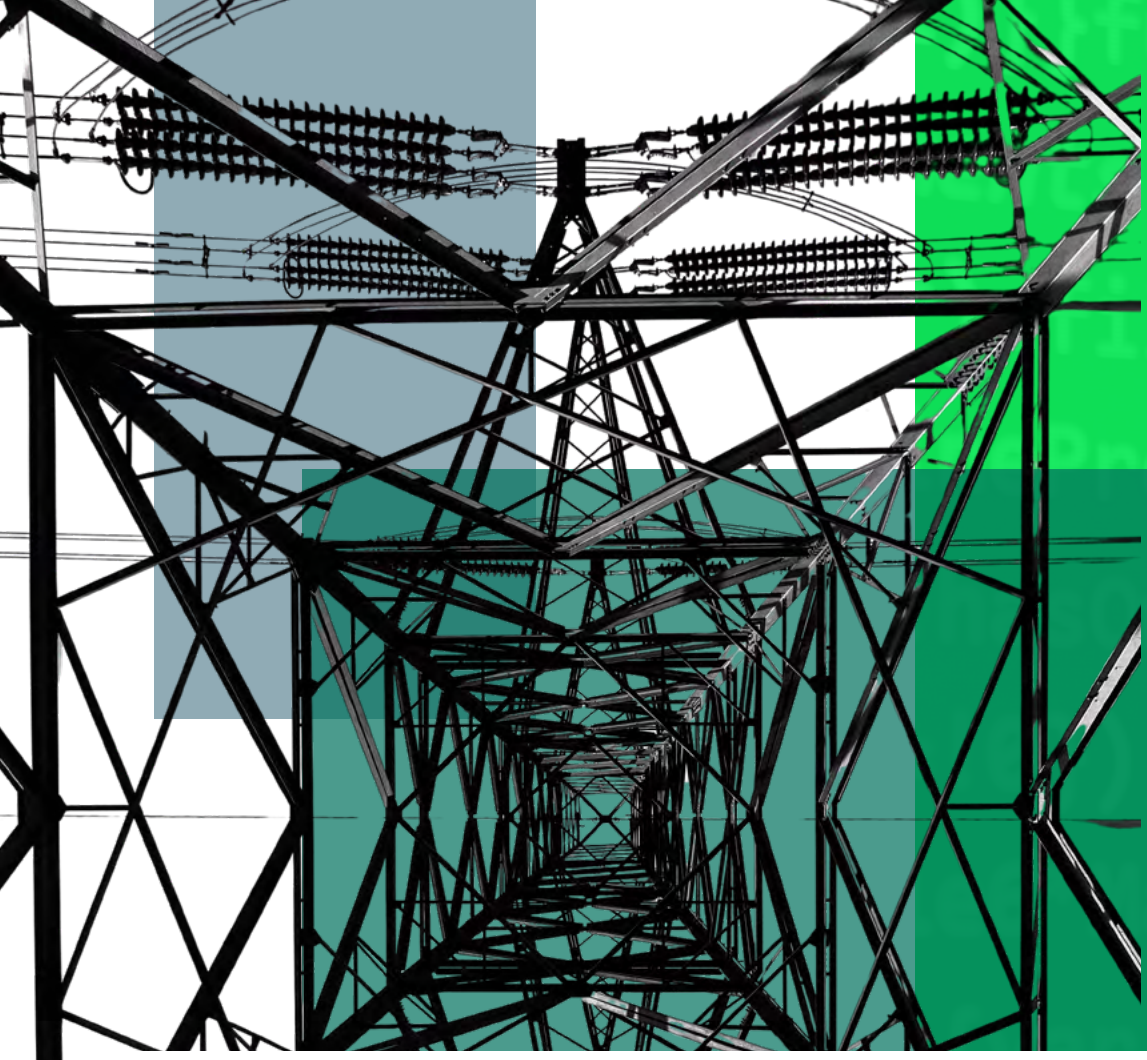


UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

GEOPOLITICAL CYBER INCIDENTS IN CANADA

2025 ASSESSMENT

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

Table of content

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 nationstates, 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 appearances. 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 Observatoire des conflits multidimensionnels (OCM) and Professor of Political Science at the Université du Québec à Montréal (UQAM). He is a recognized expert on US politics, US foreign policy and Canada-US relations. His recent work at the OCM has focused on Russian interference and information manipulation in US elections, US cyber conflict management, the effects of Sino-American geo-economic competition on Canada-US relations, and US geo-economic policy towards Canada.

Alexis Rapin is a research fellow at OCM. He works in particular on transformations in conflictuality, cyberdefense and influence operations. He has contributed to numerous scholarly publications on international politics and cybersecurity. In early 2023, he testified on Canadian cyber defense issues before the House of Commons Standing Committee on National Defence. Alexis Rapin is also a member of the editorial board of Rubicon, a French-language platform for analysis of international issues.

Danny Gagné holds a Ph.D. in political science from UQAM and is a research fellow at OCM. His research focuses on the US strategy of combat drone warfare. His recent work at OCM, focusing in particular on the manipulation of information for geopolitical ends, has been the subject of several columns on new conflictualities ("Chroniques des Nouvelles conflictualités") published by the Raoul Dandurand Chair.

Simon Hogue is Professor in the Department of Political Science at UQAM and a research fellow at OCM. His research, at the intersection of technology, power and cultural studies, examines security and war, social control and democracy in digitized societies. His most recent texts focus on the use of digital technologies in the Ukrainian war and digital resistance.

Marie Lamensch is the Global Affairs Officer at the Montreal Center for Global Security and an associate member at the Observatoire de géopolitique and OCM at the Raoul Dandurand Chair. Her research interests include international security and human rights, mass atrocity prevention, gendered disinformation, violent extremism and online hate, emerging technologies, transnational repression and digital authoritarianism.

Laurence Michalski is a master's degree candidate in political science at UQAM and a research fellow at OCM. Her research focuses mainly on American intelligence services. She is also interested in the geo-economic issues shaping relations between the United States, Canada and China.

Fanny Tan is a research fellow at OCM. A master's degree student in political science at UQAM, with a bachelor's degree in digital media (UQAM) and a certificate in video game design (UQAT), she regularly writes about technology in the media as an independant journalist. She is a tech contributor to the program Moteur de recherche (ICI Première) and a member of Lab 2038, a privacy advocacy organization.

Charlotte Vincent is an intern at OCM. A final year undergraduate student in international studies at Université de Montréal, she is interested in international security and peacekeeping issues.

2024 SOME SIGNIFICANT INCIDENTS

JANUARY

DATA BREACH AT GLOBAL AFFAIRS CANADA

Global Affairs Canada announces that it has suffered a major data breach. The breach affected the department's VPN service, enabling unauthorized access to the emails and personal information of some of its employees. No details have been released on the parties suspected of being responsible for the breach.

MARCH

CYBER INCIDENT AT FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) announces that it has been affected by a cyber incident. The system used to submit suspicious transaction reports is temporarily taken offline as part of remediation measures. No details have been released on the exact nature or origin of the incident.

MAY

STOIC PRO-ISRAELI INFLUENCE CAMPAIGN

An influence campaign aimed at disseminating pro-Israeli content about the war in Gaza is spotted on both Meta and X platforms. It is attributed to an Israeli electoral consulting firm called STOIC, and is said to have reached audiences in Canada, the United States and Israel, using, among other things, generative artificial intelligence tools.

SEPTEMBER

RRN CONTENT TARGETING JUSTIN TRUDEAU

An investigation reveals that Reliable Recent News (RRN), a fake news website linked to Russia, has recently published several contents related to Canadian politics. In particular, these publications were aimed at undermining support for Prime Minister Justin Trudeau. RRN is one of the platforms attributed to a vast Russian disinformation network known as Doppelganger.

