Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

The cyber threat to research laboratories

Canada

About this document

Audience

This report is part of a series of cyber threat assessments focused on advice about the cyber threats to Canada's critical infrastructure. It is intended for leaders in the life sciences and biomanufacturing sectors, cyber security professionals with laboratory infrastructure to protect, and the general reader with an interest in the cyber security of critical infrastructure. For guidance on technical mitigation of these threats, see consult the Canadian Centre for Cyber Security's (Cyber Centre) guidance or contact the Cyber Centre.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information, see Traffic Light Protocol.

Contact

For follow-up questions or issues please contact the Cyber Centre at contact@cyber.gc.ca.

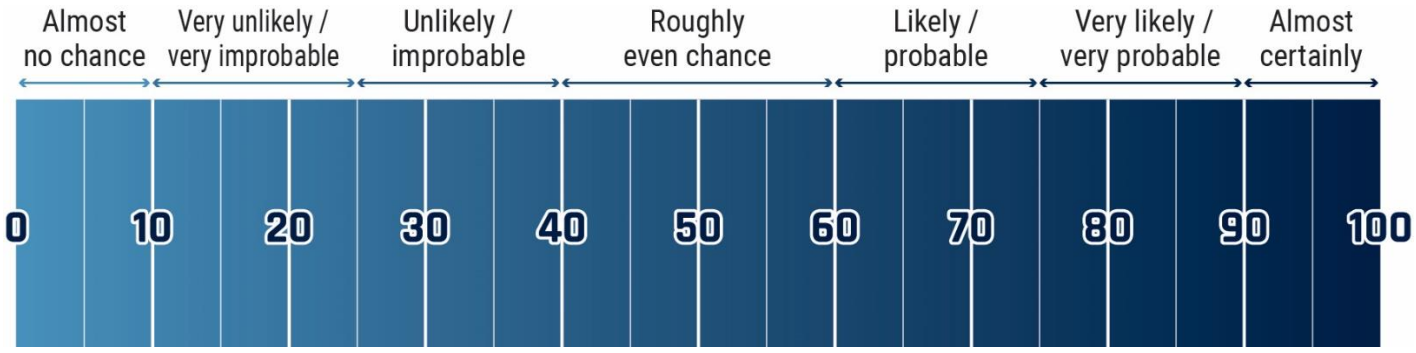
Assessment base and methodology

The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Cyber Centre. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. The Communications Security Establishment's foreign intelligence mandate provides us with valuable insight into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The assessments and analysis are based on information available as of November 30th, 2023.

Estimative language guide



Key judgements

- We assess that financially motivated cybercriminals are the most likely cyber threat to impact laboratory networks and devices through ransomware deployment and extortion for payment or through theft and sale of personal or proprietary information.
- We assess that state-sponsored actors will very likely continue to target Canadian laboratories to support their domestic biopharmaceutical and biomanufacturing capabilities through espionage. Further, we assess that People's Republic of China (PRC) state-sponsored actors are almost certainly the most significant state-sponsored threat to laboratories in Canada.
- We assess that state-sponsored actors will almost certainly target laboratories conducting research related to a foreign state's critical intelligence requirements or a perceived existential threat for espionage or disruption.
- We assess that state-sponsored actors will almost certainly use disinformation campaigns to target laboratories conducting research with the potential to cause reputational damage to foreign states. These campaigns may involve laboratory network compromise and the exfiltration, modification and release of sensitive information.
- We assess there to be an even chance that laboratories will be affected by low sophistication cyber activity such as distributed denial-of-service attacks (DDoS) by hacktivists that are unlikely to disrupt laboratory operations.

Introduction

Medical and life science research is an important part of the Canadian economy and an essential contributor to Canada's national security and health security. In addition to contributing $89.6 billion to Canada's GDP in 2022, medical and life science research creates new vaccines and therapeutics that improve Canada's resilience to public health crises. Canadian researchers are well known internationally for the discovery of insulin, their work developing an Ebola vaccine, and for successfully isolating and cultivating the virus responsible for COVID-19, paving the way for additional vaccine research.[1]

Canadian biological research laboratories, meaning laboratories that work with human or animal pathogens and toxins, have made important contributions to Canada and the global research community. The value of Canadian laboratory research makes the laboratories themselves compelling targets for cyber threat activity. Throughout the COVID-19 pandemic, the Cyber Centre observed a large volume of threat activity by both state-sponsored actors and cybercriminals against healthcare organizations and other organizations within the vaccine supply chain, including laboratories.[2]

