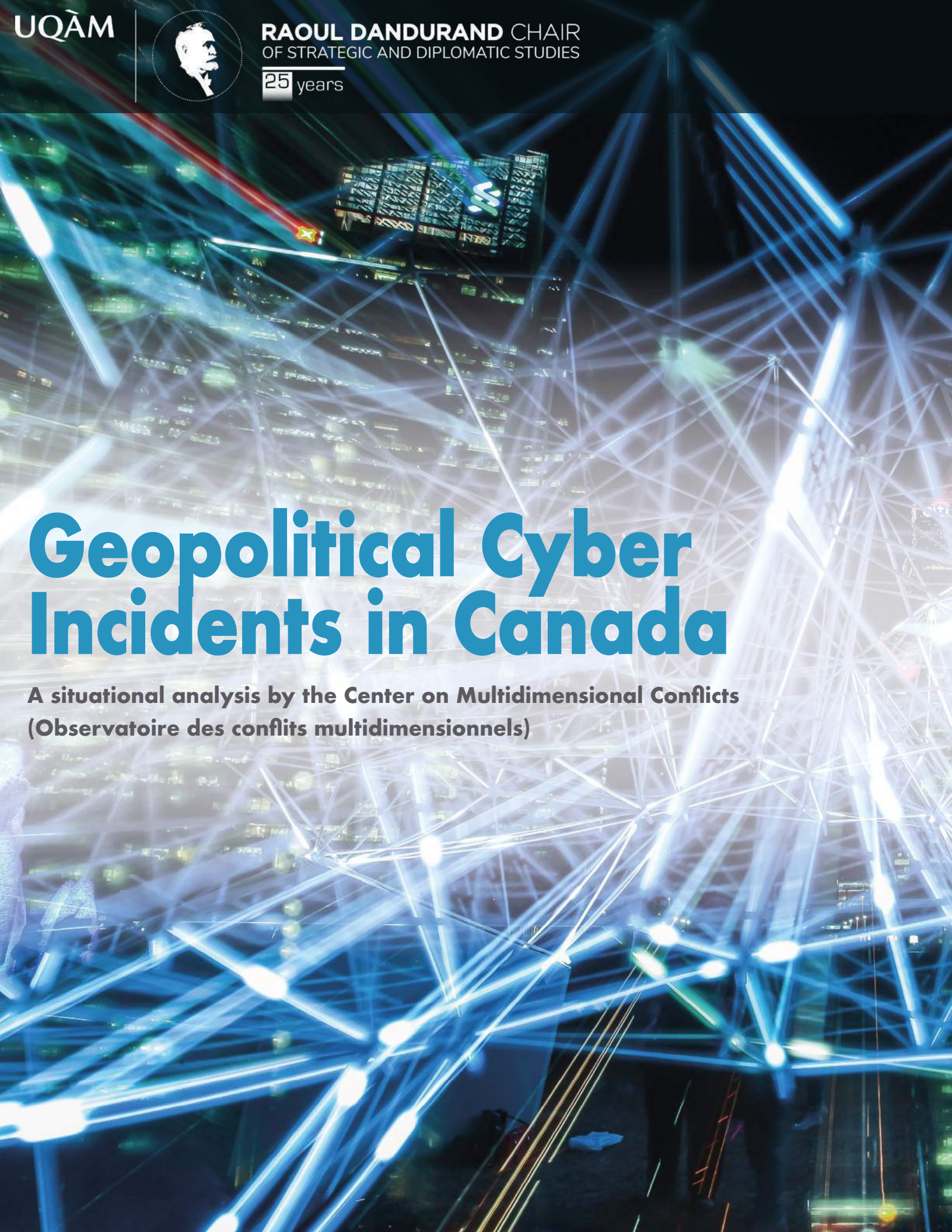
UQÀM

RAOUL DANDURAND CHAIR
OF STRATEGIC AND DIPLOMATIC STUDIES
25 years



Geopolitical Cyber Incidents in Canada

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

Introduction

During the 2016 U.S. presidential election, Russian hackers rattled one of the world's largest democracies. They spread political misinformation on social media and released emails from the Democratic Party's Democratic National Committee on WikiLeaks in an effort to get Donald Trump—Moscow's preferred candidate—elected. Russian interference continued on afterwards, frequently paralyzing American political life. Democrats questioned the very legitimacy of the Trump presidency. The United States Congress undertook numerous investigations into alleged collaboration between Moscow and Trump's entourage. And the Department of Justice launched the Mueller investigation, dividing both Washington and the American people for close to two years.

While this cyber incident did not directly affect Canada, it was nonetheless of undeniable importance to Canadians. On the one hand, it proved that it was now possible to destabilize any country in a few clicks, even a superpower like America. On the other hand, it served as a reminder that malicious actions in cyberspace are now at the heart of the international conflict landscape and that Canada, which has experienced numerous cyber incidents in recent years, must also take this into account.

The Center on Multidimensional Conflicts (Observatoire des conflits multidimensionnels or OCM) of the Raoul Dandurand Chair has therefore prepared this report on geopolitical cyber incidents in Canada. It is based on data compiled in the OCM's recently launched Canadian cyber incidents directory, which currently lists approximately 50 geopolitical and strategic cyber incidents that have directly affected Canada over the past decade. This open access directory and this report have three objectives:

1. ***To better define the phenomenon of geopolitical and strategic cyber incidents and their consequences for Canada.*** As noted in this report, these cyber incidents are more frequent than one might think and take the form of malicious actions by international (often state) actors who use cyber attacks, disinformation, cyber espionage, or data theft for political, military, or economic purposes reasons in their quest for power.

2. ***To help Canadian public officials, the media, the general public, and businesspeople better identify the types of cyber incidents affecting Canada and encourage debate on the strategies and policies needed to prevent cyber incidents and protect Canada's interests in cyberspace.*** The report focuses on three areas where Canada is vulnerable to geopolitical and strategic cyber incidents: (a) cyber espionage against Canadian businesses; (b) disinformation campaigns targeting Canadian governments or interests abroad; and (c) cyber attacks against international organizations of which Canada is a member or host country.