OCTOBER

CHINESE RECONNAISSANCE ACTIVITIES AGAINST CANADIAN SYSTEMS

The Canadian Centre for Cyber Security reveals that a group of hackers linked to China conducted "large-scale" reconnaissance activities against numerous Canadian entities during 2024. Targets included federal government departments and political parties, the House of Commons, the Senate and civil society organizations.

DECEMBER

ESPIONAGE CAMPAIGN TARGETING TIBETAN AND UYGHUR ACTIVISTS

A report reveals that a group of hackers, dubbed Earth Minotaur and presumably linked to the Chinese state, has conducted a vast cyberespionage campaign targeting Uyghur and Tibetan communities in several countries, including Canada. The hackers were able to record calls, take photos and screenshots of compromised devices.

Canada and geopolitical cyber incidents : a data snapshot

As the year 2025 gets underway, the North American news cycle is becoming increasingly politically charged, and Canada's digital space is increasingly marked by the debates that governments and public opinion engage in on a daily basis. Last February, for example, we learned that Ottawa had ordered the Communications Security Establishment — Canada's main cybersecurity agency — to deploy for the first time its cyber capabilities against transnational drug traffickers. Clearly reacting to pressure from the Trump administration on border security, Canadian authorities now seem to want to use their cybersurveillance tools (and potentially their cyber attacks capabilities) to thwart fentanyl trafficking, one of the current areas of tension with our American neighbor. This is further proof, if any were needed, that it's becoming increasingly difficult to talk about politics without talking about the digital in Canada.

This increasingly close link is the focus of our latest report on geopolitical cyber incidents in Canada, the fifth publication of its kind produced by the Raoul Dandurand Chair's Center on Multidimensional Conflicts. Between cyberespionage campaigns and online influence operations, Canada remains year after year a significant target of the cyberconflictuality shaking the global digital space. As such, the analysis carried out in this report (without claiming to be exhaustive) has identified **11 geopolitical cyber incidents in Canada in 2024**. In all, the Raoul Dandurand Chair's Directory of Canadian cyber incidents, from which the data in this report is derived, currently lists **125 geopolitical cyber incidents affecting Canada since 2010**. However, this data comes solely from open sources, and therefore reflects only a fraction of the malicious digital activity taking place in the country.

What do we know about these incidents, their nature, their targets and their origins? Here's an overview of the data available on these issues.

WHAT DO WE MEAN BY CYBER INCIDENTS ?

We define "cyber incidents" as intentional, malicious, time-bound actions, carried out at least in part in cyberspace. The term cyber incident therefore includes cyberattacks, data breaches and acts of information manipulation, among other examples (for more details, see the "Typology" section below). This analysis focuses on cyber incidents of a geopolitical or strategic nature, most often orchestrated by nation-states.

The incidents discussed here have affected Canada, including its public authorities, companies and research institutions, as well as individuals, international organizations and non-governmental organizations based in Canada. In some cases, the incidents specifically targeted Canada, while in others they affected a variety of countries (including Canada).

What are the most common types of cyber incidents?

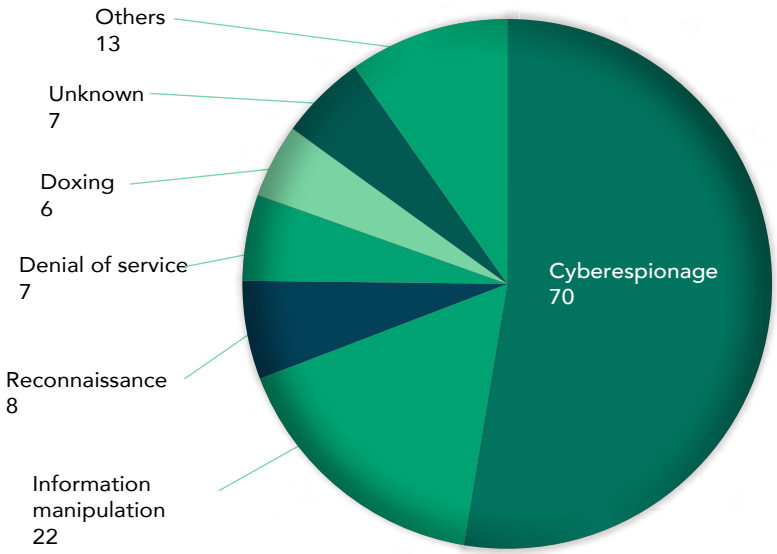
The vast majority of geopolitical cyber incidents affecting Canada continue to involve cyberespionage. These include the theft of intellectual property and state secrets, as well as the clandestine surveillance of individuals. Of the 125 incidents recorded since 2010, no fewer than 70 (56%) involve cyberespionage. Acts of information manipulation (i.e. the intentional, massive and coordinated dissemination of false or biased news for political ends) are the second most frequent type of cyber incident, accounting for 22 events since 2010 (or 18%). It should be noted that these proportions have remained remarkably stable over the five years covered by the previous reports, suggesting that a strong trend is at work.

Again in 2024, cyberespionage and information manipulation were the two most prevalent categories, with 5 and 2 incidents respectively. It should be noted, however, that several incidents in 2024 were only partially disclosed by the entities concerned, leaving doubt as to the exact nature of the malicious activities in question.

What are the known targets?

In 2024, Canadian government entities, especially federal ones, were particularly targeted. Global Affairs, the Royal Canadian Mounted Police (RCMP) and FINTRAC all suffered cyber incidents — the nature of which remains unclear — in January, February and March 2024 respectively. In April, the government of British Columbia claimed to have been targeted, apparently by state-affiliated hackers. Finally, in October, it was reported that Government of Canada departments and agencies, federal political parties, the House of Commons and Senate had been the object of intense reconnaissance activity by a group of hackers linked to the Chinese state. Such a concentration of cyber incidents targeting government agencies is probably unprecedented in Canada (see Chapter).

Most frequent types of cyber incidents (since 2010)



* Some cases may combine several types of incidents simultaneously

Source : Directory of Canadian Cyber Incidents

Nevertheless, the overall data from our directory confirms the pre-eminence of the public sector among the targets of geopolitical cyber incidents : 56% of incidents recorded since 2010 involved at least one Canadian public institution among the entities affected, compared with 37% for the private sector and 15% for civil society[1]. The degree of granularity of the information made public makes it difficult to break down these data by specific sectors of activity, but it does appear that the defense, energy and telecommunications sectors are among those most frequently targeted in Canada.

Where do most of these incidents originate from ?

Since 2010, **four countries have been responsible for the vast majority of geopolitical cyber incidents** publicly reported in Canada: China (37 incidents out of 125), Russia (32), Iran (12) and North Korea (9). These data concern the *geographical* origin of cyber incidents, and do not necessarily imply responsibility on the part of the governments of the countries mentioned (for more details, see the methodology section). In addition, due to the lack of published evidence, it appears that 23 of the incidents recorded since 2010 currently have no known origin.

Israel joined the list of suspected origins last year. In May 2024, we learned that an Israeli election consulting firm (dubbed STOIC) had conducted a major online information manipulation campaign, with a number of its contents specifically targeting Canadian audiences. STOIC's campaign was allegedly commissioned by the Israeli Ministry of Diaspora Affairs to discredit voices critical of the intervention in Gaza (see case study).

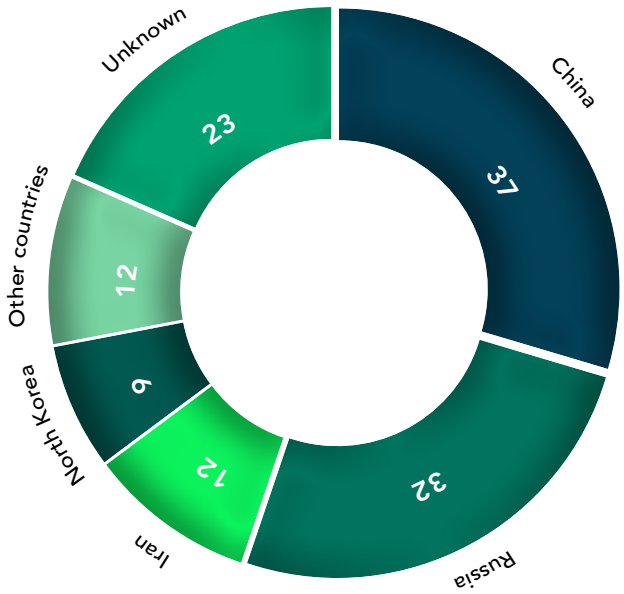
Which hacker groups targeted Canada in 2024 ?