Following the COVID-19 pandemic, laboratories, universities and research centres continue to be targeted by state-sponsored actors for espionage and victimized by cybercriminals for financial gain. At the same time, the systems laboratories rely on to safely study dangerous pathogens and toxins have become increasingly digitally transformed and integrated with information technology, and thus more vulnerable to cyber interference.[3]

Cyber threat activity against Canadian laboratories threatens Canada's research advantage, including through theft of proprietary information or disruptions to laboratory operations. Disruptions may lead to loss of research information, loss of containment and exposure of laboratory personnel or communities to biohazardous material.

Laboratory cyber threat surface

Medical and life science research is conducted in publicly and privately operated laboratories across Canada. These laboratories produce, store, manipulate and study pathogens and toxins, including those that pose a significant risk to researchers and the broader community if not properly contained. Laboratories rely on procedural and physical containment measures to safely conduct their work, which are implemented in accordance with the containment level (CL). Laboratory spaces licenced to work with Security Sensitive Biological Agents (SSBAs) include additional access controls and security screening for laboratory personnel.

Laboratory equipment and systems are becoming increasingly complex and interconnected. In addition to the introduction of connected building management systems for electrical, air handling and access control, laboratory research devices and containment systems are becoming digitally transformed. Connecting these systems provides benefits for laboratory operators, but also introduces the potential for cyber threat actors to compromise and interfere with those systems.

Key terms	
Containment level (CL)	Containment level describes the minimum physical safeguards that a laboratory requires for the safe handling of potentially hazardous biological material. There are four containment levels (CL1 to CL4) ranging from basic laboratories for work with biological material to sophisticated facilities for work with the highest-risk group of pathogens.[4]
Security Sensitive Biological Agents (SSBAs)	SSBAs are a subset of pathogens and toxins that have increased dual-use potential for legitimate scientific applications and misuse as biological weapons.

Laboratory research devices

Researchers rely on a myriad of research equipment to manipulate and study pathogens and toxins, including genome mapping machines, electron microscopes, centrifuges and more. Increasingly, this equipment is becoming connected and networked. Over the past two decades, there has been a "data deluge" in laboratory research stemming from the large amounts of data generated by research devices. To accommodate this influx of data, laboratories may maintain a dedicated science informatics network that allows for the transfer, storage and processing of research data.[5]

If threat actors compromise these networks, for example by exploiting insufficient network segmentation, they may be able to interact with and manipulate the devices on the network. By accessing these devices, threat actors can force them to operate in unintended ways, steal or manipulate research results, or steal other proprietary information such as the project files that guide a device's operation.

Containment systems

Laboratories rely on a complex arrangement of operational technology to create and maintain containment while studying pathogens and toxins. These systems include:

- ventilation systems to maintain air pressure differentials between higher and lower containment areas, maintaining inward airflow to higher containment zones
- effluent decontamination systems
- tools such as biosafety cabinets and autoclaves

While digital transformation of these devices can provide benefits to laboratory operators, such as remote control and monitoring, it also opens those systems to possible interference from cyber threat actors. Disruptions to containment systems can cause operational interruptions or a containment breach leading to personnel or community exposure to dangerous pathogens or toxins.

The threat from cybercriminals

We assess that laboratories are most likely to be victimized by cybercriminals through ransomware deployment and extortion or theft and sale of personal or proprietary information. Cybercriminals opportunistically victimize organizations and exploit them for financial gain. Laboratories support several sectors that experience higher than average cybercriminal activity, including healthcare and academia, increasing the potential for incidental exposure to cybercriminal activity and exploitation. Laboratories are a compelling victim for cybercriminal activity because of the value of the information they contain and their vulnerability to extortion tied to operational disruptions.

The evolving cyber crime ecosystem

The cyber crime ecosystem is continuously evolving to become more efficient, specialized and profitable. Cybercriminals interact through illicit marketplaces and forums to connect buyers and sellers of tools, services or network accesses. An illustrative example of this development is the **ransomware-as-a-service (RaaS) supply chain**.