3. ***List the major geopolitical and strategic cyber incidents that have affected Canada in recent years, and provide Canadians with a useful database to predict the type of incidents that may occur in the future.*** Discussing 3 of the 51 cyber incidents identified by the OCM team (cyber espionage activities against the National Research Council of Canada in 2014, disinformation targeting Canadian soldiers in Latvia, and the cyber attack on the International Civil Aviation Organization headquarters in Montreal in 2016), this report provides a preview of the information available in our Canadian cyber incidents directory.

In particular, the directory indicates when the cyber incidents that have affected Canada (public sector, private sector, etc.) took place and who they targeted, their type (cyber espionage, disinformation, etc.), and their origin (China, Russia, North Korea, etc.). The list of identified cases is not exhaustive, but it will be updated regularly by OCM researchers. We encourage Canadians to contact us if they are aware of any geopolitical and strategic cyber incidents that can be added to the directory. The criteria for determining what constitutes a cyber incident that should be included in the directory are presented later in this report.

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. Led by Frédérick Gagnon, a political science professor at Université du Québec à Montréal (UQAM) and holder of the Raoul Dandurand Chair, the OCM brings together Canadian and international researchers studying the new strategies that world actors, especially at the state level, deploy internationally to destabilize states, weaken their societies, institutions and political/electoral processes, or undermine their critical systems and infrastructure. Disinformation, cyber attacks, geo-economic offensives (including economic espionage) and political and electoral interference are some of the phenomena studied by the OCM.

The OCM contributes to the development of a Canadian debate on these issues through publications, conferences, symposiums, and media interventions, informing the public and raising awareness of how contemporary security changes, including the malicious use of digital technologies, affect states such as Canada, their governments, civil society, the private sector, and citizens.

The authors

Frédérick Gagnon holds the Raoul Dandurand Chair and is Director of the OCM and a political science professor at UQAM. He is a recognized expert on 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 geo-economic competition between China and the U.S. on Canada–U.S. relations.

Alexis Rapin holds a degree in international relations from the University of Geneva and a master's degree in international studies from Université de Montréal. A scholar-in-residence at the OCM, he studies the transformations of warfare, such as the rise in disinformation strategies and cyber defence, as well as U.S. politics. He has contributed to a number of books in English and French on armed conflicts and foreign policy.

Danny Gagné is a Ph.D. student in political science at UQAM and a scholar-in-residence at the OCM. His research focuses on American proxy war strategies and foreign interference in civil wars around the world. His recent work at the OCM has been the subject of numerous "Chroniques des nouvelles conflictualités" (published by the Raoul Dandurand Chair) on disinformation during Canadian elections and the power struggle between Washington and Huawei over 5G.

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

Simon Piché-Jacques holds a master's degree in political science from UQAM and is a research associate at the OCM. His research focuses on the involvement of intelligence agencies in emerging conflicts and on Chinese economic espionage against Canada. His recent work at the OCM has led to numerous "Chroniques des nouvelles conflictualités" (published by the Raoul Dandurand Chair) on espionage in Canada's strategic sectors and Russian subversion strategies.

Summary

TOP TEN INCIDENTS

2011

CYBER INTRUSION AT THE TREASURY BOARD

A cyber attack sought to steal access to the Treasury Board, the Department of Finance, and Defence Research and Development Canada. Hackers tried to hijack the computers of senior Canadian government officials in order to steal key passwords that unlock government data systems. A virus was also reportedly installed in computer networks to search for specific documents.

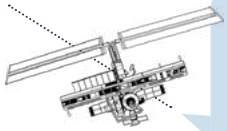
2012

NORTEL REVELATIONS

Chinese economic espionage operations targeted Canadian telecommunications giant Nortel over several years, contributing to its bankruptcy in 2009. Chinese hackers stole passwords from senior executives in order to break into the company's computers. They then retrieved sensitive corporate data through a backdoor. The incident was revealed in February 2012.

2014

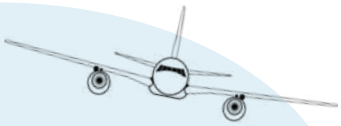
HACKING OF THE NATIONAL RESEARCH COUNCIL OF CANADA



The National Research Council of Canada (NRC) was targeted by a major cyber espionage operation originating in China. A significant amount of sensitive information may have been stolen, as the NRC was working on the development of quantum communication and satellite technologies.

page 16

2016



HACKING OF THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

The computer system of the International Civil Aviation Organization (ICAO) fell victim to a massive cyber attack. Malware was intended to target member states and airlines. Cyber spies accessed the passwords and emails of over 2,000 ICAO system users and may have accessed data on Canadian citizens.

page 24

2016

CYBER ATTACK ON THE WORLD ANTI-DOPING AGENCY

The World Anti-Doping Agency says that a group of Russian hackers accessed its data by hacking into its administration and management system. The group then released confidential medical information about athletes onto the web, including information on seven Canadian athletes. The systems of the Canadian Centre for Ethics in Sport were also compromised. These actions followed revelations in May 2016 of a massive doping campaign involving Russian athletes at the 2014 Sochi Olympic Games. In 2018, the Government of Canada attributed the intrusion to the Russian military intelligence agency.

2017

DISINFORMATION CAMPAIGN AGAINST THE CANADIAN FORCES IN LATVIA

In the wake of the (NATO-led) deployment of 450 Canadian soldiers to Latvia, a wave of fake news was posted in Russian on the web to discredit the contingent's presence. In April 2018, Prime Minister Justin Trudeau officially accused the Russian government of being behind these false rumours.

page 20

2018

SAUDI TROLLING CAMPAIGN

En As a diplomatic crisis played out between Canada and Saudi Arabia, Saudi trolls launched a coordinated Twitter campaign to tarnish the Canadian government's image. The tweets exploited issues such as the treatment of First Nations in Canada and Quebec's sovereignty debate.

2018

OPERATION CLOUD HOPPER

Canada and a number of allied countries blame China for a massive economic cyber espionage campaign. Since at least 2016, Canadian companies have been among the targets of hackers seeking to steal intellectual property and corporate secrets. Information has been stolen from the telecommunications, biotechnology, automotive, and mining industries.

2019

PIPELINE AND IMMIGRATION TROLLING CAMPAIGN

An analysis has revealed that 9.6 million tweets were posted between 2013 and 2019 to shape the narrative on Canadian political issues. Topics included pipeline development in Canada and immigration policies. According to Twitter, the fake accounts behind these tweets were linked to Russia, Venezuela, and Iran.