Several cyber incidents affecting Canada in 2024 have been attributed to hacker groups already well known to the cybersecurity community. Among them is Flax Typhoon (also known as RedJuliett or Ethereal Panda), a perpetrator most likely affiliated with the Ministry of State Security of the People's Republic of China. This group is said to have operated a botnet that infected over 9,000 connected devices on Canadian soil (see case study).

Another group of Chinese hackers, known as Earth Minotaur, is said to have carried out

[1] It should be noted that an incident can simultaneously affect different types of targets.

Geographical origin of cyber incidents (since 2010)

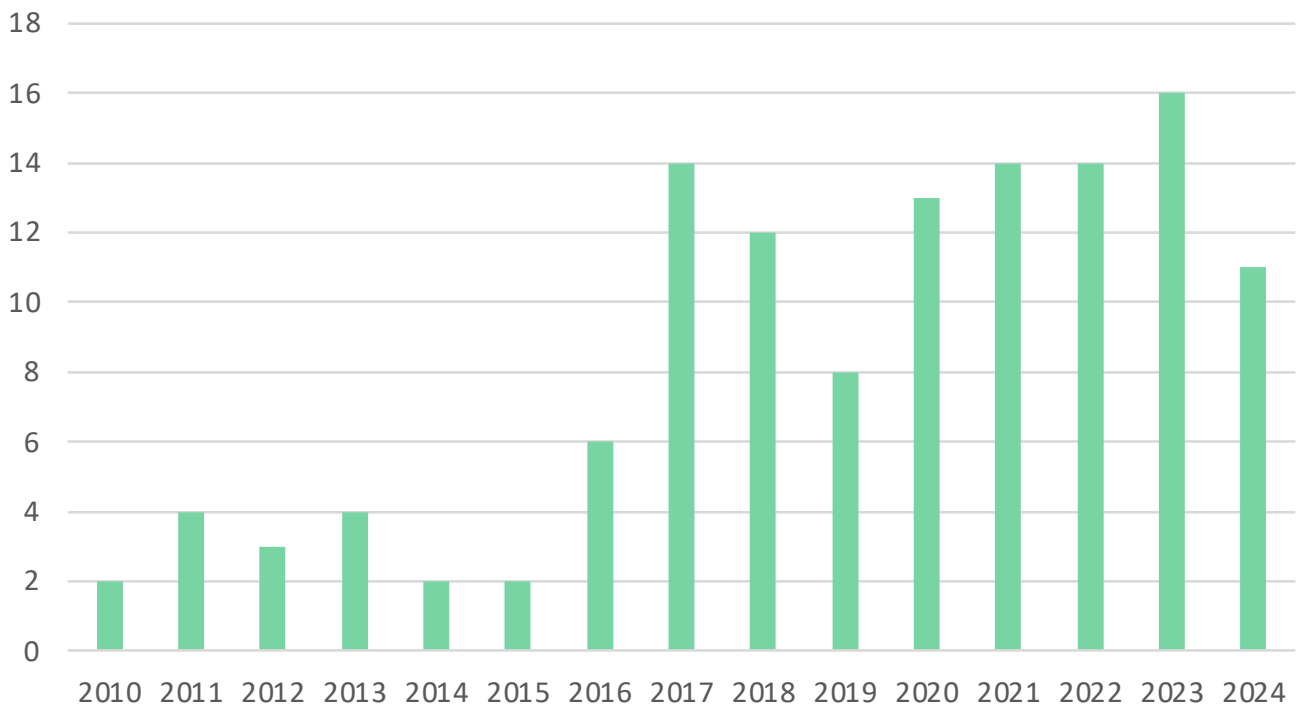


Source : Directory of Canadian Cyber Incidents

a major cyberespionage campaign targeting Tibetan and Uighur communities in several countries, including Canada (see case study). Previously unknown, Earth Minotaur is said to employ a range of tools very similar to those previously deployed by other Chinese groups. However, its affiliation with state bodies in the PRC cannot be formally confirmed.

By late 2024, a group of Russian hackers dubbed RomCom (also known as CIGAR or Storm-0978) had also targeted Canadian entities, though their number and nature were not specified. Interestingly, RomCom is said to conduct both intelligence operations and criminal activities, replicating a "hybrid group" profile increasingly seen in Russia. Frequently targeting Ukrainian state bodies, RomCom is likely to have links with the Russian security apparatus, according to the Google Threat Intelligence Group. The next sections of our report provide a detailed portrait of the main geopolitical cyber incidents that affected Canada in 2024.

NUMBER OF CYBER INCIDENTS REPORTED PER YEAR



CYBERESPIONAGE : still the most frequent type of cyber incident

Cyberespionage has been a widespread phenomenon in Canada for many years. Cyberespionage activities consist of "obtaining information through digital means without the information holder's prior consent", in particular to steal sensitive data and information for governments, companies or individuals.

As our Canadian Cyber Incident Directory shows, this is the most frequent type of cyber incident in our database for the period 2010-2025, including the year 2024. Our observations concur with those of the Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025-2026 report, which points out, among other things, that countries such as China and Russia have an interest in intensifying their cyberespionage activities against Canada in the future. According to the report, China continues to use cyberespionage to serve a number of foreign policy objectives: theft of intellectual property or industrial secrets, influence on public opinion or transnational repression of groups it considers a threat (Uyghur diaspora, Falun Gong followers, supporters of Taiwanese independence, etc.). For its part, Moscow sees Canada as a "valuable target", not least because of its status as a NATO member, but also because of "its support for Ukraine against Russian aggression, and presence in the Arctic". In recent years, for example, the APT29 group has conducted cyberespionage campaigns against Canadian research centers in an attempt to accelerate Russian discoveries on the COVID-19 vaccine. Another major example of a cyberespionage campaign affecting Canada was revealed in 2018, when we learned that China had, over a period of 12 years, conducted a vast campaign of economic cyberespionage against a dozen countries, including Canada, in sectors such as finance, telecommunications, healthcare, biotechnology, automotive and mining and drilling.

Serial targeting of government agencies

The year 2024 was no exception, with at least five cyberespionage campaigns specifically targeting Canada. In January, Canadian media such as CBC and the National Post reported that Global Affairs Canada had been the victim of a major data breach lasting over a month, enabling hackers to access the emails and steal the personal information of civil servants working for the department. A month later, it was the RCMP's turn to reveal that a large data breach detected in its systems had compromised essential data and threatened the organization's security.

> \\ As it stands, these incidents sometimes give the impression that the Canadian authorities are overwhelmed by the events, or unable to provide the public with sufficient information to reassure them about the cyber risks facing Canadian society. \\

In April, a cyberespionage campaign targeting the British Columbia government was a reminder that this type of cyber incident can target provincial governments as well as federal institutions in Ottawa. As with the attacks on Global Affairs Canada and the RCMP, investigations into this incident did not reveal the identity of the hackers or the extent and nature of the compromised data. However, cybersecurity expert Emeline Manson

pointed out that government computer systems are particularly attractive to hackers, as they contain confidential data that can be used for identity theft.

This modus operandi was probably used in another cyberespionage operation targeting Canada in 2024, namely the campaign by the Russian group RomCom, discovered in November by the IT and cybersecurity company ESET. Backed by Moscow, the hacker group took advantage of previously unknown security vulnerabilities in Windows systems and the Mozilla Firefox Internet browser to install malware on a wide range of computers in Europe and North America. The (probable) aim was to collect personal information on individuals or government secrets in countries such as Canada.

Incidents shrouded in mystery

The year 2024 reaffirms three conclusions about the phenomenon of cyberespionage in Canada. Firstly, Canada is not immune to a reality now firmly rooted in the contemporary international system: the tendency of various states to take advantage of digital means to conduct transnational espionage campaigns that are growing in scale, frequency and sophistication. Secondly, the year 2024 once again confirms the diversity of perpetrators, targets and motives behind cyberespionage incidents targeting Canada. In a world where Ottawa's interests diverge considerably from those of the governments and regimes that rule China, Russia, North Korea, Iran and even India, cyberespionage campaigns are likely to multiply in the future. Finally, this situation raises the question of Canada's ability to prevent such operations, detect them early, thwart them and learn from past attacks to perfect cyber defense strategies.

As it stands, these incidents sometimes give the impression that the Canadian authorities are overwhelmed by the events, or unable to provide the public with sufficient information to reassure them about the cyber risks facing Canadian society. Indeed, Ottawa has rarely been able (or has deliberately omitted) to reveal to its population the identity of the perpetrators of operations that specifically targeted the Canadian government, as well as the hackers' objectives. The March 2024 attack on FINTRAC is a case in point.

The operation against FINTRAC, a cyberespionage campaign or another type of cyber incident?

On March 5, 2024, a message announcing that FINTRAC systems were not available at this time, was displayed on the website of the Financial Transactions and Reports Analysis Centre of Canada, the Government of Canada unit whose mandate is to "assist in the investigation of money laundering and terrorist activity financing offences or threats to the security of Canada". Victim of a cyber incident, FINTRAC had suspended its online activity in order to protect the integrity of its internal systems and the confidentiality of its data. Although the intelligence agency has been less than forthcoming about the information compromised, it claims that the attack did not affect its intelligence and protected systems. Nevertheless, the hackers — whose origin has not yet been publicly established — have caused lasting disruption to FINTRAC's IT systems. Indeed, it was not until December 2024 that its reporting system returned to normal operations.

Outside observers note that the breaches created in this attack could have represented an unexpected windfall for criminals, and probably allowed suspicious transactions to fly under the radar of the agency. Although FINTRAC officials would not divulge exactly what tasks they have been unable to perform in recent months, the fallout from this incident on Canadian security could be considerable. Each year, FINTRAC receives some 20 million suspicious transaction reports from 31,000 different sources. Depending on their relevance, the information is passed on to law enforcement or tax authorities in order to prevent various crimes. For example, FINTRAC played a key role in a human trafficking case in Saskatchewan in 2023. As a result of this investigation, three people were charged with the mistreatment of a Bangladeshi woman visiting Canada on a visitor's permit.

FINTRAC may also prove an attractive target for cyber attacks, as it is not only a key player in the fight against terrorism, but also one of the bodies monitoring compliance with the economic sanctions imposed by Ottawa. Without presuming the identity of those responsible for the incident, it is important to note that states seeking to circumvent sanctions regimes could have an interest in carrying out this type of attack. For example, the US Department of Justice's Office of Foreign Assets Control was targeted by a group of hackers linked to the Chinese state in January 2025. The fact that FINTRAC works closely with similar government bodies responsible for detecting financial crime elsewhere in the world also explains why it may be targeted. This episode thus demonstrates the magnitude of the consequences that a cyber incident can trigger, offering criminal or state actors numerous options for weakening or destabilizing Canada.

TRANSNATIONAL REPRESSION IN THE DIGITAL AGE : a growing threath

In Canada and around the world, transnational repression, used by governments to repress their exiles and diasporas beyond their borders, is asserting itself with force. In addition to "traditional" methods of surveillance and intimidation, the emergence of new digital technologies amplifies the scope of threats to victims. Taking advantage of the multiplication of surveillance tools within an unbridled industry, authoritarian regimes have, more than ever, the capacity to extend their control abroad. The clandestine nature of these operations, often undemanding in terms of political and financial capital, makes it difficult to hold their perpetrators accountable, giving them the opportunity to act with impunity.

The global surveillance industry

The growth of the global surveillance industry offers its clients — both governmental and private — an ever-expanding arsenal of law enforcement tools. Despite the shockwaves generated in 2021 by the revelations about Pegasus, the powerful spyware of Israeli origin that was deployed against at least 180 victims in some twenty countries (including Canada), the surveillance industry still largely escapes regulation. As a result, it continues to equip actors wishing to exert control beyond their borders with sophisticated tools that are becoming less and less expensive.

Although authoritarian regimes are often criticized for their digital persecution of dissidents, whether through the development of their own state control capabilities or through the use of outsourced companies, the discovery of new spyware reveals the global nature of the surveillance industry, from which neither Western companies nor governments escape. For example, Israel and Italy, home to a growing number of spyware distribution companies, are now major hubs of this worrying industry.

Beyond spyware

Spyware is just one of the many tools available to authoritarian regimes to infiltrate the devices of dissidents abroad. The installation of backdoors, granting clandestine access to the devices of targeted individuals, or the compromise of websites using the watering hole technique — which infects visitors via the stealth download of malware — are two types of attack frequently used to keep an eye on diasporas abroad deemed problematic.

Unlike more powerful spywares, capable of infecting victims' devices automatically, these attacks make use of social engineering, where attackers pose as a relative or member of an organization associated with their field

of expertise to entice their victims to click on a malicious link. According to the researchers, these types of attacks reveal the growing appetite of threatening actors to infiltrate their targets' cell phones, giving them access to a range of personal data, such as text messages and call lists. What's more, these attacks also enable them to spy on their victims via their phone cameras, microphones or GPS.

The data-sharing obligations that some technology companies owe to state security and intelligence services, notably in China, may also play a role in strengthening the ability of states to spy on their diasporas abroad, who depend on digital platforms to communicate with each other and with their loved ones back home. The creation of mutual legal cooperation agreements on "cybercrime" issues could also represent a victory for authoritarian regimes, strengthening their ability to identify, track down and demand the return of dissidents living in exile.

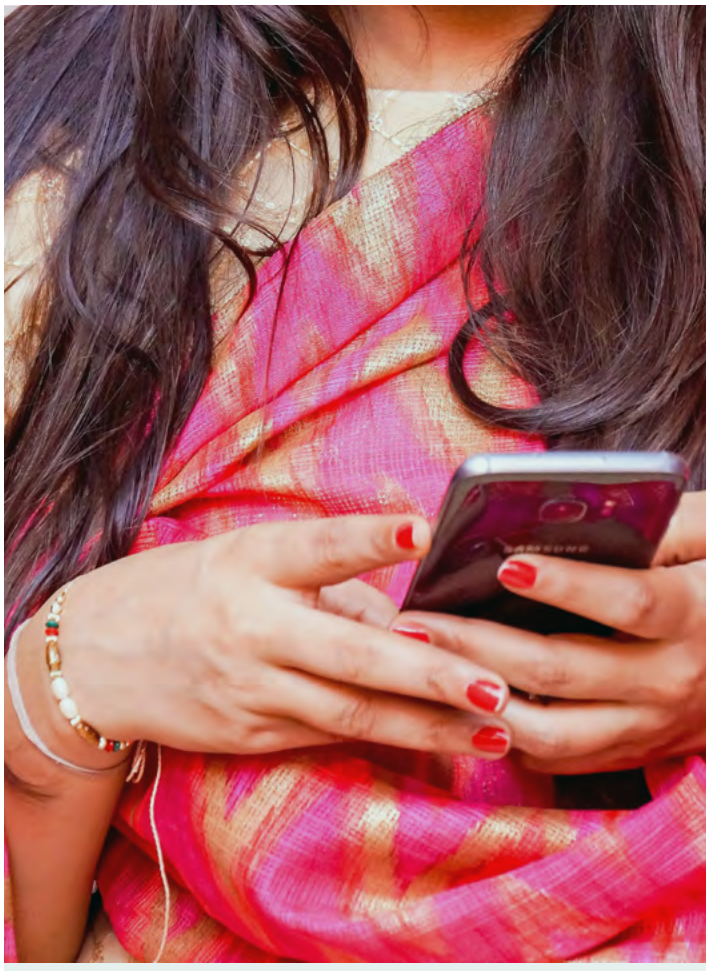
In Canada

In Canada, transnational repression falls into the broader category of foreign interference, a threat that is the subject of growing public and governmental awareness. This awareness led to a public inquiry in January 2025, chaired by Judge Marie-Josée Hogue. Although she admitted in her final report that she had only "scratched the surface" of transnational repression, she nonetheless asserted that it represents "a genuine scourge", undermining democratic institutions and preventing members of oppressed communities from participating in democratic life and fully enjoying their rights and freedoms.