The ransomware-as-a-service supply chain

Most ransomware attacks against Canadian organizations are very likely linked to RaaS groups. RaaS groups develop and maintain ransomware and lease it to other cybercriminals in exchange for payment.[6] Other cybercriminals contribute to this supply chain by offering specialized services such as selling network access, communicating with victims, laundering ransom payments and more. In 2021, a laboratory's network was compromised and its systems encrypted by ransomware after a student downloaded pirated data visualization software. Security researchers assessed it was likely the actor that gained access to the network through the pirated software and sold the access to a different cybercriminal who then deployed ransomware.[7] The laboratory lost a week of research data and their systems and networks had to be entirely rebuilt.[8]

We judge that the RaaS system and the overall increasing availability of malicious cyber tools, lower the barrier to entry for cybercriminals and increases their ability to conduct disruptive attacks against victim organizations.

Ransomware: Encrypting data or devices and holding them for ransom

Ransomware continues to be the most disruptive threat to Canadian organizations, including laboratories. Cybercriminals typically apply at least two methods of extortion against their victims when deploying ransomware. The first method is often device or file encryption, and the second is often data exfiltration and threatening to publicly release organizational data if ransom demands are not met.[9]

Ransomware can be costly to victim organizations even aside from the cost of remediating infected systems. Ransomware can interrupt key business and operational processes, which can translate to loss in laboratory research productivity and loss of research data and results. In 2020, a United States clinical laboratory was victim to a ransomware attack that caused systems to be inaccessible for almost a month, forcing research work to be conducted on paper and causing research delays.[10]

In addition to impacting information technology (IT) systems, ransomware may directly or indirectly impact operational technology (OT), such as laboratory research devices and containment systems. Some cybercriminal groups deploy ransomware variants that specifically target OT, and even IT-isolated ransomware incidents can impact an organization's ability to monitor or control their OT, forcing shutdowns.[11] A ransomware attack against critical laboratory containment systems could result in loss of containment, resulting in personnel or community exposure to dangerous pathogens or toxins.

Data exfiltration: Stealing information for sale or exploitation

Laboratory networks contain various forms of information that can be valuable to cybercriminals, including the personal information of employees or patients, information on suppliers and partners, and proprietary or sensitive business information. Such information can be used to conduct additional fraudulent activity against the laboratory, laboratory staff or its partners. Data exfiltration may also be used as a lever to extort victim organizations for ransom payment, both instead of and in addition to traditional ransomware device encryption. Stolen organizational data is also often posted for sale on criminal marketplaces, allowing other cybercriminals to acquire data for their own fraudulent or exploitative purposes. This also provides an opportunity for nation states and commercial competitors to acquire illicitly collected proprietary information without themselves engaging in cyber threat activity.

The threat from state-sponsored actors

State-sponsored cyber threat activity against research facilities, including laboratories, peaked during the COVID-19 pandemic. During this time, foreign state intelligence services reallocated sophisticated cyber capabilities from other efforts to collect information on Western vaccine development and public health measures.[12] Many countries continue to prioritize improving their domestic biopharmaceutical and biomanufacturing capacity, in some cases including by collecting information through cyber threat activity. Additionally, laboratories involved in geopolitically-significant research, especially where key state interests are implicated, are compelling targets for cyber activity designed to steal or modify research findings or create disinformation around the research.

Cyber Centre publications related to COVID-19

- Cyber threat bulletin: The continued impact of COVID-19 on cyber threat activity
- Cyber threat bulletin: Impact of COVID-19 on cyber threats to the health sector
- Cyber threat bulletin: Impact of COVID-19 on cyber threat activity
- Cyber security advice and guidance for research and development organizations during COVID-19

Economic and research espionage: Stealing Canadian research and intellectual property

We assess that state-sponsored actors will very likely continue to target Canadian laboratories to support their domestic biopharmaceutical and biomanufacturing capabilities through espionage. Laboratory research capacity is a limited resource, particularly for laboratories operating at the CL3 or CL4 level or working with SSBAs.[13] Theft of proprietary information derived from laboratories is a cost-efficient method of obtaining valuable research without making significant investment into domestic research capabilities.

Laboratories contain a myriad of information that can be used to support foreign state bioresearch capabilities and undermine Canadian economic interests. Advanced research across sectors is a common target for espionage. State-sponsored actors frequently conduct spear-phishing campaigns against Western researchers, including within the biopharmaceutical and biomanufacturing sectors. We assess that PRC state-sponsored actors are the most significant state-sponsored threat to laboratories in Canada. The PRC has robust domestic biopharmaceutical and biomanufacturing capacities and a history of using stolen intellectual property to provide competitive advantage.[14] In addition to commercially focused espionage, we assess it likely that state-sponsored actors have an interest in stealing dual-use research information, including information related to SSBAs, with defensive or offensive military utility.