2020

RUSSIAN CYBER ESPIONAGE RELATED TO COVID-19

Canada, the United Kingdom, and the United States have officially accused Russia of cyber intrusion against their research organizations working on COVID-19. The names of the affected organizations remain unknown, and authorities have not specified whether the intrusions included a cyber attack on a Canadian pharmaceutical company announced in April 2020.

Geopolitical cyber incidents in Canada

Cyber security issues have been making headlines across Canada regularly for many years now. While the majority of incidents involve cyber crime, malicious geopolitical acts originating from adversaries are also on the rise. One could mention China's cyber espionage at the NRC in 2014, the hacking of the Canadian Centre for Ethics in Sport by Russia in 2016, and the cyber attacks on research organizations working on COVID-19 in 2020. Canada has yet to fall victim to cyber incidents as spectacular as those experienced by some other countries. In 2015, for example, Ukraine was the victim of a cyber attack that left 225,000 of its citizens without electricity for several hours. Nevertheless, we see that cyber threats have quietly but steadfastly become part of the daily lives of Canadians.

These events, often seen as isolated incidents, sometimes framed as mostly technical issues and quickly forgotten in the news cycle, are nevertheless part of a diffuse but now pervasive dynamic of international cyber conflict. Whether through industrial espionage, disinformation campaigns, electoral interference, or cyber sabotage, more and more nations are using cyber space to aggressively advance their interests.

> The federal government alone has been subject to close to 2,500 attempted computer intrusions by foreign state actors every year.

Whether or not Canada is a party to this escalation, it is clearly paying the price; in 2017, the Communications Security Establishment revealed, for example, that the federal government alone has been targeted by nearly 2,500 attempted computer intrusions by foreign state actors every year. While the vast majority of them remain inconsequential, a small fraction sometimes results in significant breaches.

The analysis conducted for this report, which is based on open sources and does not claim to be exhaustive, has identified 51 geopolitical cyber incidents that have directly affected Canada over the past decade. What are these cyber incidents? How is their frequency changing? What do we know about their origin? This section is intended to provide a brief overview and an overview of these issues. The information presented here is based on data from the Canadian cyber incidents directory recently launched by the OCM of the Raoul Dandurand Chair. It is based on a specific methodology and classification established by the authors of this report, and readers are encouraged to review it in the "How this report was prepared" section.

What do we mean by cyber incidents?

We define "cyber incidents" as intentional, malicious, time-bound actions carried out at least in part in cyber space. The term cyber incident therefore includes cyber attacks, data theft, and disinformation, among other things (for more details, see the "Typology" section). This analysis focuses on geopolitical or strategic cyber incidents. In other words, the incidents dealt with here are not primarily related to domestic crime, but rather international power relations; they originate most often outside Canada and are mostly orchestrated by foreign governments for military, political, economic, or other purposes.

The incidents discussed here have affected Canada, including its public authorities, the general public, research institutions, and companies or individuals or international organizations based in Canada. Some targeted Canada specifically, while others were aimed at multiple countries including Canada. These incidents date as far back as 2011.

What types of cyber incidents are most common?

Two categories of cyber incidents largely dominate this study. First, the majority of cyber incidents identified in Canada (26 out of 51) appear to be instances of cyber espionage. This category includes several different scenarios. In most cases, intellectual property is stolen—or attempts to steal it are made—from Canadian research institutions or major industrial companies. A good example is the economic cyber espionage campaign Cloud Hopper attributed to China in 2018 (see the "Cyber espionage" section). It also often involves more traditional interstate espionage aimed at collecting confidential government information, like the 2011 cyber intrusion against the Treasury Board of Canada.

Most cyber incidents identified in Canada (26 out of 51) appear to be cases of cyber espionage. This category includes several different scenarios.

The second most frequently observed category is disinformation (or manipulation of information): "the intentional, massive, and coordinated dissemination of false or biased news in cyberspace for hostile political purposes" [translation] (Jeangène Vilmer et al., 2018). There have been at least 17 such events directly involving Canada since 2017. One example is the wave of trolling from Saudi Arabia that occurred in August 2018 as a diplomatic crisis between Ottawa and Riyadh played out. Often these are long-term incidents spread over a certain time. This was the case of a Twitter disinformation campaign uncovered in 2018 and attributed to Russia that exploited a variety of subjects, including the Quebec City mosque mass shooting and the Edmonton vehicle-ramming attack.

How is their frequency evolving?

The data used in this analysis (going back to 2011) show an upward trend in the frequency of cyber incidents. There are essentially two periods. The 2011–2015 period was characterized by an average of two cyber incidents per year, whereas the 2017–2020 period averaged nine incidents per year. It is important to note that much of this rise was driven by acts of disinformation, which has increased overall worldwide since 2016 (see Bradshaw et al., 2021). Note that in the case of espionage or disinformation campaigns, incidents can sometimes span several years, so the year when they started or were publicized is taken as the reference year (see the "How this report was prepared" section).

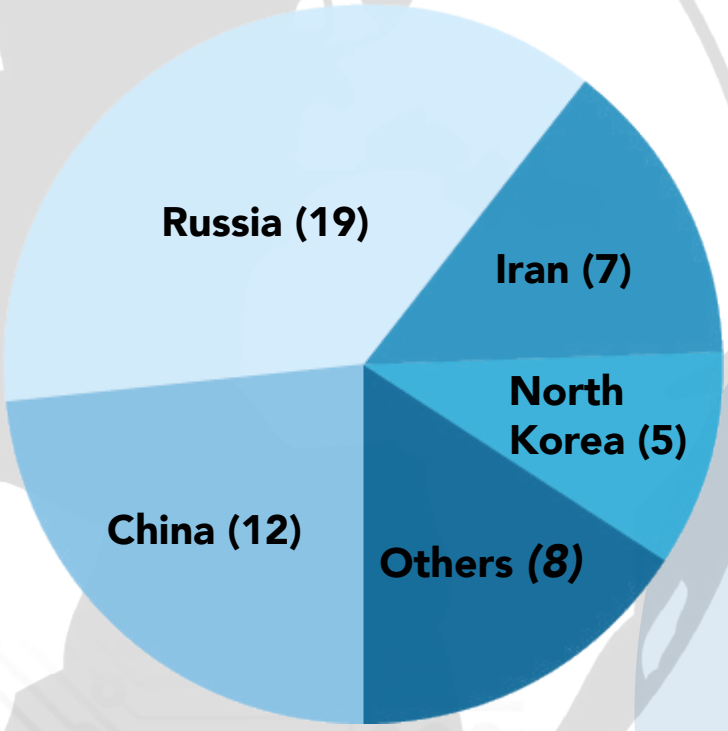
Where do these incidents most often originate?

It is relatively rare that responsibility for a geopolitical cyber incident is strictly and publicly attributed to a specific actor or foreign government. This report therefore focuses more on the geographic origin, by country, of cyber incidents affecting Canada. Only four countries appear to account for

the vast majority of cyber incidents identified in this analysis, namely Russia (19 incidents), China (12), Iran (7), and North Korea (5).

It is important to note, however, that there are significant differences in the types of incidents from each country. The bulk of the incidents from Russia involve disinformation, such as fake news about Canada being disseminated on the web by Russian-based media. Conversely, almost all of the incidents originating in China are related to cyber espionage, most often intellectual property theft. Six cases are still unclear, as their geographic origin remains difficult to establish. Some may have originated in Canada.

Distribution of cyber incidents by country



The tip of the iceberg

The data collected as part of this analysis do not purport to be exhaustive and certainly do not represent the full range of geopolitical cyber incidents that have affected Canada. Many incidents are never publicized, or are publicized very belatedly, for various reasons. Public authorities (in Canada and elsewhere) often prefer to remain quiet about incidents deemed sensitive, such as those involving national security. And the private sector also has strong incentives not to publicize computer breaches, except for certain legal obligations, in order to preserve the image and credibility of the affected companies.

It is therefore important to consider that many incidents remain unknown to the Canadian public at this time and, as a result, have not been identified in this open-source report. The OCM invites readers to bring to its attention any cyber incident that should be added to the Canadian cyber incidents directory to make it as comprehensive as possible.

Three major trends

Beyond raw data, what general observations can be made from the last ten years of cyber incidents? The purpose of this section is to highlight three major trends arising from the incidents identified here: the high prevalence of intellectual property theft, the still very indirect nature of acts of disinformation, and Canada's challenges arising from its status as a "host country" to various international organizations.

CYBER ESPIONAGE

HIGHLY COVETED CANADIAN KNOW-HOW

As the majority of the geopolitical cyber incidents identified in this report involve cyber espionage, a first important finding stands out. This espionage includes, of course, the clandestine pursuit of state secrets, but also, and more importantly, the theft of intellectual property. Foreign hackers have shown that they deeply covet Canadian knowledge, be it scientific research and discoveries or trade and economic secrets. Thus in addition to government bodies, some of the main targets of cyber espionage in Canada (as in many other countries) are universities, research centres, businesses, and other research and development organizations. Some specific areas in particular seem to have been targeted in recent years.

First, we see a strong interest in strategic and military technologies. One example is the 2011 hacking of Defence Research and Development Canada, an agency of the Department of National Defence. This phenomenon appears to be even more pronounced in areas where Canada has cutting-edge expertise, such as aerospace, which was one of the sec-

tors involved in the 2014 hacking of the NRC (see the case study on page 16). A more recent campaign, attributed to China in March 2019 and involving several countries in addition to Canada, was aimed at maritime military technology.

Second, cyber espionage directed at Canadian know-how also appears to extend widely to non-military technology sectors, but which nevertheless have strategic value, such as energy, mining, quantum computing, and information technologies.

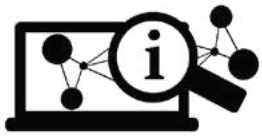
Foreign hackers have shown that they deeply covet Canadian knowledge, be it scientific research and discoveries or trade and economic secrets.

Examples include the cyber espionage attack on the telecommunications firm Nortel publicized in 2012, or the Cloud Hopper cyber espionage campaign publicized in 2018, which reportedly affected a number of Canadian companies. More recently, the pharmaceutical sector and institutions working on a coronavirus vaccine have been priority targets as a result of the COVID-19 pandemic. At least one Canadian pharmaceutical company (whose name has not been revealed) is alleged to have been the target of a cyber espionage attempt in April 2020.

The coronavirus crisis also shows that seemingly secondary economic sectors such as pharmaceutical research can suddenly take on strategic value and thus become a target for foreign powers.

At first glance, the geopolitical nature of intellectual property theft for civil use may not seem obvious. However, cyber espionage is most often attributed to hackers with direct or indirect ties to foreign governments. Many states, including China, consider their economic and technological competitiveness as a national security issue that the state apparatus must actively support. The coronavirus crisis also shows that seemingly secondary economic sectors, such as pharmaceutical research, can suddenly take on highly strategic value and thus become a target for foreign powers.

DISINFORMATION



CANADA AS A TARGET RATHER THAN A TARGET AUDIENCE

While the second most common type of cyber incident identified in this report is disinformation, it is important to note that such actions most often involves Canada indirectly, with many disinformation campaigns talking about Canada, but not aiming primarily to influence Canadian public opinion. It is therefore useful to distinguish between the various disinformation tactics affecting Canada based on their subject (who are they talking about?), their target audience (who are they trying to disinform?) and their purpose (who is the information intended to harm?).

First, there is evidence of efforts—rather limited for the time being—to manipulate information about Canada and aimed at a Canadian audience, most often for the purpose of harming the Canadian state (for example, by disparaging certain controversial public policies). A case in point was the 2018 Russian Twitter disinformation campaign in which a number of fake tweets criticized the Trudeau government's migration policies. Another was the summer 2018 Twitter trolling campaign by Saudi Arabia slamming Canada's record on First Nation human rights, conducted as a diplomatic crisis was unfolding. The overall objective of such efforts is to challenge the legitimacy of government and undermine Canada's social cohesion, but so far they represent a minority of the identified cases.

A second, more frequent approach is to manipulate information about Canada with the aim of harming the Canadian state but not specifically addressing a Canadian audience. For example, there were Russian disinformation campaigns in 2017 and 2018 that relayed fake news about Canadian troops based in Latvia and Ukraine. They were run in the local languages and sought to tarnish the image of the Canadian Forces among the Latvian and Ukrainian populations in order to raise questions about the benefits of their presence (see page 20 for the case study). Such information manipulation appears to be quite common, even though it is not intended to sway public opinion in Canada and therefore attracts less attention. Nevertheless, it harms Canada's image abroad and seeks to influence Canada's foreign policy.

Finally, a third, more ambiguous approach is to refer to Canada, but not for the benefit of a Canadian audience and not necessarily with the aim of harming Canada's interests, at least not on the face of it. This was the case, for example, of false rumours from Russia in 2017 about protests in the Canadian Football League (CFL) at a time when racial controversy was raging in the United States. Another example was a Facebook campaign attributed to Iran in 2018 that featured content mentioning Canada but targeting the United States and Saudi Arabia. Such campaigns seek to stoke controversy in other countries or against other governments and thus appear to speak of Canada only "accidentally."

A HOST COUNTRY

CANADA CAUGHT BETWEEN A ROCK AND A HARD PLACE IN CYBER OPERATIONS

A third noteworthy trend concerns Canada's status as a "host country." Several major cyber incidents identified in this analysis were not directed at Canadians per se, nor were they directed specifically at Canadian interests, but they affected Canada because it is host to entities, individuals, or infrastructure of geopolitical or strategic importance. These incidents therefore demonstrate that rivalries between other states or internal tensions in other countries can occasionally spill beyond their borders and have collateral effects on Canada. There have been a number of such cases.

A first example is state-orchestrated cyber attacks on international organizations based in Canada. This was the case, for example, of the Montreal-based World Anti-Doping Agency, which was hit in 2016 by a cyber attack attributed to Russia, which was said to be retaliating for the doping scandal involving Russian athletes. That same year, ICAO, also headquartered in Montreal, was the victim of a major cyber attack originating in China. The purpose of the operation appeared to be to obtain confidential information held by

the organization and to target member states using ICAO systems. However, it may also have compromised the personal information of Canadian citizens dealing with ICAO (see page 24 for the case study).

Rivalries between other states or internal tensions in other countries can occasionally spill beyond their borders and have collateral effects on Canada.

Some cyber incidents may also involve Canadian residents, or individuals based in Canada, whose personal (including political) activities attract the attention of foreign states. One example is the case of the Saudi dissident Omar Abdulaziz, who was living in Quebec in 2017 when targeted by a clandestine electronic surveillance operation by the Saudi government. Another is a major cyber espionage campaign — Dark Caracal — that came to light in 2018. The Lebanese state is believed to have targeted activists with the campaign, possibly including certain people residing in Canada. Such incidents obviously jeopardize the rights of those involved and more broadly raise questions about respect for Canada's sovereignty.

A third and last example has been very rare thus far but remains a noteworthy scenario: incidents whose final target is a third country, but which affect Canadian infrastructure or systems as a result. In 2019, Canada's electrical infrastructure was reportedly hit by cyber intrusions from Russia whose primary purpose was apparently to assess vulnerabilities in the U.S. power grid. Since the United States and Russia have a highly conflicted relationship in cyberspace and Canada supplies a significant amount of electricity to the United States, Canadian infrastructure is a potential target for Russia. While this was the only such incident identified in this analysis, it does illustrate the risks to computer-controlled critical infrastructures linking Canada and the United States, such as power grids and pipelines.

In the following section, we present three case studies of major cyber incidents which affected Canada in recent years. They are taken from the many cases identified in our Canadian cyber incidents directory and provide concrete, detailed examples of the three major trends presented above.

Photo @ Óðinn

Cutting-edge technologies under Chinese scrutiny: The hacking of the NRC in 2014

On July 23, 2014, the Harper government issued a news release stating that the National Research Council of Canada had been the victim of a major Chinese state-sponsored cyber espionage operation. Ironically, this cyber operation occurred at a time when the NRC was developing a "tamper-resistant" communications system that could prevent such clandestine activities.

July 2014. The relationship between Ottawa and Beijing was strained, to say the least. The Canadian government had been delaying the signing of a major bilateral foreign investment treaty with China (the Foreign Investment Promotion and Protection Agreement, FIPA) and had just imposed new economic sanctions on Chinese state-owned enterprises. In an effort to ease tensions and set the stage for a potential visit to Beijing by Prime Minister Stephen Harper, John Baird, Canada's then-Minister of Foreign Affairs, travelled to China to meet with his counterpart. The diplomatic effort quickly proved to be futile, as the

Treasury Board Secretariat sounded the alarm that the Chinese state had just orchestrated a "highly sophisticated" cyber espionage operation targeting the National Research Council, Canada's innovation and research and development (R&D) backbone.

Vulnerability of Canadian computer systems

According to the official event report, the Canadian government blamed a hostile Chinese-state-sponsored actor for breaching NRC networks through malicious software contained in an email. Hackers could likely have obtained not only sensitive information on ongoing research projects and programs, but also personal data on NRC employees. As soon as the intrusion was detected, the NRC's computer system was shut down. The price tag to restore the institution's networks was a whopping $32.5 million, paid for by the federal government. China, meanwhile, denied the allegations, saying that Canada was making accusations without any shred of evidence.

The price tag to restore the institution's networks was a whopping $32.5 million, paid for by the federal government.

The event raised many questions about how effectively Canada's vital systems were being protected, as the 2011 cyber attacks (also attributed to China) against the Treasury Board and the Department of Finance were still fresh in people's minds. In 2012, the Auditor General, Michael Ferguson, had already pointed out in a report that Canada was lagging behind in critical computer network security and called for the creation of an interdepartmental network to share necessary information in that regard.

Cyber defence: from standard cryptography to quantum cryptography

The specific aims behind the Chinese hackers' intrusion into the NRC networks remain unclear. There are theories, however. At the time of the cyber attack, NRC researchers were working on various technologies of strategic value, notably in relation to satellites and GMOs, as well as quantum computing. This latter sector, the most coveted, focuses on the development of highly sophisticated calculators capable of performing a series of calculations that are completely out of reach of standard computers, even the most powerful ones.

In all likelihood, the cyber attack on the NRC targeted this critical area. According to the Report on the Quantum Canada Symposium and Workshop, a 2017 study by the U.S. consulting firm McKinsey & Company, Canada ranked fifth in the world in terms of investment in quantum science, first in quantum computing, and first among the G7 countries in per capita spending on research. Thus as a leader in the field, Canada naturally piques the curiosity of its competitors.