Three states in particular are accused of being perpetrators of transnational repression in Canada : Iran, the People's Republic of China (PRC) and India. In 2024, Canada saw at least two major cases of transnational repression linked to the latter two governments: the assassination of Sikh activist Hardeep Singh Nijjar in British Columbia (allegedly involving the Indian government, according to Canadian intelligence agencies), and the PRC's foreign police offices on Canadian soil.

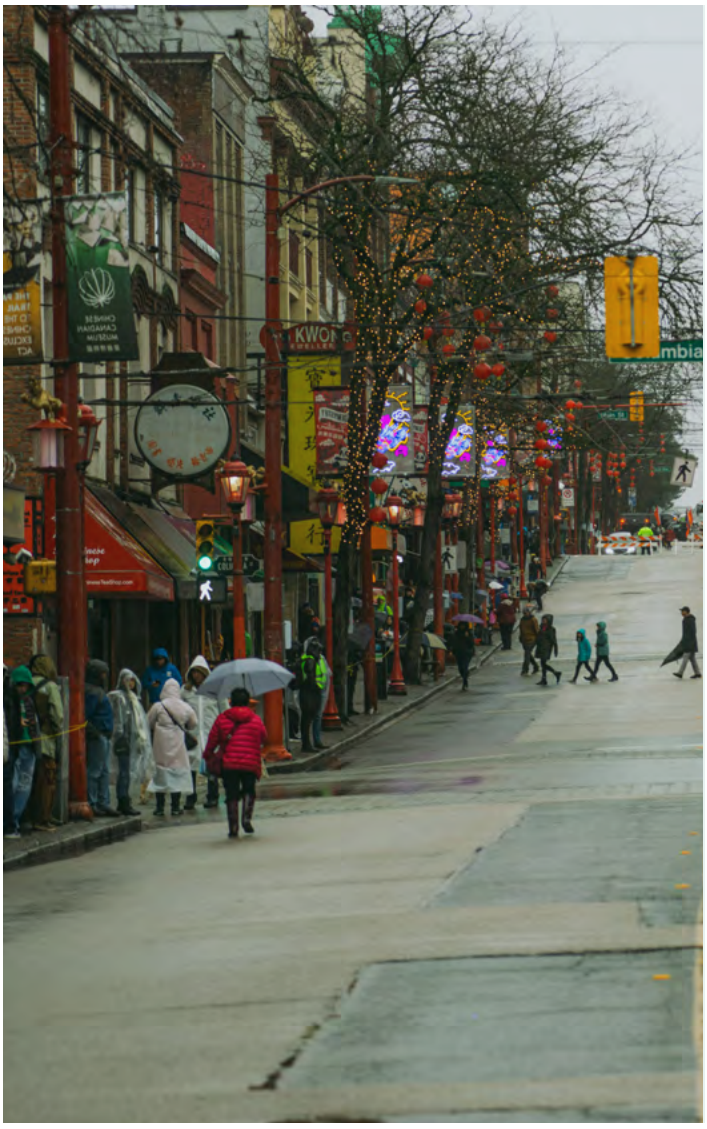
> \\ While these high-profile incidents represent extreme cases of threats and physical abuse against victims in Canada, the reality of transnational repression within the country is far less visible. \\

While these high-profile incidents represent extreme cases of threats and physical abuse against victims in Canada, the reality of transnational repression within the country is far less visible. Indeed, the overwhelming majority of repressive digital activities carried out in Canada by foreign



actors are conducted using digital intrusion tools and techniques that are difficult to detect. Our directory of cyber incidents records some of these "invisible" cases of repression, such as the cyberespionage of Ethiopian dissidents based in or passing through Canada in 2017, or the case of Iranian activists based in Canada in 2020. And as elsewhere in the world, victims of transnational repression based in Canada are not only spied on; they are also intimidated and threatened, notably via the manipulation of digital platforms used in everyday life, such as Weibo, WhatsApp or X.

For example, attackers may suspend their targets' social networking accounts by reporting their profiles en masse, or may disseminate false information about them to tarnish their reputation online, particularly among members of the same diaspora. The aim is to create tension within communities, thereby weakening them and undermining their mobilization efforts. Attacks can be carried out in plain sight, or more discreetly, by sending threats via private messaging.



Everyday anguish

Recent research into the social, professional and psychological consequences of transnational repression warns of the demobilizing effects of the phenomenon. Victims may isolate themselves and suspend, or even cease altogether, their activism out of fear or exhaustion. By extension, online intimidation tactics also have the effect of terrorizing other diaspora members and force them into silence, lest they be targeted by similar acts. In recent years, civil liberties groups have increasingly focused on the gendered aspect of transnational digital repression, lifting the veil on the disproportionate consequences experienced by women activists targeted by such tactics, compared to their male counterparts.

For the witnesses heard at the Canadian Public inquiry and the activists interviewed by human rights groups, transnational repression is a daily obstacle, a shadowy threat difficult to expose and to contain given the lack of resources available to those who suffer it. With 22% of Canada's population born abroad, and authoritarian regimes benefiting from an ever-growing arsenal of digital surveillance tools, there is no doubt that the spread of state oppression within Canadian borders will continue to be a major issue in the years to come.

Earth Minotaur's campaign against Tibetan and Uyghur activists

In December 2024, the cybersecurity firm Trend Micro revealed that Earth Minotaur, an advanced persistent threat (APT) group likely linked to China, had been spying on Tibetan and Uyghur activists in several countries, including Canada.

The attacks involve contacting targets within group conversations on instant messaging platforms, such as WhatsApp and WeChat. To entice them to click on malicious hyperlinks and increase their chances of success, attackers impersonate different individuals. Their "carefully crafted" phishing messages pretend to come from official Chinese bodies, or display Chinese news related to COVID-19, religions, Tibetan or Uyghur populations, and travel to China.

When clicking on the hyperlink, the victim is redirected to an exploit kit — a kind of toolbox targeting specific vulnerabilities in a computer system — referred to by cybersecurity researchers as MOONSHINE. MOONSHINE then installs the DarkNimbus backdoor on the target's device, without their knowledge. Described by the researchers as a "comprehensive Android surveillance tool", the backdoor enables attackers to steal privileged information from its targets, such as contact or phone call lists, SMS messages, clipboard contents, browser bookmarks and conversations from several instant messaging applications. The attackers were also able to record calls, take photos and screenshots, as well as carry out certain operations on the targeted devices.

The MOONSHINE exploit kit has already been used in the past against the Tibetan community by another China-linked threat actor, named POISON CARP by the Citizen Lab. At the time, the attack already represented "a significant escalation in social engineering tactics and technical sophistication" from those typically used against the Tibetan community. Since then, MOONSHINE's capabilities have improved, now featuring new vulnerabilities and more protections to counter detection efforts.

According to Trend Micro researchers, the MOONSHINE exploit kit, used by other sophisticated hacker groups such as POISON CARP and UNC5221, is still under development. However, no link could be established between Earth Minotaur and the other actors who have exploited this kit in the past, suggesting that this is a new protagonist in the cyberthreat landscape.

INFORMATION MANIPULATION AND GENERATIVE AI : evolution or revolution ?

As we look ahead to 2025, information manipulation campaigns will follow one another, but not be the same: the use of generative artificial intelligence (AI) for fraudulent purposes is on the rise, in Canada and elsewhere. As early as the end of 2023, Microsoft revealed the existence of an Iranian influence operation based on a fake video report created by generative AI, to which Canadian Internet users had allegedly been exposed. Other such cases were added to the list in 2024 (see box below).

Using artificial intelligence to generate content on social media is now common practice. South of the border, the US presidential elections provided an opportunity to observe this growing trend. According to the firm Thales in the US, traffic generated by bots represented no less than 32% of Internet traffic in 2022, and is expected to rise to around 35% by 2023. With the Canadian population set to go to the polls in 2025, we need to take a serious look at the potential for information manipulation arising from the AI revolution, whose imitation capabilities are proving increasingly realistic.

Information fog

In September 2024, we learned that a vast Russian influence campaign dubbed "Doppelganger", dismantled by the American justice system, included content about Canada. A fake news site published more than a dozen articles ridiculing Justin Trudeau and emphasizing the leader of the Conservative opposition, Pierre Poilièvre. Although this is apparently not the case for Canadian content, the Doppelganger campaign included several AI-generated pieces. It's worth noting that, in Ottawa's toolbox for combating disinformation, there is currently no legislation covering the artificial manipulation of voices and images, the hallmark of malicious actors creating deepfakes. Stéphane Perrault, Canada's Chief Electoral Officer, is urgently calling for reform of existing legislation in this area.

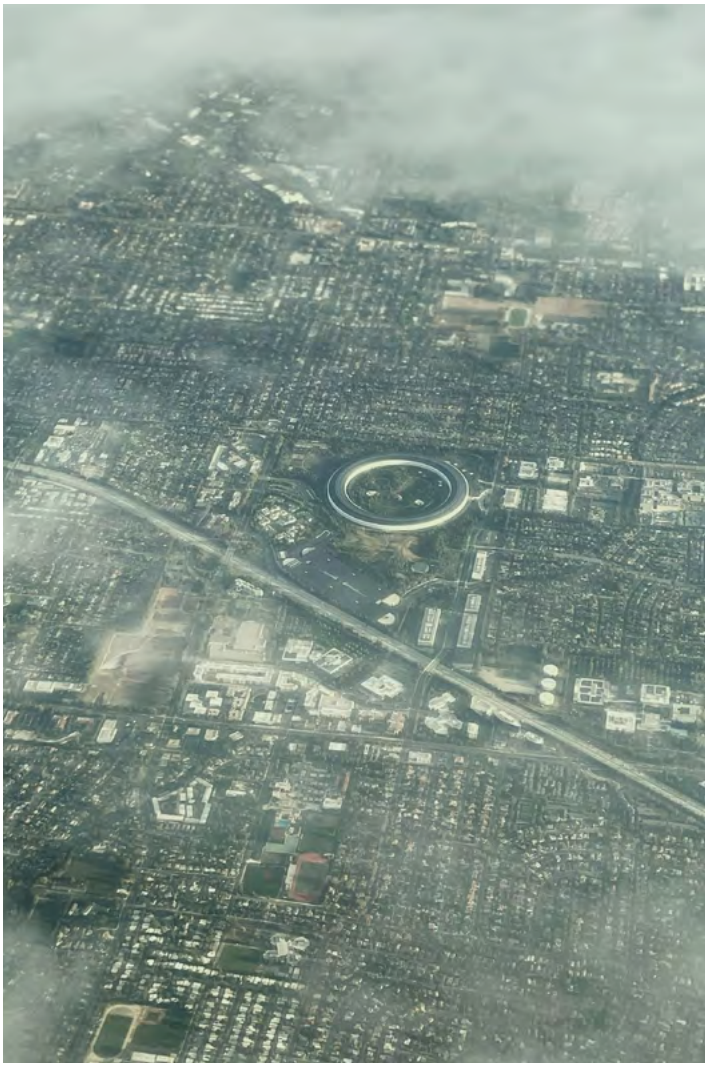
In October 2024, an Algerian cybercriminal group dubbed FunkSec claimed to have intercepted a conversation between Donald Trump and Benjamin Netanyahu. The deception was quickly spotted: the so-called recording was in fact a conversation generated by artificial intelligence, the group probably seeking to gain visibility to attract the attention of potential customers. Although this incident does not specifically concern Canada, it does suggest that private hacker groups simply seeking to promote their services could also be contributing to the thickening of online information fog.

Content moderation on the wane

While the private sector and technology giants have played a major role in the fight against misinformation in recent years, recent news is cause for concern. Meta announced in January 2025 that it was discontinuing its fact-checking operations. Just like Elon Musk's approach on X, Mark Zuckerberg is passing the torch to the user community, which is not necessarily the best equipped to do this work. The impact this decision will have remains to be seen, as Donald Trump's return to the White House seems to herald an era of deregulation for some of the leading Tech Giants who reacted positively to his victory. In fact, Vice President JD Vance declared on February 11, 2025 that the United States would not participate in an international regulatory regime for AI, the Paris AI Action Summit, which he said would hamper innovation.

Another worrying phenomenon is the seemingly increasing capability of artificial intelligence to act

autonomously. Indeed, the US news verification firm NewsGuard recently published figures about the proliferation of websites created with generative AI, but which administer themselves with minimal human intervention, if not completely autonomously. While no such sites were listed in the first half of 2023, the firm now lists around 1150 of them, operating in 16 different languages and publishing articles that are sometimes written entirely by bots. A variety of subjects are discussed, including politics and the war in Ukraine, which seems to be one of the particularly popular topics for 2024. It's not hard to imagine how these mechanisms could contribute to a growth of online information manipulation.



A technology on the rise

Among recent advances in the field of AI, we note that generative adversarial networks (GANs), have made major progress since their first appearance in 2014. These programs pit two artificial neural networks against each other in a kind of competition to create, say, an image. In turn, one AI creates an image and another tries to determine whether it is genuine. The two systems then train each other to create increasingly convincing images.

> \\ Content created by artificial intelligence is undoubtedly always more persuasive, but doesn't necessarily generate more interaction on social media. \\

In a study published in 2022, hundreds of participants took part in an experiment in which they had to determine from a series of faces which were genuine and which were generated by AI. The results were far from reassuring: not only were the participants unable to tell the difference, but a large proportion of AI-generated faces were judged more likely to be genuine. With the meteoric progress of generative AI, 2022 now seems a long way off. Although the number of fake accounts created by the use of such technologies is currently low, a recent study shows that they are mainly used to polish phishing campaigns and amplify the spread of inauthentic messages on social networks.

That's not to say we're sailing blindly into the storm. Content created by artificial intelligence is undoubtedly always more persuasive, but doesn't necessarily generate more interaction on social media. And while it can propel influence campaigns more systematically, taking up more and more space on platforms, it has so far often failed to convince the targeted users. Finally, there is as yet no evidence that exposure to AI-generated content or receipt of messages from conversational bots leads to any consequent change in political or ideological allegiances.

STOIC's pro-Israeli influence campaign

In March 2024, DFRLab, a US organization that studies disinformation and influence campaigns, uncovered an operation aimed at disseminating Islamophobic content in the United States, all in connection with the war in Gaza. The investigation exposed fake content, written in English and Hebrew, propagated by over 130 fake accounts on X belonging to so-called students of Jewish origin, African-Americans and concerned citizens. These accounts called for the release of hostages kidnapped by Hamas on October 7, 2023, criticized the demonstrations on university campuses and denounced the activities of the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), portrayed as being aligned with Hamas.

As Meta seized on the results of the DFRLab investigation, an internal analysis not only identified 510 fake profiles on Facebook and 32 on Instagram, all created in a very short period of time, but also established links with campaigns in other countries, including an influence campaign run under the aegis of the United Citizens for Canada account. OpenAI, the American firm behind ChatGPT, confirms that its services, notably ChatGPT, were used to create written content. The various investigations also show that generative AI was used to create faces to enhance the fake profiles, making them more credible.

The company behind the operation is the Israeli marketing firm STOIC. It is believed to have received $2 million from the Israeli Ministry of Diaspora Affairs to carry out the operation. What role did United Citizens for Canada play? The fake account was mainly used to share anti-Muslim content with journalists, politicians and genuine social media users. The account warned against the imposition of Sharia law in Canada, while criticizing Canada's lax immigration policies for allowing violent Islamist groups to take root. However, according to Mike Dvilyanski, Head of Investigation at Meta, the campaign generated few reactions: although fake profiles were used to boost the campaign and generate more shares, genuine interactions were rare and fake profiles were relatively easy to spot and suspend.

Yet this case is not insignificant. Firstly, while influence campaigns are nothing new, the links between Tel Aviv and STOIC suggest a close collaboration between states and the private sector to subcontract these operations, making them increasingly difficult to identify and attribute. States thus acquire a layer of plausible deniability to conceal their involvement, which could make them more willing to undertake such campaigns in the future. Moreover, the probable involvement of the Israeli state in the operation also demonstrates that influence campaigns in Canada are no longer likely to be the sole preserve of "traditional" rival powers (Russia, China, Iran, etc.), but could in future also come from countries regarded as partners.

BOTNETS AND OFFENSIVE INFRASTRUCTURES : when cyberoperations generate “collateral victims”

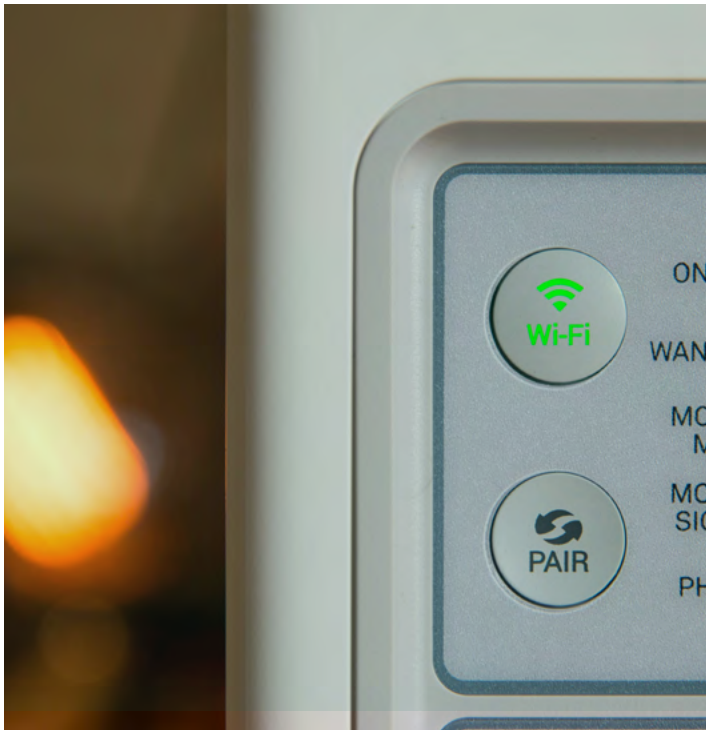
Can you suffer from a cyber attack without being its direct target ? Although the issue is not the most discussed by the cybersecurity community, the answer is a clear yes. In fact, as part of their malicious activities, hackers frequently use intermediate targets, whose computer systems are intended to serve as a springboard for a larger operation. In most cases, this involves discreetly taking over a piece of network (a server or router, for example), with a view to building up an offensive infrastructure. Although not itself a victim of data theft or denial of service, the entity concerned nonetheless sees its IT system partially hijacked — usually without its knowledge.

The year 2024 was a reminder that this kind of incident does, at least occasionally, affect Canada. In September, the member states of the Five Eyes announced that they had dismantled a network of “zombie computers” (a botnet) operated by a group of Chinese state-sponsored hackers, comprising almost 260,000 connected devices and including over 9,000 Canadian devices. Owned by small businesses or even private individuals, these machines were discreetly controlled remotely by the hackers and used as vectors for other operations, such as cyberespionage (see box below). However, this event is not a first for Canada. In March 2022, a report published by cybersecurity firm Trend Micro revealed that a botnet of routers, clandestinely set up by the hacker group Sandworm, affiliated with Russian military intelligence, was instrumentalizing the equipment of several Canadian entities.

Hijacking and obfuscation

To understand what is at stake in the clandestine creation of offensive infrastructures, we might compare collateral victims to car owners, whose vehicles are discreetly stolen at night to commit theft and burglary. Although they are not themselves the target of the crimes in question, the owners see their property used against their will, and for nefarious purposes to boot. This remote control is generally obtained by installing malware or a backdoor on the devices in question, and can last from a few days to several months, depending on the type of activity undertaken. Frequently deployed by cybercriminals, such processes are also occasionally used by state-sponsored hacker groups — and cases of infrastructure sharing between the two spheres have already been documented.

In the case of state-affiliated hackers, hijacked IT infrastructures can serve a variety of purposes. A discreetly remote-controlled corporate server, for example, may be used to temporarily store data stolen from the primary target, pending final exfiltration. A personal



computer, once attached to a botnet of several thousand other devices, can contribute to a denial of service attack against a website by flooding it with inauthentic requests. Home routers, meanwhile, can serve as transit nodes for hackers, lengthening and complicating the path taken to hack a target in order to disguise the true origin of a cyberattack. In other words, these compromised devices can provide hackers with storage space, processing power and an obfuscation mechanism.

Collateral victims, real damage

Although these collateral victims are usually chosen at random, they do have certain specific characteristics: they are, in general, small organizations with very modest IT staff, whose infrastructure is subject to few security controls. They may be small businesses, municipalities or educational institutions, for example, or even private individuals. Trend Micro's investigation from 2022 revealed, for example, that the botnet set up by Russian intelligence hackers counted a small local plumbing company in the USA among its victims. What's more, such organizations often use cheap or aging connected devices, whose vulnerabilities are not or no longer repaired by the companies that designed them. A large-scale Chinese cyberespionage campaign publicized in 2023, for example, relied on the exploitation of old, non-updated routers, presumably owned by small businesses or private individuals. The Fancy Bear hacker group, linked to Russian military intelligence, has recently done the same in the UK and the USA.

> \\ The IoT revolution means that the attack surface available to hackers is currently growing exponentially, and the barriers put in place to secure these new digital territories are often outdated. \\

As hackers are usually careful to maintain a limited level of activity on rogue devices, those targeted rarely realize that part of their network is being stealthily exploited for illegitimate purposes. This does not mean, however, that no harm is done to intermediate victims. Hijacking a device's processing power, for example, can temporarily impair system performance, slowing down the parallel activities of the legitimate user. In extreme cases, careless or clumsy handling by hackers could even bring down the rogue network, forcing its owner to undertake sometimes costly remediation measures. In a study published in 2018, researchers at Princeton University even envisaged the possibility that a botnet grouping together numerous connected household appliances could one day be used to destabilize a community's electrical grid by suddenly ordering energy-hungry appliances to be switched on en masse.

Towards collective security

In fact, one current development is contributing significantly to heightened concerns about the construction of clandestine infrastructures: the rise of the Internet of

Things (IoT), which sees millions of connected objects joining the global Internet every day, from digital photo frames to "smart" toasters. Often small, inexpensive and hastily designed, these devices frequently present major security flaws, which can easily deliver access to hackers seeking to build an offensive infrastructure. As an example, the Mirai botnet, one of the largest observed to date, counted among its "zombie devices" many small, inexpensive and poorly-secured objects — including connected cameras. The IoT revolution means that the attack surface available to hackers is currently growing exponentially, and the barriers put in place to secure these new digital territories are often outdated.

\\ The introduction of minimum cybersecurity standards for devices marketed in Canada could be an avenue worth exploring. Such initiatives could encourage other countries to follow suit, and thus stimulate a form of collective security. \\

From a security and strategic point of view, it's tempting to see the problem of compromised IT infrastructures as a secondary issue. After all, the users concerned are far more like tools than direct victims of state-sponsored hacker groups. The fact remains that the hijacking of digital devices is a source of threat for other players around the world. While Canada officially aspires to promote "responsible State behavior in cyberspace", preventing the clandestine use of Canadian IT infrastructures for malicious purposes seems important. In this respect, the introduction of minimum cybersecurity standards for devices marketed in Canada could be an avenue worth exploring. Such initiatives could encourage other countries to follow suit, and thus stimulate a form of collective security. Recent developments in the European Union could also encourage manufacturers to adopt better practices. In cyberspace, probably more than anywhere else, protecting others often also means protecting oneself.

Dismantling the "Raptor Train" botnet

On September 18, 2024, the cybersecurity agencies of the Five Eyes member countries issued a joint advisory that quickly caused a stir in the digital sector. It announced the successful dismantling of a vast botnet operated by a group of hackers linked to the People's Republic of China. Known as Raptor Train, the botnet was believed to have compromised up to 260,000 digital devices, including routers and connected cameras, most of them used in homes or offices. With almost 9,200 compromised devices, Canada accounted for 3.5% of the botnet's infrastructure — ranking 6th among the 20 or so countries affected.

According to the press release, the botnet could be used, among other things, as a proxy to disguise the origin of Chinese-led cyber operations, and as a vector for distributed denial of service (DDoS) attacks. Nicknamed Flax Typhoon in the cybersecurity industry, the group that built and operated this botnet is believed to be linked to China's Ministry of State Security through a government contractor called Integrity Technology Group. According to reports from cybersecurity firms, the botnet took its first steps in May 2020 and reached its growth peak in mid-2023.

The list of devices compromised to build the botnet, the largest attributed to China to date, is varied. It included home and office routers and modems, network-attached storage servers, connected cameras and digital video recorders (typically used for video surveillance systems). Black Lotus Labs, the company that first spotted the botnet, estimates that these devices were infected for periods typically ranging from 17 to 75 days, depending on their role in the Raptor Train infrastructure.

It was the FBI, with the authorization of the American courts, that led the remediation operation — which lasted a fortnight — that enabled the dismantling of Raptor Train. However, Flax Typhoon's hackers attempted to obstruct the clean-up operation by launching a parallel denial of service attack against the FBI's operational infrastructure — without success. In January 2025, the Treasury Department announced sanctions against Integrity Technology for taking part in cyber operations targeting US entities.

Canada, for its part, has not adopted similar measures. In October 2024, in conjunction with the release of its National Cyber Threat Assessment 2025-2026, the Canadian Centre for Cybersecurity stated that China currently represents the "most sophisticated and active state cyber threat to Canada today".

CONCLUSION

An end to Ottawa's silence : Canada must be transparent about cyber incidents

For the first time since its launch in 2020, this report observes a drop in the number of cyber incidents reported in Canada. From 16 cyber incidents in 2023, Canada has been targeted by foreign actors only 11 times this year, according to available data. This finding is surprising in view of a busy international news cycle that tends to suggest an intensification of geopolitical cyber incidents around the world: from electoral interference in the USA and Romania, to the infiltration of the networks of American telecom giants, to the sabotage of undersea Internet cables in the Baltic Sea. More shockingly, this finding is at odds with the National Cyber Threat Assessment 2025-2026 report published by the Canadian Centre for Cybersecurity, which notes, in no uncertain terms, that the country "is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors, from cybercriminals to hacktivists, that are targeting our critical infrastructure and endangering our national security". The Centre also notes that in "the last two years, we have witnessed a sharp increase in both the number and severity of cyber incidents, many of which target our essential services".

If the Canadian Center for Cybersecurity's conclusion is worrying, it has, at the very least, the merit of disqualifying any talk of complacency. Canada is no exception to this global trend. Neither its virtue nor its diplomacy are protecting the country, nor is Canada's "grand return" to the international stage announced by the Trudeau government in 2015. Canada is well entrenched in Western, Anglo-Saxon and North American networks of alliances that are prime targets for China, Russia, Iran and North Korea. But then, how can we explain the gap between the OCM repertoire and this global trend?

We believe that Ottawa's silence and secrecy explain why it is so difficult to get an overall picture of the phenomenon in Canada. As Canada's Foreign Interference Commission (or Public Inquiry Into Foreign Interference) noted in its final report, the government has proven to be a "poor communicator" and "insufficiently transparent" when it comes to foreign interference. The same observation applies to other spheres of national security.

For those who follow the activities of Canadian security institutions, this criticism comes as no surprise. Cyber incidents affecting Canada are often accompanied by terse press releases, such as those announcing the Chinese smear campaign targeting Canadian parliamentarians and the cyber attacks on Parliament, the National Research Council, Global Affairs, Rideau Hall and the National Security and Intelligence Review Agency. As the press releases are excessively general, the reader cannot derive any relevant information from them. Rather, it is through the work of private actors, from companies or civil society, that it becomes possible to piece together the events — although it must be acknowledged that many firms within the cybersecurity industry are also becoming increasingly evasive in what appears to be a desire to preserve their corporate interests.

But this should not be seen as a simple division of labor. The Canadian government's lack of transparency has consequences. It hinders research, that is, the development of knowledge about an "existential threat" to Canada's security, in the words of the Commission on

Foreign Interference. Moreover, by limiting the transmission of information to the Canadian public, the government is omitting the factual and contextual elements that enabled the government to reach its conclusion on the events. The government's conclusions must be accepted on the basis of authority — because Ottawa says so — rather than shared and understood by the public.

This form of non-communication encourages contestation — including that of dubious foundation — and hinders healthy public debate on government management. Thus, while Washington announced in December 2024 that it had been the victim of the largest cyberattack in US history, Ottawa remained silent. Yet Salt Typhoon, the group responsible for the attack, has been active for several years and has attacked Canada, among other prime targets. Many experts also point out that Canadian communications networks share the same vulnerabilities as those deployed in the USA. If it turns out that Canada was spared, the attack could at the very least have served as an opportunity to explain why it was so.

Admittedly, transparency can impose operational constraints on security institutions, for example by revealing the tactics and strategies of the authorities, something the Canadian government claims to justify its silence. However, this constraint also exists elsewhere. The head of the American cybersecurity center, CISA, was not at all enthusiastic about revealing the existence of the Salt Typhoon cyberattack. This did not stop the US government from being transparent, with all the risks and constraints that this decision imposed.

Sharing information is based on a relationship of trust. By cloaking themselves in secrecy, security institutions show that they have little, if any, trust in the Canadian public. This lack of trust, which bordered on condescension in the words of David Johnston, Special Rapporteur on Foreign Interference, is deleterious to research, public debate and, more broadly, the consolidation of social cohesion in Canada. At a time when the legitimacy of governments is constantly being called into question, we must join the Commission on Foreign Interference in calling for greater government transparency: "The Commission's experience has shown that a great deal of information can be made public without compromising national security". We can only hope that Ottawa will commit to greater dialogue with civil society in the future.

Methodology

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 :

CYBERESPIONAGE : 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 (see Jeangène Vilmer et al., 2018).

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

Text editing
Daphné St-Louis Ventura
Louis Collerette

Graphical design
Françoise Conea

With the support of

BANQUE NATIONALE

Cover design : Françoise Conea