Issue-specific compromise: Motoring or manipulating globally-significant research

We assess that state-sponsored actors will almost certainly target laboratories conducting research related to that state's critical intelligence requirements or a perceived existential threat for espionage or disruption. Laboratories contribute to research and other forms of testing that have significant geopolitical implications for foreign states, for example responses to shared public health crisis or biological and chemical weapons non-proliferation testing. We assess laboratories involved in such research, for example in relation to the COVID-19 pandemic, will almost certainly attract sophisticated, risk-tolerant state-sponsored threat activity intended to steal, manipulate or destroy research information. In 2018, Russian state-sponsored actors planned to compromise a Swiss laboratory conducting tests related to the Skripal poisoning in the United Kingdom and alleged Russian chemical weapons use in Syria.[15] The operation was intended to include a combination of physical laboratory access and cyber exploitation but was prevented by Dutch and Swiss authorities.

Disinformation: Controlling international narratives and undermining Canadian research credibility

We assess that state-sponsored actors will almost certainly use disinformation campaigns to target laboratories involved in research with the potential to cause reputational damage to foreign states. These campaigns may involve laboratory network compromise and the exfiltration, modification and release of sensitive information. Where key state interests are implicated, nation states may use hack and leak operations to refute laboratory findings and support the state's disinformation campaigns. These operations can include theft and subsequent public release of sensitive information that has been modified or presented out of context to undermine the legitimacy of the findings. Internationally sourced disinformation has been observed influencing domestic misinformation around biological research.[16] Disinformation themes may question the findings' legitimacy, allege equal or greater wrongdoing by the West, or undermine confidence in the safety and security of laboratory operations.

Following the 2016 ban on Russian athletes participating in the summer Olympics after findings that they were systematically providing their athletes performance-enhancing drugs, Russian state-sponsored actors targeted anti-doping agencies worldwide, including the World Anti-Doping Agency in Montreal and the Canadian Centre for Ethics in Sports (CCES).[17] CCES networks were compromised after Russian hackers conducted a close-access operation targeting senior officials attending a conference abroad. Once the CCES networks were compromised, the hackers exfiltrated sensitive information including confidential medical information on athletes, such as waivers for consuming normally prohibited substances.[18] Stolen information was both published online and incorporated into misinformation campaigns. In some instances, social engineering was used to trick journalists into publishing manipulated information as fact.

Foreign ownership

Foreign ownership of laboratories or key support organizations, including suppliers contracted to provide material, expertise or services during laboratory construction and operation, provides an additional threat vector that may be exploited by state-sponsored actors. We assess with almost certainty that the PRC and Russia have the capacity to compel their researchers and domestic industry to cooperate with intelligence collection efforts and act against the interest of the contracting Canadian organizations.[19] Cooperation may be compelled through lawful access programs that target sensitive information transferred through or stored within their jurisdiction. It may also be compelled more broadly through extrajudicial coercion that may include direct provisioning of research information by foreign-owned laboratories within Canada to foreign states. We assess that, given the opportunity, the PRC and Russia will very likely attempt to use foreign ownership connections to steal proprietary information from laboratories or gain access to laboratory networks.

Hacktivists and terrorists

We assess it unlikely that terrorist groups will target laboratories through cyber means for data exfiltration or to cause operational disruptions. Terrorist groups may have an interest in collecting information in relation to SSBAs and their application for biological weapons as a tool to advance their ideological objectives. However, we are not currently aware of groups with the requisite sophistication and intent to do so through cyber compromise against laboratories.

We assess there to be an even chance that laboratories will be affected by low sophistication cyber activity such as DDoS by hacktivists that are unlikely to disrupt laboratory operations. Pro-Russian hacktivists have targeted Western critical infrastructure since the start of the Russian invasion of Ukraine with low sophistication cyber activity intended to intimidate and undermine support for Ukraine. This activity primarily includes techniques such as DDoS attacks against the public facing websites of highly visible critical infrastructure organizations. For example, in April 2023, pro-Russian hacktivists conducted DDoS attacks against Canadian critical infrastructure and government websites, including the Prime Minister's website.[20]

Outlook

Cyber compromise of laboratories can have significant implications for Canada's physical, economic and national security. Theft of proprietary information threatens Canada's research advantage. The increased connectivity of the OT involved in laboratory research and maintaining containment increases the opportunity for cyber compromise to have physical impacts, including exposure of laboratory staff and the wider community to deadly, virulent pathogens and toxins.