Why is there so much interest in quantum systems? Because this photonic technology seems destined to shake up many scientific fields in the near future, from medicine to aerospace and telecommunications, prompting many specialists to announce the forthcoming dawn of a "quantum revolution."[1]

A 2017 study by the U.S. consulting firm McKinsey & Company claimed that Canada ranked fifth in the world in terms of investment in quantum science, first in quantum computing, and first among the G7 countries in per capita spending on research.

However, this leap forward comes with its share of risks. The decryption power promised by quantum calculators will likely render most current cryptography mechanisms obsolete. This will make it very difficult to ensure the integrity of a number of critical infrastructures and the confidentiality of many communications. It should nevertheless take until 2030 for these supercomputers to achieve a degree of power that could pose an immediate security threat.

That being said, 2030 is not far off. Knowing that R&D normally takes a lot of time, some states have stepped up their efforts to gain the technology before others. China has already launched its first quantum satellite into orbit (2016) to create the world's first integrated quantum communications network[2]. For its part, Defence Research and Development Canada has just developed a science and technology strategy to maintain its position as a leader in quantum research and allow the Department of National Defence and the Canadian Armed Forces to maintain a certain strategic advantage.

Cutting-edge technology: no time to waste for Beijing

While illustrative, the NRC incident is only one of many similar incidents that have occurred in Canada over the past two decades. China, in particular, has been singled out on numerous occasions for spying on sectors considered strategic: the Nortel case, revealed in 2012, compromised telecommunications network hardware and software; the scandal involving McGill University professor Ishiang Shih in 2018 related to monolithic microwave integrated circuits; and that

1 Unlike a traditional computer, a quantum calculator does not use bits (a binary sequence of 0s and 1s), but rather qubits (an infinite sequence of overlapping combinations of 0s and 1s, including decimals). A system that "thinks" in this way very quickly performs multiple equations, calculations, and operations simultaneously from a mass of information far greater than usual. In terms of cyber security, a quantum communications system offers a seamless cryptography process that ensures the secure transfer of information flows. Quantum communication systems rely on the physical properties of photons rather than computer code. As a result, the photons used to communicate cannot be easily intercepted or decoded between a transmitter and a receiver without the encryption keys.

2 The integrated system consists of over 2,000 km of fibre optic backbone (on the ground) and two ground-to-satellite links, covering a large part of China's land mass..

same year, the affair surrounding LinkOcean involved naval reconnaissance technologies (hydrophones).

China frequently deploys its espionage arsenal to reduce its technological lag, accelerate its trade decoupling strategy, fuel its military-industrial complex, or bypass its reliance on technologies from the West (such as semiconductors). It is still struggling with this dependence, albeit openly, as Xi Jinping himself stated in a 2016 statement, "Our dependence on core technology is the biggest hidden trouble for us."

"Geopolitics is interested in you"

In this ruthless race for new technologies, led primarily by China but including other states as well, Canada has not been left unscathed and has fallen victim to many hidden traps. Already in 2013, the Advanced Threat Report published by the U.S. IT security firm FireEye indicated that Canada was the third most targeted country by advanced persistent threat (APT) computing attacks after the United States and South Korea[3]. Furthermore, according to the Communications Security Establishment, between 2013 and 2015, 2,500 state-sponsored cyber activities were detected by the Canadian government, which is more than 50 per week.

More recently, in February 2021, the Director of the Canadian Security Intelligence Service, David Vigneault, called on Canadian business leaders and academics to be more vigilant about espionage and intellectual property theft, warning that although they might not be interested in geopolitics, "geopolitics is interested in [them]."

Between 2013 and 2015, 2500 state-sponsored cyber activities were detected by the Canadian government.

While espionage is certainly not new, it is now a pervasive threat in any strategic environment where the notion of competition exists. China is well aware of this and is exploiting this new reality. Nothing seems able to slow its ambitions for the time being.

3 The term "advanced persistent threat" (APT) broadly refers to sophisticated and stealthy ("advanced") cyber attacks, during which the authors establish a long-term ("persistent") presence in a targeted computer system. APT also often refers to groups of state-funded hackers pursuing economic and/or geopolitical objectives.

Photo @ U.S. Army Europe

Fake news assault on the Canadian Forces in Latvia

Since 2017, Canadian troops deployed to Latvia as part of a NATO mission have been the subject of repeated, sustained disinformation campaigns. Orchestrated by Russia, these campaigns are primarily intended to tarnish the contingent's image among the local population. Such operations can complicate cooperation or even stoke tensions between Canada and allied countries.

With its modest military potential, limited presence abroad, and international policy focused on multilateralism, Canada may not appear as a first-choice country to be targeted by disinformation campaigns by foreign powers. Yet mainly because of its membership in NATO and participation in NATO activities, Canada is frequently at the receiving end of such acts, which are generally aimed at tarnishing its international image. Since 2017, Canadian troops stationed in Latvia as part of NATO's missions in the Baltic region have been the target of repeated, sustained disinformation campaigns.

Deployed as part of Operation Reassurance, the Canadian contingent (one of the largest deployed overseas) includes 450 soldiers, one

frigate, and a half-dozen CF-18 fighter jets. With some 50,000 Russian troops stationed across the Latvian border, they are but a small contribution and are there largely for deterrence purposes, exercises, and training, as well as to modernize local facilities. However, since their deployment in June 2017, Canadian troops have been targeted by disinformation campaigns orchestrated by Russia that seek to discredit them and disavow their presence.

A well-orchestrated barrage of fake news

In June 2017, four days before Canadian troops were to land in Latvia, a fake news story about Canadian soldiers stationed in Ukraine was published online by three Russian media outlets. According to this news report, 12 Canadian Special Forces members had just been killed in the Donbass region, where a civil war rages between pro-Russian separatists and Ukrainian forces. However, Canadian troops in Ukraine are only there to conduct training missions and are stationed far from the Donbass. The fake news authors backed up their claim with photos of Canadian soldiers carrying a coffin that had actually been taken in Iraq years earlier. Distributed on Russian websites, the content was presumably intended to cast doubt on the merits of Canada's military presence abroad and sow doubts about its peaceful intentions. Did Latvia have to worry about the upcoming Canadian mission?

As the Canadian contingent prepared to set foot in this Baltic country, another fake news story appeared in Russian on a Latvian news site. It stated that Russel Williams, a former Royal Canadian Air Force colonel sentenced to life in prison for a series of murders, was commanding the troops now stationed at the Adazi base. Photos of him in women's underwear, which had surfaced during his trial, were used to condemn alleged sexual deviance within the Canadian Army. Another fake news story came shortly thereafter, stating that NATO troops were circulating with loaded weapons through Riga, the Latvian capital, putting the local population at risk.

Since their deployment in June 2017, Canadian troops have been targeted by disinformation campaigns orchestrated by Russia that seek to discredit them and disavow their presence.

Latvian experts in Russian propaganda saw this as proof that Moscow was now treating Canada the same as other NATO members deployed in the former Soviet republics. Disinformation was indeed a daily reality for German soldiers stationed in Lithuania and British soldiers in Estonia at that time. The Canadian Armed Forces had to learn quickly how to deal with an information minefield. A dozen soldiers were immediately assigned to watch out for and identify propaganda campaigns aimed at the contingent.

Photo @Diego Delso

The end of a battle, but not the war

In the fall of 2017, a new wave of fake news stories surfaced on Russian-language news sites. Among them was an allegation that Canadian soldiers would be housed in luxury apartments at the expense of Latvian taxpayers. It was quickly refuted. Other stories with misleading photos depicted soldiers buying large quantities of alcohol, or forest training sites littered with garbage. However, the images actually showed soldiers from other countries stationed elsewhere or were simply photos taken out of context. The purpose of these actions seems to always be the same: to stir up anger among locals by portraying Canadian soldiers as parasites or troublemakers.

The wave of disinformation targeting the Canadian Armed Forces upon their arrival in Latvia slowed down in the summer of 2018. The Canadian Forces learned important lessons from this. Soldiers now receive training on the risks of disinformation and the contingent also organizes public events to connect with locals and let them observe and better understand the nature of Canadian operations. However, the Russian-language campaigns did not stop completely. In April 2020, misleading contents accused the Canadian troops of spreading COVID-19 and portrayed the Latvian base of Adazi as a hot spot of active cases. The fake news emerged as Canadian soldiers were completing preparations for a NATO military simulation, Exercise Steele Crescendo, which

would have them operate outside the limits of their base. Latvian authorities quickly refuted the information, but the damage had already been done.

In April 2020, several misleading stories accused the Canadian contingent of spreading COVID-19.

Poking a hornet's nest

At first glance, such information operations may seem negligible compared to the scale of NATO's presence in Europe. They are nevertheless taken seriously by Canadian authorities. Latvia is divided between a population that is pro-Western and a Russian-speaking minority that is culturally and politically closer to Moscow. In 2017, Defence Minister Harjit Sajjan shared his concern that Canadian troops might become the target of violence by pro-Russian extremist groups stirred up by Moscow. In 2014, for example, isolated clashes between Latvians and NATO soldiers were instrumentalized by Russian media to further escalate tensions.

This illustrates how the presence of NATO troops in Latvia is a hot button issue. The authorities of the Baltic republic are concerned about the territorial ambitions of its Russian neighbour, and the majority of the population welcomes the presence of the Atlantic Alliance. However, the Russian-speaking community in the eastern part of the country, which represents about 37% of the population, has a different view, often seeing NATO as an occupying force. This minority was fairly supportive of Russia's annexation of Crimea in 2014 and endorses Vladimir Putin's policy of using force to defend Russian-speaking populations in Europe. Riga thus fears that Russia will use the Russian-speaking populations of Latvia to destabilize the country, perhaps for the purpose of a territorial intrusion. This type of strategy preceded the Russian military interventions in Georgia in 2008 and Crimea in 2014.

In addition to these regional geopolitical issues, disinformation campaigns targeting the Canadian contingent in Latvia raise other challenges for Ottawa. The 2017 disinformation campaign, for example, took place less than a year before Latvian parliamentary elections (a recurrent "coincidence" in Russian disinformation campaigns). By sowing controversy over the presence of Canadian troops in the country, these campaigns also seek to make this an election issue and force local politicians to take a stand. In addition to influencing public opinion in the countries in question, such operations may thus hinder cooperation between Canada and allied governments.


Photo @ Jason Thibault

The 2016 cyber attack on ICAO, an international organization based in Montreal

The International Civil Aviation Organization (ICAO) headquartered in Montreal is a United Nations agency, but its mission is more technical in nature than political. There was therefore good reason to believe that it would not be a priority target for interstate cyber espionage. However, in 2016 it was the victim of the worst cyber attack in its history, one that potentially put Canadians' personal data at risk.

ICAO is a specialized agency of the United Nations (UN) where 193 member countries work together every day. Created in Montreal in 1944, it is responsible for the regulatory framework governing international civil aviation safety. It oversees the transport of people and goods by air worldwide and strongly influences the development of international policies and rules aimed at air transport standardization. It has between 800 and 1,000 international employees, most of whom are based in Montreal.

As a highly technical international organization, it would not appear to be of particular strategic interest to state-sponsored hackers.

In 2016, however, ICAO was notified that two of its servers had been breached. It was far from suspecting it at the time, but it was on the verge of being hit by the most serious cyber attack in its history.

A contaminated "watering hole"

The alarm was sounded on November 22, 2016, by a cyber intelligence analyst working for the American defence and security firm Lockheed Martin. Not mincing words, he called the attack "a significant threat to the aviation industry." This cyber attack targeted two of the international organization's servers and put at risk the many users and institutions that access the ICAO's digital platform every hour. A Turkish government site was also infected, which is how the cyber attack came to light.

With the breach now detected, the investigation was transferred internally for analysis by Secureworks, a U.S.-based cyber security firm employed by the UN. The analysis was worrying: the hackers appeared to have infiltrated two of the organization's email servers and to have been hibernating there for a long time. The hackers had flown under the radar through a watering hole attack, a technique well known to cyber security analysts.

As its name suggests, a "watering hole" attack consists of booby-trapping a first user's system, which then infects external visitors or users of that system (who "drink" from the contaminated watering hole). More specifically, it involves putting malware on a


Photo @Jeangagnon

site, usually outside of the company's security safeguards, to be visited by the targeted individuals. The victims become infected in turn and spread the malware further. These attacks are complex, as the infected websites generally belong to trusted entities, such as business partners, whose servers' security is usually not questionable.

As its name suggests, a "watering hole" attack consists of booby-trapping a first user's system, which then infects external visitors or users of that system (who "drink" from the contaminated watering hole).

Attackers armed with patience

While familiar, this type of attack is not particularly frequent, mainly because it requires a great deal of patience on the part of the hackers. Watering hole attacks are a significant threat, however, as they are difficult to detect. Another major issue in managing this type of cyber attack is employee training. While it is easy to train employees to recognize and avoid phishing[1] emails, there is no way for an ordinary user to identify a compromised website without a specifically designed tool.

This appears to have been the main issue in the cyber attack on ICAO, whose email servers served as the main watering hole. The hackers quietly infiltrated the servers and were lying in wait for months before being detected. As a generator of abundant Internet traffic from many countries, ICAO was the ideal target for a watering hole attack. In all likelihood, the purpose of the infiltration was cyber espionage. ICAO was therefore a logical choice, particularly since it serves as a gateway to other players in the aerospace industry, which allowed the hackers to access more data for the purpose of stealing intellectual property.

A typical pattern for Emissary Panda

Who should be blamed for this cyber attack? A preliminary analysis by Secureworks found that it was the work of the Chinese hackers group Emissary Panda. This was not the first foray of the group, which has been active since 2010 and is also known as APT27, Lucky-Mouse, Threat Group 3390, and Bronze Union. Emissary Panda had previously conducted significant intellectual property theft operations, targeting major organizations in North and South America, Europe, and the Middle East. It regularly targets the aerospace, defence, technology, energy, and finance sectors.

A Secureworks report states that Emissary Panda is located in the People's Republic of China, and it seems plausible that it is subsidized and supported by the Chinese

1 Phishing is a technique used by computer fraudsters to obtain access or personal information for the purpose of identity theft or to break into a computer system. It most often comes in the form of fraudulent emails that try to fool the user by mimicking a legitimate email.

government. The group is characterized by its tendency to compromise Microsoft Exchange servers, notably through the use of backdoors and the theft of identification credentials. It is also known for its long-haul cyber espionage campaigns, lying low on servers for extended times before exfiltrating data, which was the pattern in ICAO's case. The group uses this time to seek out other access points, learn how the network is structured, and identify important data.

A long-running cyber attack with unknown consequences

While ICAO did not confirm what exactly had been stolen, it is likely that the cyber attack compromised a number of commonly used aviation documents on its website, enabling hackers to get information from a wide range of aviation and government organizations around the world. Further details of the attack surfaced in 2019, suggesting that email server accounts as well as domain and system administrator accounts were affected. The scheme reportedly allowed hackers to access the credentials and passwords of over 2,000 system users.

Notably for Canada, the hackers may also have had access to employees' employment records, the medical records of patients who used the ICAO headquarters clinic, the financial transaction records of companies dealing with ICAO, and the personal information of anyone who had physically visited ICAO premises in Montreal.

The scheme reportedly allowed hackers to access the credentials and passwords of over 2,000 system users.

It is therefore plausible to imagine that some data on Canadian residents were compromised during the attack. The incident shows the importance of Canada's status as "host country" in terms of cyber security; a cyber attack targeting an international organization can have collateral effects for Canada.

How this report was prepared

The data and cases presented in this report are taken directly from the Canadian cyber incidents directory developed 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 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 2011. 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. The incidents originate most often 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 of incidents and their definitions

The Canadian cyber incidents directory on which this report is based identifies eight categories of geopolitical cyber incidents. This typology centres 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 maintained by the Council on Foreign Relations, an American think tank, and on other sources listed below. The following are specific definitions for each type of incident.

CYBER ESPIONAGE : The act of obtaining information through digital means without the information holder's prior consent. This category includes, for example, 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 defences or vulnerabilities, such as in anticipation of future actions.

DISINFORMATION : 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 all or part of an infrastructure, or to interrupt the operation of a computer-controlled system for an extended period.

Dates and origin of incidents

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

The date we assign to a cyber incident may refer to when the incident actually took place or when it was publicized. We prefer the first approach, but the exact start date of an incident often cannot be determined. This is particularly true of waves of cyber espionage, which are stealthy by nature, and disinformation campaigns extending over long periods of time. In such cases, we use 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 (political) responsibility for it. We give pre-eminence to geographic data in this report because they are technically easier to establish and because it is quite rare that responsibility for a cyber incident is publicly attributed. In either case, 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 the online directory for more details on the origin of each incident.

What sources are the directory and report based on?

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.

Further reading

The "chroniques des nouvelles conflictualités" of the Center on Multidimensional Conflicts (Observatoire des conflits multidimensionnels or OCM) of the Raoul-Dandurand Chair provide a bimonthly analysis of current events relating to contemporary strategic issues in cyber security, disinformation, political and electoral interference, and geo-economics.

Other online cyber incident databases and resources

Cyber Operations Tracker : This comprehensive database captures a large proportion of the state-sponsored cyber operations that have taken place around the world since 2005. It is maintained by the Digital and Cyberspace Policy Program of the Council on Foreign Relations, an American think tank. Its methodology inspired that of our Canadian cyber incidents directory.
https://www.cfr.org/cyber-operations/

Significant Cyber Incidents : More of a timeline than a database, this online registry is nevertheless a very useful archive of major cyber incidents that have occurred since 2006. It is maintained by the Center for Strategic and International Studies, an American think tank. It also inspired our directory and report.
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Live Cyber Threat Map : Many firms maintain real-time maps of cyber attacks (or attempted attacks) occurring around the world. The ThreatCloud map is not necessarily the most advanced or detailed, but it is very comprehensive and intuitive, providing an instant look at attacks occurring worldwide over the Internet. https://threatmap.checkpoint.com/

References on cyber issues

Wired : The "Security" section of this renowned U.S. online magazine offers high-quality coverage of U.S. and international cyber news through feature articles and in-depth investigations with contributions from some of the best writers in the field.
https://www.wired.com/category/security/

CyberScoop : Akin to a "cyber security news agency", CyberScoop offers readers a fast, accessible, and thorough digest of cyber news, whether on international security, cyber crime or cyber security policy developments. https://www.cyberscoop.com/

IT World Canada : Mainly aimed at information technology professionals, this small, specialized site offers a uniquely Canadian approach to cyber news.
https://www.itworldcanada.com/

Vygl le balado : This podcast, produced by the Quebec cyber security agency Vygl, offers an insightful and relaxed look at cyber security news. It is one of the few of its kind in French.
https://vyglbalado.libsyn.com/

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