cyberespionage, to prevail in the geo-economic competition affecting sectors that are critical to Canada. However, the cases studied in 2022 illustrate that Beijing may also be increasingly tempted to use disinformation campaigns to undermine the credibility of Canadian companies involved in the Chinese-Canadian rivalry in the critical minerals/rare earths and semiconductor sectors. The 2022 Chinese influence operation targeting Toronto-based Appia Rare Earths & Uranium Corp. is a case in point.



A Canadian case: Appia Rare Earths in Beijing's crosshairs (June 2022)

In June 2022, the Canadian mining company Appia Rare Earths & Uranium Corp. announced the discovery of a new rare earth deposit in the Athabasca Basin in northern Saskatchewan. According to U.S. cybersecurity firm Mandiant, Appia Rare Earth soon became the target of a Chinese malicious actor dubbed DRAGONBRIDGE, which ran an information manipulation campaign to discredit the company, which Beijing sees as a strategic competitor. The group reportedly created thousands of fake accounts on social media, websites and online discussion forums to promote narratives aligned with Chinese government interests and critical of Appia Rare Earths & Uranium Corp.

Among the Facebook and Twitter posts attributed to DRAGONBRIDGE, several comments aimed at highlighting the potentially harmful effects of Appia Rare Earths' projects on the environment and on workers' health. Throughout its campaign, DRAGONBRIDGE also targeted other rare earth mining companies in North America, including Lynas Rare Earths and USA Rare Earth, both of which had announced new projects in the United States in 2022. Again, social media posts were inauthentically disseminated to undermine the companies' reputation, claiming for instance that pollution caused by rare earth mining seriously threatened the health of local communities.

As Joe Biden and Justin Trudeau have promised to support such companies to increase production of critical minerals/rare earths and semiconductors in Canada and the U.S., campaigns like the one led by DRAGONBRIDGE may turn into a trend in the years to come. When Biden and Trudeau met in Ottawa in March 2023, they reiterated that the U.S. will be using the Defense Production Act to provide US$250 million to boost Canadian and U.S. critical minerals mining and processing projects. Meanwhile, Canada has promised to invest $1.5 billion in this sector in the years to come. Ottawa and Washington also want to create a North American semiconductor production corridor, starting with an investment by Canada and IBM to expand the testing and packaging capabilities of IBM's Bromont, Quebec facility. The Quebec government also has its own strategy to help repatriate critical supply chains to North America, as outlined in the "Québec Plan for the Development of Critical and Strategic Minerals 2020-2025."

China certainly pays good attention to these developments, which directly conflict with its desire to cement its position as an undisputed leader in these strategic areas. As this report demonstrates, China is already the primary source of geopolitical incidents targeting Canada. By aligning its industrial and manufacturing policies, as well as its Indo-Pacific Strategy, with those of the United States, Canada is strengthening ties with its traditional ally. But at the same time, it is placing itself in the crosshairs of an ever-growing Chinese power that does not hesitate to use various digital and geo-economic tactics (economic espionage, intellectual property theft, cyber attacks, etc.) to undermine its competitors.

Conclusion

AI and the future of cyber operations

In late February 2023, a YouTube video depicting Justin Trudeau seemingly being interviewed by U.S. podcast host Joe Rogan appeared on the web and was viewed several hundred thousand times in less than a week. Although the video was designed for comical purposes by an entertainment company, the deepfake's overall quality seems to have fooled a number of Internet users. Anecdotal at first glance, this episode may well provide us with an early taste of the role that artificial intelligence (AI) technologies may, in a not-so-distant future, play in disinformation campaigns and other malicious cyber activities.

Indeed, to various observers such as the think tank Eurasia Group, the growing capabilities and accessibility of AI technologies increase the chance of them being used as "weapons of mass disruption" in the service of state-sponsored agents of influence. Generative AI tools can now create false images and audio recordings that appear credible even to experts. Armies of bots, already deployed at low cost on social networks, can now be augmented by AI technologies to further influence online public discussions, intensify partisan polarization, or artificially boost support for political causes and candidates. AI-generated text can also be used to create compelling media contents and publications that seems to come from legitimate news sources.

The increasing accessibility of AI technologies may not only serve as a force multiplier for states already skilled in influence operations but could also stimulate the deployment of such campaigns by new actors who previously lacked the resources and expertise to do so. Canada, which does not seem to have been among Russian disinformation primary targets so far in the context of the Ukrainian conflict, may for instance witness an AI-powered uptick of such activities in the near future. Canada could also become the victim of new state actors who already had geopolitical motives but so far lacked means and opportunities.

AI could also play a growing role in transnational repression activities, such as those observed against activists based in Canada. Iran and China, two countries already using various AI-powered tools for surveillance purposes within their borders, could export such tactics to target dissenters and exiles more aggressively throughout the world, including in Canada. As discussed previously in this report, in late 2022, Canadian security agencies warned members of the Iranian diaspora about attempts by the Iranian regime to track and harass activists on Canadian soil. It is conceivable that in the future authoritarian states may use AI-enhanced facial recognition technologies to identify people participating in demonstrations in Canada, from pictures and videos posted on social networks for instance.

In addition to their usage for disinformation and digital repression purposes, AI tools are also being increasingly used to facilitate cyber attacks. As an example, cybercriminals can now automatically generate code to be used in ransomware schemes, while AI-generated voices can be used to fraudulently access portals secured by voice recognition systems. A recent study published in the journal Applied Artificial Intelligence further shows that individuals are particularly vulnerable to AI-enabled phishing attempts.

In mid-March 2023, the research firm OpenAI released the latest version of its famous large language model, ChatGPT-4. Despite the precautions taken by its developers, it took only a few days for observers to appreciate its various ethical flaws. Hence, there is little doubt that cybersecurity professionals will have to adapt quickly and demonstrate sizable agility to protect IT systems from increasingly sophisticated attacks. Otherwise, 2023 may well usher in the first major Canadian geopolitical cyber incidents enabled by artificial intelligence.

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, distinguishes 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 other sources listed below. Here are specific definitions for each type of incident:

CYBER ESPIONAGE: 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

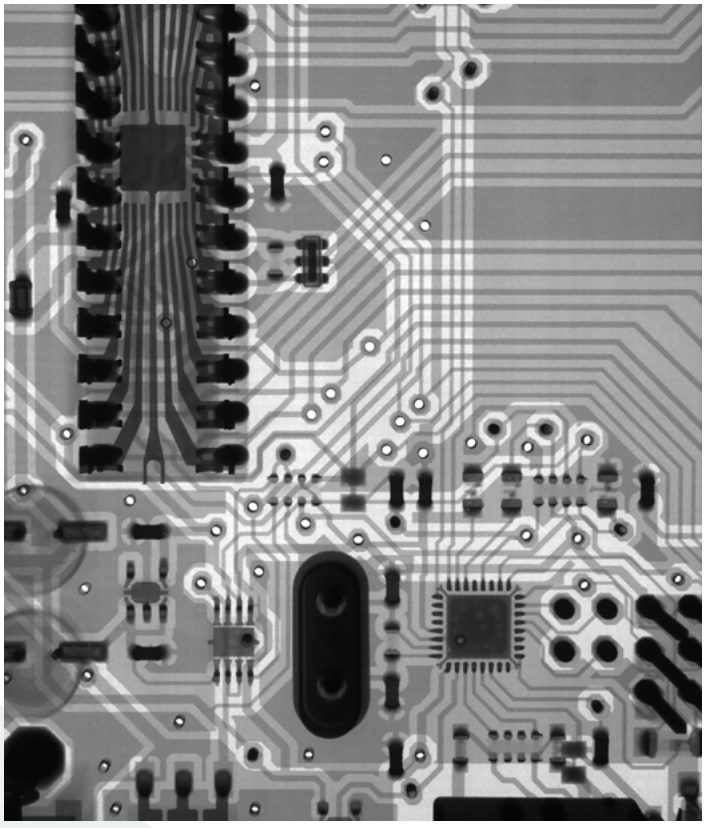
The information in this report is based on open sources, and the details of many cyber incidents, or the manner in which certain conclusions were reached by the actors involved, are often unknown or confidential.

The date we assign to a cyber incident may refer to when the incident actually took place or when it was publicized. The first approach is preferred, 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, as well as disinformation campaigns which may extend over long periods. In such cases, we use the date when the incident was identified or publicized as our reference point.

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 public attribution of cyber incidents to specific actors is less frequent. 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 directory 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 of each case.



Raoul-Dandurand Chair
in 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:

BANQUE NATIONALE