Many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. The Cyber Centre encourages all critical infrastructure network owners, including those responsible for laboratory networks, to take appropriate measures to protect your systems against the cyber threats detailed in this assessment.

Please refer to the following online resources for more information and for useful advice and guidance:

- Introduction to the Cyber Threat Environment
- National Cyber Threat Assessments
- Baseline cyber threat assessment: Cybercrime
- Cyber threat bulletin: Cyber threat to operational technology
- Ransomware playbook (ITSM.00.099)
- Defending against data exfiltration threats (ITSM.40.110)

- Security considerations for research and development (ITSAP.00.130)
- Protect your medical research equipment from cyber threats (ITSAP.00.134)
- Social engineering (ITSAP.00.166)

[1] Nicole Bogart. "Canadian scientists make COVID-19 research breakthrough, isolating virus". CTV News. March 13, 2020.

[2] Canadian Centre for Cyber Security. "Cyber threat bulletin: The continued impact of COVID-19 on cyber threat activity". December 21, 2020.

[3] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023-2024". October 28, 2022.

[4] Public Health Agency of Canada. "Canadian Biosafety Standard, Third Edition". Section 1.3.6.4. November 24, 2022.

[5] Gordon Bell, Tony Hey, and Alex Szalay. "Beyond the Data Deluge". Science 323:5919. March 6, 2009; for example, see Steven R. Spurgeon et al. "Towards data-driven next-generation transmission electron microscopy". Natural Materials 20:3. 2021.

[6] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023 – 2024". October 28, 2022. Page 7.

[7] Tilly Travers. "MTR in Real Time: Pirates pave way for Ryuk ransomware". Sophos. May 6, 2021.

[8] Tilly Travers. "MTR in Real Time: Pirates pave way for Ryuk ransomware". Sophos. May 6, 2021.

[9] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023 – 2024". October 2022.

[10] Toby Cornish, David McClintock. "Are you Prepared? Laboratory Downtime in the Ransomware Era". American Journal of Clinical Pathology 157:4. April 2022.

[11] TrendMicro. "IoT and Ransomware: A Recipe for Disruption". September 28, 2021.; See also, David Sanger, Clifford Krauss, Nicole Perlroth. "Cyberattack Forces a Shutdown of a Top U.S. Pipeline". The New York Times. May 8, 2021.

[12] Canadian Centre for Cyber Security. "Cyber threat bulletin: The continued impact of COVID-19 on cyber threat activity". December 21, 2021.

[13] King's College London. "Global BioLabs Report 2023". March 15, 2023.

[14] Alex Keown. "Extradited Scientist Found Guilty of Stealing GSK Secrets". BioSpace. May 3, 2022.

[15] Sean Gallagher. "Russians tried to hack Swiss lab testing samples from Skripal attack". Ars Technica. September 17, 2018.

[16] Karen Pauls, Jeff Yates. "Online claims that Chinese scientists stole coronavirus from Winnipeg lab have 'no factual basis'". CBC. January 27, 2020; Justin Ling. "How 'Ukraine bioweapons labs' myth went from QAnon fringe to Fox News". The Guardian. March 18, 2020.

[17] Murray Brewster. "Canadian agency astonished to be targeted by alleged Russian cyberattack". CBC. October 5, 2018.

[18] Andy Greenberg. "How Russian spies infiltrated hotel Wi-Fi to hack their victims up close". Wired. October 4, 2018.

[19] Canadian Centre for Cyber Security. "The Cyber Threat from Supply Chains". February 8, 2023.

[20] Communications Security Establishment. "Statement from the Minister of National Defence – Cyber Threats to Critical Infrastructure". April 13, 2023; Rachel Aiello. "Russia being able to 'bring down' Canadian gov't websites won't dissuade support for Ukraine: Trudeau". CTV News. April 11, 2023.

CAT. D96-108/2024E-PDF
ISBN 978-0-660-70775-4

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada