PHISHER, HACKER, ATOMIC SPY

Insider Threat in the Canadian Nuclear Industry

Abstract

Incidents of insider threats are on the rise in Canadian critical infrastructure, primarily due to the increased digitalization of the workplace, as well as the deterioration of the socioeconomic and geopolitical landscape. Meanwhile, the reemerging nuclear industry is drawing significant interest from threat actors who view it as a lucrative and strategic target for financial gain, intellectual property theft, as a vector to conduct coercive diplomacy, or as a hostage to promote their ideologies. With insider threat representing the primary attack vector in the majority of data breaches, an incident of that nature in the Canadian nuclear industry would rapidly evolve into a matter of national and international security.

This research presents the findings of an industry-wide threat assessment, which revealed that Canada's legislative and nuclear regulatory framework lacks adequate measures to protect against insider threats. The absence or partial implementation of effective safeguards leaves the industry at a high risk of insider-initiated attacks.

The assessment identified five key vulnerabilities that threat actors can exploit to jeopardize the safe and sustained delivery of the industry's critical services: poor cybersecurity security governance, human factors limitations, insufficient regulatory due diligence, lack of legal precedents, and limitations associated with third-party risk management. Seven pragmatic recommendations were identified.

Audrey Crowe

Carleton University - Masters of Infrastructure Protection & International Security

Table of Contents

Hacker, Phisher, Atomic Spy: Insider Threat in the Canadian Nuclear Industry

Klaus Nielsen, Wei Ling Yu, Jeffrey Deslisle, Qing Quentin Huang, Cameron Ortis, Sébastien Boulanger-Dorval, Sébastien Vachon-Desjardins, Xiangguo Qiu, Kending Cheng, Yantai Gan, Yue-Sheng Wang, William Majcher, Kenneth Marsh, and most recently, James Mousaly. These names have rarely been listed next to one another in an open-source document, yet they all have something in common. These individuals all have been charged with or convicted of theft of intellectual property (IP), breach of the *Security of Information Act* (SOIA), breach of trust, fraud, and trafficking of identity information. They represent more than a decade of insider threat in Canadian critical infrastructure (CI).

Cases of insider threat have increased over the past decade, driven in part by the digitalization of the workplace, a trend accelerated by the COVID-19 pandemic, as well as the deterioration of the sociopolitical and geopolitical landscape. Recognizing value and vulnerabilities, threat actors are increasingly targeting CI sectors to achieve their respective financial, ideological, defence or strategic objectives (Canadian Centre for Cyber Security [CCCS], 2020, 2022, 2024). This trend is expected to worsen as the nature of warfare continues to migrate from the physical to the cyber battlefield. Cyberattacks have become common currency for state actors, criminal organizations, ideologically motivated violent extremists, and lone wolves. They level the playing field by allowing threat actors to conduct cost-effective, military-grade, non-lethal operations across borders while being protected by plausible deniability within the safety of their own jurisdictions.

In parallel, the nuclear industry has seen a global re-emergence over the same decade due to its ability to provide clean, sustainable energy. The industry is seeing a significant influx of investment and has become one of the fastest-growing sources of energy globally (International Energy Agency, 2024). This trend is set to accelerate as 22 nations committed at COP28 to triple global nuclear energy output by 2050, signaling a significant global shift toward nuclear power. This commitment relies on the modernization of aging nuclear infrastructure, advancing research and development of new nuclear technologies, and will expand the reliance on uranium mining and manufacturing.

The nuclear industry holds a unique position within the Canadian CI. Its services span across four distinct yet interdependent sectors with varying regulatory oversight: energy, health, manufacturing, and government. As a global industry leader, Canada is a prime target for threat actors, and its employees are facing a growing risk of recruitment, coercion, and exploitation. These insiders hold valuable access to critical and safeguarded facilities, information and nuclear materials. This access and knowledge are particularly valuable to threat actors seeking to achieve financial gains, develop clandestine nuclear capabilities, or to exert pressure by engaging in coercive diplomacy.

Considering the virulent threat landscape and the rapid digital transformation of the nuclear industry, a case of insider threats in the nuclear industry would have severe national and international security impacts. With insider threats representing the primary attack vector in over 75% of data breaches (IBM Security, 2024; Ponemon Institute, 2023), the Canadian legislative and nuclear regulatory framework is ill equipped to safeguard the industry against such risks. While the framework provides generally adequate governance and requirements for the *physical* protection of nuclear materials, multiple concerns have been raised over the pressing need to strengthen cybersecurity measures within the industry. The Communications Security Establishment (CSE) has issued multiple warnings to CI sectors about being actively targeted by sophisticated threat actors. Meanwhile, a decade ago, the International Atomic Energy Agency (IAEA) advised the Canadian nuclear regulator to extend its cybersecurity requirements to vulnerable nuclear facilities (International Atomic Energy Agency [IAEA], 2016). Yet, as of 2025, the

Canadian nuclear industry still lacks a legislative and regulatory framework that comprehensively protects *all* license holders (also referred to as "*licensees*").

As the federal government and the Canadian Nuclear Safety Commission (CNSC) develop a cybersecurity legislative and regulatory framework at a painstakingly slow pace, threat actors are thriving. The chasm between the deployment of protective legislation and the rapidly evolving threat landscape is ever expanding. In a profit-driven world where security is often viewed as a non-revenue-generating cost, organizations rarely prioritize these investments unless required by law.

A robust nuclear security legislative and regulatory framework is fundamental in assuring the safe and sustained delivery of the industry's critical services. The framework serves as the foundation for responsible and accountable nuclear security governance by establishing baseline requirements and assuring the industry's compliance through enforcement. Without robust regulations, there is an increased risk of critical services disruptions, or radiological releases to the population and the environment, and the possibility for nuclear materials to be diverted for malicious purposes. These risks have highly consequential national and international security impacts.

A Threat and Risk Assessment (TRA) was conducted to assess the effectiveness of the existing legislative and regulatory framework in protecting the Canadian nuclear industry from insider threats. The TRA provided both quantitative and qualitative analyses of the impacts, threats, existing safeguards, and vulnerabilities related to insider-initiated attacks.

The TRA concluded that the legislative and nuclear regulatory framework does not adequately protect the industry from the insider threat, resulting in a *HIGH* risk of insider-initiated attacks. The TRA identified five key vulnerabilities driving the risk rating: poor cybersecurity governance, human factors limitations, insufficient regulatory due diligence, lack of legal precedents, and limitations associated with third-party risk management.

This research contributes to the current literature on security risk management and nuclear security policy on two fronts. On one hand, it builds on existing threat and risk assessment methodologies by offering a comprehensive yet scalable qualitative and quantitative framework that supports industry and sector-wide assessments. This approach effectively balances the simplicity of basic methods with the complexity of more advanced models currently in use. On the other hand, this research addresses a gap in current nuclear security policy literature by delivering a cross-sector, cross-jurisdictional, evaluation of the legislative and regulatory framework—an "all-of-nuclear" approach. Existing research on Canadian nuclear security risks and policies typically focus on nuclear power generation, overlooking the critical interdependencies among the various nuclear licensees across the three affected CI sectors.

Please note that this document is a condensed and restricted version of a more extensive research study. Certain sensitive information has been intentionally omitted, to protect intellectual property and maintain information security.

1. Defining Insider Threat in the Nuclear Context

There is no standard and globally applied definition of insider threat. Therefore, in the context of this research, insider threat was defined as follow, based on Public Safety Canada's and the IAEA's definitions:

> *Any individual with knowledge or authorized access to nuclear materials, facilities, information, intellectual property, trade secrets, physical and digital assets, who, maliciously or inadvertently misuses their trusted knowledge or access to harm the*

> *organization's employees, customers, operations, assets, reputation or interests."*
> (IAEA, 2020a; Public Safety Canada, 2022)

These individuals include current, former and retired employees, students, third-party vendors, contractors, collaborators, national and provincial regulators, standard and safety authorities, as well as domestic and international regulatory agencies inspectors.

Insider threats are categorized into three profiles based on intention – their conscious decision-making process – and their motivation to cause harm (see Table 1). The accidental insider is the most prevalent profile. These individuals' actions are not the result of a deliberate decision to act against security policies or a motive cause harm. For example, a distracted employee falling for a convincing phishing attack, by clicking on a malicious link is considered an accidental insider. At the opposite end of the spectrum, the malicious insider deliberately chooses to act against security policies and is driven by a motivation to cause harm. A contractor recruited by a foreign nation who purposefully sabotages nuclear operations by introducing a malware-infected USB key in exchange for money is considered a malicious insider. At the intersection of the two profiles is the negligent insider, who, out of laziness, or carelessness makes a conscious decision to act in contravention to security policies but is not motivated by the desire to cause harm. An employee who regularly leaves sensitive documents on their desk unattended is considered a negligent insider.

Table 1
The Three Insider Threat Profiles

	Accidental Insider	Negligent Insider	Malicious Insider
	Inadvertent Insiders		
Intent – deliberate decision	No	Yes	Yes
Motive to cause harm	No	No	Yes*

** Exception: coerced insiders acting under duress.*

Regardless of their nature, these insiders' actions undermine organization's conventional and cybersecurity defenses by affecting the confidentiality, integrity and availability (CIA triad) of information and operations. However, their behaviours stem from different underlying factors, which must be understood to effectively mitigate the risks.

The accidental insider is driven by individual and organizational factors. Individual factors include inattention caused by personal problems, excessive workload, multi-tasking, sickness or neurodiversity. Organizational factors, on the other hand, include elements such as unclear policies, processes and procedures, poor cybersecurity literacy, and improper change management. The negligent insider's behaviour is also driven by personal and organizational factors. These include complacency, poor comprehension of security policies purposes and consequences, cognitive bias, poor security culture, inadequate leadership or enforcement of security policies. Accidental and negligent insiders are collectively referred to as inadvertent insiders throughout this research. They represent the majority, 75%, of insider threat cases (Ponemon Institute & DTEX, 2025).

While the malicious insider is the most disruptive of the three profiles, it is the least recurrent. This insider represents 25% of the overall insider-initiated attacks, and the primary attack vector in only 7% of all data breaches (Ponemon Institute & DTEX, 2025; IBM & Ponemon Institute, 2024). The malicious insider's behaviour is driven by four motivating factors, represented by the acronym MICE.

M	Money
I	Ideology
C	Coercion
E	Ego

(Charney, 2010; Zul-Azri & al., 2022)

The current socioeconomic and geopolitical context aligns directly with inadvertent and malicious insiders' motivations and vulnerabilities. In the post-pandemic context, multiple nuclear stakeholders and the supporting supply chain have maintained fully remote or hybrid work arrangements. This has reduced the natural behavioural monitoring that occurs in the office, and increased employees' opportunities to deviate from security policies. A 2022 study reported that 75% of insider threat criminal prosecutions in the United States involved remote workers (Lang, 2022).

Moreover, the looming global economic downturn is also affecting malicious and inadvertent insiders (International Monetary Fund, 2025; World Bank, 2025). For decades salaries have not kept up with inflation, putting a strain on insiders' finances, and increasing their temptation to engage in fraudulent activities. The situation is highly exploitable by threat actors on two fronts: it facilitates the recruitment of malicious insiders on a financial basis, and it facilitates the exploitation of human error arising from cognitive distraction caused by financial hardship.

With more than 60 active violent conflicts across the globe, the effervescent geopolitical context is also affecting nuclear insiders. Cognitive warfare tactics fueled by online misinformation, disinformation and malinformation (MDM) campaigns, inflammatory politics and transnational repression are amplifying political polarization (Nord & al., 2025; Institute for Economics & Peace; 2025). The situation is making malicious insiders increasingly susceptible to transnational coercion and ideologically driven recruitment by threat actors. It is also a catalyst for self-radicalization, especially when coupled with psychological fragility or personal hardship (Kenyon & al., 2021). The strained geopolitical climate is equally affecting inadvertent insiders. Individuals from diaspora communities, as well as those working in sectors affected by the ongoing tariff war are experiencing significant hardship, increasing their susceptibility to distraction and errors, which can be exploited by threat actors.

The ongoing mental health crisis also has a part to play in exacerbating the already volatile situation (World Health Organization [WHO], 2022). Reports show that the global mental health state has not recovered from the COVID-19 pandemic, and that multiple countries, including Canada, have insufficient resources to support their citizens (Sapien Lab, 2025; Statistics Canada, 2023). Nearly half of the workforce suffers from ego depletion symptoms, impairing employee's cognition and judgment and making them more prone to errors, persuasion, and coercion; factors easily exploited by threat actors. (Sapien Labs, 2025). Personality disorders associated to overinflated ego, particularly dark triad conditions (narcissism, Machiavellianism, and psychopathy) are equally posing a risk to the nuclear industry (Twenge & al., 2014). Dark triad traits are consistently identified in individuals convicted of espionage and breaches of trust, and these traits are also linked to a higher inclination for fraudulent activity, sabotage, and coercion (Harms & al, 2022; Baweja & al., 2023). Dark-triad personalities are more prevalent in highly educated male populations and are known to be attracted to fields of employment

that are high-risk and demonstrate power, authority and leadership, like the nuclear industry (Jonason & al., 2017; Yrondi & al., 2015; Diller & al., 2021).

2. TRA Methodology

A 12-steps hybrid methodology was developed to conduct the industry-wide TRA. The methodology employed elements of the Harmonized Threat and Risk Assessment (HTRA), the Design Basis Threat (DBT), and CARVER+Shock Analysis (Communications Security Establishment [CSE] & Royal Canadian Mounted Police [RCMP], 2007; Food and Drugs Administration [FDA], 2009; IAEA, 2021). This approach was adopted to address the limitations and challenges inherent in each methodology: the absence of quantitative risk assessment in the DBT, the extensive and time-consuming scope of the HTRA methodology, and the superficial nature of the CARVER+Shock analysis.

The HTRA methodology offers clear quantitative evaluation criteria, which is not present in the DBT or CARVER+Shock methodologies. Elements of the HTRA were utilized to support the evaluations of factors that required detailed quantitative analysis and prioritization such as the critical assets, threat impacts, threat likelihood and the overall threat, vulnerability and residual risk levels.

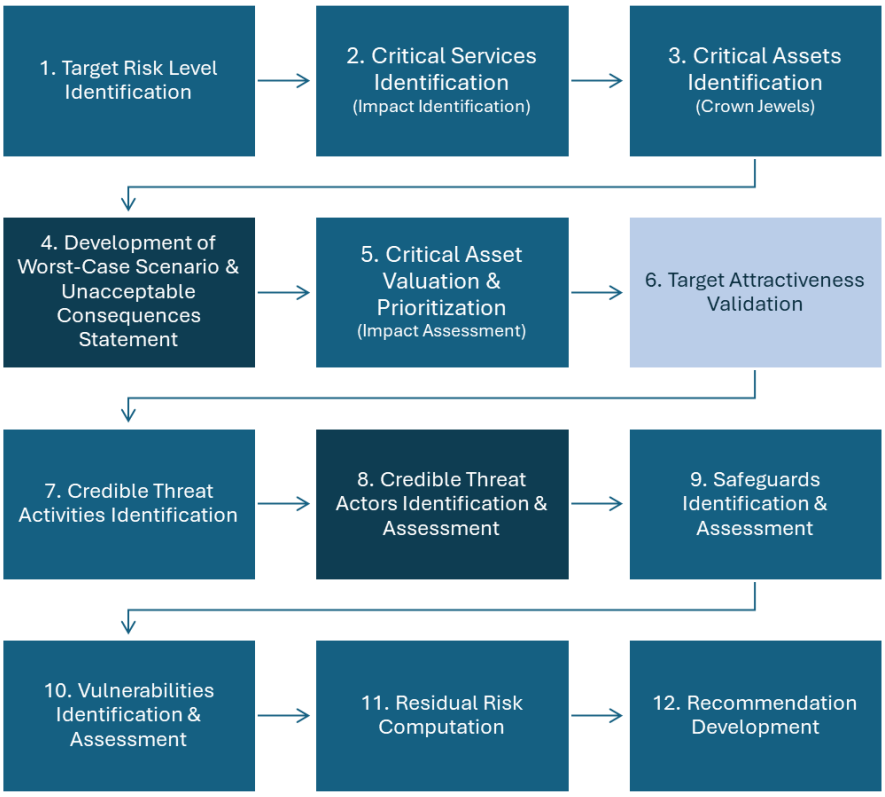
The utilization of the DBT methodology brought focus to the TRA. Qualitative elements of the DBT were used to identify unacceptable consequences and plausible worst-case scenarios. These assumptions were used as the foundation for the threat activities' quantitative analysis. Additionally, applying the DBT principles allowed for the assessment to hone-in on credible, deliberate threat actors, recognizing that malicious or inadvertent insider exploits are always driven by a deliberate threat actor.

Finally, the CARVER+Shock assessment was employed early in the process to validate that the industry's critical assets are indeed attractive targets for threat actors. In contrast to the HTRA methodology, which reach this conclusion only at the end of the assessment, CARVER+Shock offers this validation upfront, preventing the unnecessary effort of conducting a complete TRA on assets that are not appealing targets. The TRA was conducted following the 12-step methodology presented in Figure 1.

2.1. Challenges and Limitations

Four major challenges and limitations were encountered as part of this TRA. The first challenge was the complexity and compartmentalized nature of the legislation and regulations. With the safeguards protecting against insider threat set across multiple instruments, a deep dive into a breadth of acts, regulatory documents, and mandatory standards was required. Secondly, the dynamic nature of the threat landscape and the regulatory environment posed a challenge. To mitigate, a time boundary was set for the TRA, where the research dataset was continuously updated from 1 June 2023 to 30 October 2024, incorporating new information as it became available. Thirdly, the absence of mandatory reporting requirements in Canada and the highly sensitive nature of the information across the nuclear industry made data collection challenging. Partially available information was triangulated with closely related materials and supplemented with access-to-information requests. Industry experts were also consulted for substantiation. The final challenge, the absence of a comprehensive yet adaptable TRA methodology, was addressed by developing a hybrid approach that combines the strengths of three widely recognized and commonly used TRA methodologies.

Figure 1
12-Step Hybrid TRA Methodology



Note: medium blue steps originate from the HTRA methodology, dark blue from the DBT methodology, and the light blue step from CARVER+Shock.

3. Threat and Risk Assessment

3.1. Target Risk Level Identification

A target risk level of *MEDIUM* was selected for the TRA. This level offers a balanced approach that considers the fine line between security risk management and the conduct of nuclear operations. It also considers the entire industry's cybersecurity maturity level, which is lagging compared to other CI sectors (Dias et al., 2024)

3.2. Impact Assessment

3.2.1. Critical Services Identification

The Canadian nuclear industry does not have a global mission statement to derive critical services from. However, an analysis of key industry players'[1] mission statements led to the identification of four critical services:

[1] Bruce Power, Ontario Power Generation (OPG), Canadian Nuclear Laboratories (CNL), McMaster University, École Polytechnique de Montréal, TRIUMF, New Brunswick Power, Cameco, Canadian Nuclear Safety Commission, Canadian Nuclear Association.

- The safe and sustained generation of electricity, worth CAD$ 40.4B in 2022 (International Trade Administration, 2023);
- The safe and sustained generation of radioisotopes, valued at CAD$ 589M in 2023 (Research and Markets, 2024);
- The safe and sustained delivery of research and development (R&D) activities, worth more than CAD$288M in 2022 (Statistics Canada, 2024), and;
- The safe and sustained operation of the nuclear supply chain throughout its lifecycle, from uranium extraction to nuclear waste disposal, valued well over CAD$ 6.6B in 2023 (Global Affairs, 2023; Rabson, 2023; Cameco, 2024).

3.2.2. The Crown Jewels – The Canadian Nuclear Industry's Critical Assets

The Canadian nuclear industry's critical assets were derived from its critical services. The assessment identified six *interdependent* critical assets:

- Nuclear power plants (NPPs), supporting the generation of electricity and radioisotopes used in nuclear medicine and food sterilization;
- Research reactors, supporting the NPP maintenance activities, the production of radioisotopes, and the delivery of innovative R&D activities;
- Uranium mines and mills (UMM), providing the global industry with the raw materials necessary for nuclear fuel fabrication;
- Nuclear fuel processing facilities (NFPFs) supporting the NPPs and internationally;
- Medical and research facilities, supporting the delivery of R&D activities and the production of radioisotopes, and;
- The supply chain, supporting the entire industry with expertise, services, materials, software and equipment. Please note, this critical asset refers to the broader supply chain that extends beyond the nuclear supply chain.

3.2.3. Plausible Worst-Case Scenario and Unacceptable Consequences

Two elements from the DBT were introduced at this stage to provide a tangible foundation for the critical asset valuation: the development of a plausible worst-case scenario and the identification of unacceptable consequences. Both are based on the mission statements of public safety and nuclear security agencies:

> *Any incident resulting in a disruption in critical service delivery, a release of radiological dose to the public or the environment, the theft or sabotage of nuclear materials or controlled equipment, and, or, resulting in a confidentiality, integrity or availability compromise of intellectual property, trade secrets or business information.*

An incident of this nature would trigger serious national security consequences, including power and nuclear medicine disruptions, physical and psychological harm to the population, a decline in public trust in nuclear energy, economic destabilization, and the erosion of Canadian sovereignty and national values. It could also trigger legal sanctions under the international nuclear safeguards' agreements, further damaging Canada's global reputation. It would also have considerable international security repercussions, including North American power disruptions, shortages of medical radioisotope, the proliferation of nuclear materials and information for malicious purposes, an increase in illicit nuclear weapons stockpiles, an intensification of geopolitical instability, and diminishing confidence in

international institutions and multilateral cooperation. From a climate perspective, it would reduce public support for the peaceful use of nuclear energy, triggering a third wave of nuclear phase-out, thereby exacerbating climate change.

3.2.4. Critical Asset Valuation

The nuclear industry's six critical assets were evaluated, prioritized, and scored based on the potential national and international impacts resulting from the compromise of their confidentiality, integrity, and availability, as well as the physical and psychological consequences of a worst-case scenario attack. Financial impacts were also assessed for both domestic and global contexts. The degree of injury to each criterion was quantified using the HTRA evaluation criteria. The results are shown in Table 2.

Table 2

Canadian Nuclear Industry Asset Prioritization

Critical Asset	Injury Total (/35)	Asset Priority	Asset Score
Nuclear Power Plants	30	1	5
Nuclear Fuel Processing Facilities	28	2	4
Uranium Mines and Mills	28	2	4
Supply Chain	25	3	3
Research Reactors	25	3	3
Medical & Research Facilities	22	4	2

The evaluation concludes that NPPs are the most critical asset, given their direct impact on all other CI sectors, their impact on the highly integrated North American electrical grid, and the magnitude of public injuries sustained should an incident occur. Nuclear fuel processing facilities and uranium mines and mills are ranked a close second, as they provide the nuclear materials essential for sustaining both domestic operations and a significant portion of the international NPP fleet, holding a substantial share of the global supply[2]. The broader supply chain and research reactors are ranked third, demonstrating their importance to the industry but expressing less destructive consequences should their information or operation be compromised. Finally, medical and research facilities were assigned a priority of four, due to existing redundancies and slighter breadth of the physical and psychological consequences.

3.2.5. On Target Attractiveness

To ensure proceeding with the TRA was justified, a target attractiveness validation was performed using the CARVER+Shock methodology. Originally developed by the U.S. Department of Defense as a tool to efficiently identify and prioritize an adversary's most impactful and disruptive targets, the methodology can be applied in reverse to evaluate domestic targets level of attractiveness. The assessment is based on seven criteria, criticality, accessibility, recuperability, vulnerability, effect, recognizability, and shock, each scored on a scale of ten. Table 3 outlines the results of the assessment.

[2] 12% of the global raw uranium supply, and 21% of the global UF_6 conversion services used to produce nuclear fuel (Cameco, 2023).

Table 3
Summarized Results from CARVER+Shock Assessment of the Canadian Nuclear Industry's Critical Assets

Critical Asset	Total (/70)	%	Asset Priority
Nuclear Power Plants	60	86	1
Nuclear Fuel Processing Facilities	58	83	2
Uranium Mines and Mills	58	83	2
Supply Chain	56	80	3
Research Reactors	52	74	4
Medical & Research Facilities	49	70	5
Industry Average	56	79%	-

The assessment shows that the industry's critical assets are indeed attractive to threat actors, with an average score of 79%. The NPPs represent the most attractive targets, with a score of 86%, while medical and research facilities gathered a score of 70%. The results for all critical assets are generally consistent with the asset prioritization results.

3.3. Threat Assessment

3.3.1. Credible Threat Activities

As part of the threat assessment, the six credible insider-initiated threat activities below were identified. These activities are convergent in nature; they can interact or compound and can plausibly result in the identified worst-case scenario and its associated unacceptable consequences. These threats pose a significant risk to the confidentiality, integrity, and availability (CIA) of mission-critical digital and physical systems, sensitive intellectual property, trade secrets, personnel, and the public support required to assure the safe and sustained delivery of the industry's critical services.

- Cyberattacks;
- Espionage, theft of IP, or data leaks;
- Sabotage;
- Procurement or installation of counterfeit or compromised equipment or software;
- Fraud;
- Subversion or spread of misinformation, disinformation, malinformation (MDM).

3.3.2. The Presence of Credible Threat Actors

Four credible threat actor categories with nuclear motives and the capability to exploit insiders were identified: states and state-sponsored actors, criminal organizations, ideologically motivated violent extremists (IMVE), and lone-wolf insiders. These threat actors are known to interact closely with each

other. To alleviate the complexity their interactions, threat activities were attributed to the threat actor responsible for recruiting the other[3].

State and State-Sponsored Actors

State and state-sponsored actors have fully integrated hybrid and sub-threshold warfare techniques in their defence, diplomacy, and economic toolboxes. Many have well-funded, dedicated programs to the recruitment, exploitation, coercion or infiltration of nuclear insiders, operating primarily under the umbrella of plausible deniability.

Russia's foreign intelligence agency, the Main Directorate of the General Staff of the Armed Forces, has multiple cyberwarfare units that systemically leverage hacktivist and cybercriminal organizations to exploit nuclear insiders. With more than 20 reported attacks targeting British, American, Czech, and Ukrainian nuclear facilities since 2017, the Russian federation employs cyberwarfare for strategic, subversive, ideological and diplomatic coercion purposes. Agents and cybercriminals[4] instill fear, gather intelligence and establish a foothold in nuclear environments in preparation for future sabotage operations, with the aim to destabilize western democracies and assert regional hegemonic control.

The People's Republic of China (PRC) possesses a multiprong arsenal at its disposition to target nuclear insiders, which support its economic and hegemonic superpower objectives. Over the past two decades, the PRC has integrated a whole-of-nation approach to intelligence collection within its legislative framework. Its *National Intelligence Law* requires Chinese citizens and companies worldwide to support and cooperate with the state's intelligence agencies, including granting access to devices, networks, information, and intelligence when requested. The PRC controls multiple sophisticated cyberwarfare units that hide behind inadvertent insiders' legitimate actions to conduct deceitful, long-term espionage and pre-positioning attacks. These includes advanced persistent threats like Salt Typhoon and Volt Typhoon, which targeted the American nuclear sector (New Jersey Cybersecurity and Communication Cell, 2025). Additionally, China has a long history of recruiting, infiltrating and coercing nuclear insiders that pre-dates its Thousand Talent Program (Zweig & al, 2020). Between 1987 and 2021, the PRC repatriated 162 scientists from the Los Alamos nuclear laboratories to fuel innovations in its civilian and defence nuclear sectors (Strider, 2022).

North Korea has equally developed a multiprong arsenal within its military intelligence, the Reconnaissance General Bureau (RGB). RBG's Bureau 121 is known to conduct ransomware attacks against nuclear facilities, most recently in South Korea, India and America, to fund and advance its nuclear weapons program (U.S. Department of Justice [U.S. DoJ], 2025a). To the same effect, Department 53's army of illegitimate remote workers have virtually infiltrated every Fortune 500 big-tech company (Miller & Nicker, 2025). The establishment of laptop farms by Western nationals facilitated the infiltrations (U.S. DoJ, 2025b). Those big-tech companies play a direct role in supporting the global nuclear sector, including Canada's. The RGB Third Bureau is also known to use social engineering tactics targeting inadvertent insiders in Brazil, France, Germany, India, Britain, America, and South Korea to gain access to civilian and defence nuclear IP (Cybersecurity & Infrastructure Security Agency, 2024; Greig, 2024).

The Iranian regime is systematically exploiting transnational and cybercriminal networks to recruit nuclear insiders to acquire dual-use and controlled equipment and information, advancing both its

[3] For example, if a state or state-sponsored actor provided funding to an IMVE to conduct a ransomware campaign, the event was categorized under "state or state-sponsored actor".

[4] Such as Sébastien Vachon-Desjardins, the ex-federal IT employee who was one of the most prolific members of the Russian CaaS group NetWalker.

civilian and illicit military nuclear programs (Mailey, 2024). In the late 2000's an Iranian and an Emirati national were charged with attempting to export controlled equipment, high-speed cameras, with known nuclear and military applications (U.S. DoJ, 2023). A similar case occurred in 2016, where an Iranian national was sentenced for illegally exporting controlled mass spectrometry equipment to Iran via Canada and the United Arab Emirates (U.S. DoJ, 2021). Tehran is also known to recruit insiders to conduct cyber and kinetic military operations against nuclear facilities, as demonstrated the 2012 and 2013 cyberattacks against the IAEA, the 2024 cyberattack on the Shimon Peres Negev Nuclear Research Center and, in 2025 when it bombed the Weizmann Institute's nuclear research facilities (BBC, 2012; Reuters, 2013; Borger, 2025).

Israel leverages Mossad and the Israeli Defence Forces' Unit 8200 extensively to recruit and exploit insiders for sophisticated, well-coordinated cyber and kinetic operations against nuclear targets. This includes the execution of multiple cyberattacks against Iranian nuclear facilities over the past two decades, starting with Stuxnet. It also includes the recruiting and handling of the insiders who supplied critical intelligence regarding the nuclear programme in the preparation of the 12-day war in June 2025 (Frankel & Mednick, 2025).

Finally, the United States' Central Intelligence Agency's Special Activities Division and US Cyber Command are known to recruit and exploit insiders in the conduct of sophisticated convergent sabotage operations. They are widely believed, alongside their Israeli counterparts, to have co-developed the STUXNET malware and recruited the insider that delivered the payload on Iran's nuclear program over two decades ago (De Falco, 2012; Beuth, 2024). Both organizations have also launched cyberattacks against North Korea's nuclear weapons program and the illicit entities financing it (Bae, 2025).

Criminal Organizations

Criminal organizations are also known to extensively target the nuclear sector and their supply chain. Criminals gain access by recruiting malicious insiders or exploiting inadvertent insiders through social engineering, as well as via lost or stolen credentials and digital devices. Criminal organizations are primarily driven by financial gain. They typically generate funds through direct extortion, such as ransomware attacks or theft of physical nuclear assets, or by receiving payment via traditional criminal networks and cybercrime-as-a-service models. In 2021, the cybercriminal group DarkSide launched a ransomware attack against the Brazilian nuclear operator Eletronuclear, forcing it to shutdown its business servers (Reuters, 2021). The same year, Sol Oriens, an American nuclear weapons program contractor was targeted by the ransomware-as-a-service group Revil (Greig, 2022). In 2023, the U.S. Department of Energy was affected by the MOVEit supply chain attack, carried out by the cybercrime group Cl0p. The following year, the Yakuza leader Takeshi Ebisawa was charged by U.S. authorities for conspiring to traffic nuclear materials (U.S. DoJ, 2025c).

Ideologically Motivated Violent Extremists

Ideologically motivated extremists exploit inadvertent nuclear insiders much like criminal groups do, but their objectives are rooted in ideology rather than financial gain. Their actions are guided either by a fundamental opposition to nuclear energy or by an effort to leverage the nuclear sector to advance or fund their political, religious, or social agendas. In 2012, three nuclear weapons protesters, including an 82-year-old nun, infiltrated the Y-12 uranium enrichment site in Oak Ridge, Tennessee, a key facility of the American nuclear weapons program (Bunn & Sagan, 2014). The protesters are thought to have obtained insider information to plan and execute their attack, which resulted in a vandalized uranium storage building. Two years later, during the siege of Mosul, Iraq, members of the terrorist group ISIL reportedly removed 40 kilograms of low-grade uranium from the city's university research center (Dahl,

2014). With the right knowledge, the stolen materials could be used to develop a dirty bomb or to poison the population by contaminating food supplies. In 2018, the founder of the terrorist organization Atomwaffen Division was jailed for illegally possessing explosive equipment with the intent of targeting a nuclear facility, upon conditional release, he was sentenced with similar intents (U.S. DoJ, 2018; George Washington Program on Extremism, 2025; U.S. DoJ, 2025d). On the digital front, the hacktivist group BlackReward compromised the Iranian Atomic Energy Organization's email system in 2022, in opposition to Tehran's oppressive theocratic government (Sharwood, 2022). A similar incident occurred in 2023 where members of the international hacktivist group Anonymous conducted Distributed Denial of Service (DDoS) attacks on the Japan Atomic Energy Agency, Japan Atomic Power Corporation and the Atomic Energy Society of Japan's websites over the state's plan to release treated radioactive water into the Pacific Ocean (Japan Times, 2023). The same year, the Idaho National Laboratory's human resource data cloud content was leaked by SiegedSec, a hacktivist group self-described as "gay furry hackers". While the group is historically known to protest far right and anti-LGBTQ+ agendas, the INL hack came with a formal request for research on the creation of "catgirls". The attack resulted in the unauthorized disclosure of 45,000 current and former employees' sensitive personal information (Greig, 2023), which could be used to conduct future more destructive spear-phishing campaigns.

Lone-Wolf Insiders

Lone-wolf insiders are malicious insiders unaffiliated to other threat actors. They are known to abuse their privileged access and knowledge for personal gain, vengeance or self-radicalized ideological purposes. In 2009 Alex Maestas, a Los Alamos laboratory technician attempted to appropriate plutonium contaminated gold with apparent personal gain motives (Hobbs & Pope, 2015). In 2014, a Belgian contractor with access to the Doel power station deliberately sabotaged reactor operations by draining the lubricant from one of the reactor turbines, causing it to overheat and shut down. While the individual's motivations have not been validated, the attack forced a five-month outage of the reactor, costing Electrabel 138 million euros (Scharff, 2024). Two years later, Charles H. Eccleston, a disgruntled former employee of the American Nuclear Regulatory Commission (NRC), was imprisoned for offering the Filipino government access to 5,000 NRC employees' email accounts and proposing to conduct espionage and sabotage spear-phishing attacks in exchange for $18,800 (U.S. DoJ, 2016). Eccleston had intended to make the same offer to the Chinese, Iranian or Venezuelan governments should the Manila refuse. Most recently, in 2024, James Mousaly, a then-employee of Ontario Power Generation, one of Canada's largest nuclear operators, was arrested and charged for deliberately communicating safeguarded information to a foreign entity over social media. The public safety authorities identified that Mousaly acted with the intent to cause damage to Canada, but that, fortunately, the risks resulting from the leak were effectively mitigated.

3.3.3. Threat Valuation

The threat levels for each threat actor category were calculated using the HTRA evaluation criteria, considering their likelihood of attack and associated impact. Likelihood was quantified by the frequency of attack, which was substantiated by news articles, government, and industry sources. The degree of impact was informed by open-source intelligence and defence literature. The summarized results of the threat assessment are presented in Table 3, while the complete results can be found in Appendix A.

Table 3

Threat actor categories and their respective threat levels

Threat Actor Categories	Average Threat Level Across the 6 Insider Threat Activities	Trend
State & State-Sponsored Actors	5 - Very High	⇧
Criminal Organizations	4 – High	⇧
Ideologically Motivated Violent Extremists (IMVE)	3 - Medium	⇧
Lone-Wolf Insider	3 - Medium	⇧

The threat assessment reveals that state and state-sponsored actors pose a very high risk to the Canadian nuclear industry. This is largely due to their significant interest in obtaining both physical and digital access to the industry's assets to advance their financial, defense, and strategic objectives. Their motivations are reflected in highly sophisticated, well-funded programs capable of carrying out frequent attacks. The second greatest threat to the industry comes from criminal organizations. This rating is due to the ruthless and pervasive nature CaaS groups, their growing sophistication fueled by AI, and their impactful success rates. IMVE and lone-wolf insiders pose a moderate threat. This is mainly driven by the lower frequency of attacks, which can be attributed to the lone-wolf insiders' fear of retaliation and limited resources, and IMVE's preference for more violent operations directly connected to their ideologies.

3.4. Risk Assessment

3.4.1. Safeguards Assessment

A thorough review of federal and provincial legislation, along with the nuclear regulatory framework, identified 25 safeguards that include requirements for mitigating insider threats (see Appendix B). These safeguards support one or more of five key security functions: deterrence, prevention, detection, response, and recovery. The assessment revealed that the deterrence function overwhelmingly dominates the 25 safeguards, resulting in a largely reactive approach to insider threat mitigation. Moreover, the effectiveness of many safeguards is constrained by overarching assumptions that conflict with the realities of the 2025 threat landscape.

Assumption 1: The threat actors are affected by the safeguard

The legislative and nuclear regulatory framework scarcely applies to the most prominent threats: state and state-sponsored actors and CaaS organizations. The framework applies to individuals and organizations located in, or conducting business in Canada. A large portion of these threat actors operate internationally and may never set foot in Canada. While extradition agreements exist with like-minded states, not all are reciprocal. Moreover, no such agreement exists with the most prominent and persistent threats: China, Russia, Iran, and North Korea.

Assumption 2: The threat actors behave in an intentional and rational manner

This assumption is flawed on two fronts. It fails to consider the exploitation of inadvertent insiders, representing more than 75% of the insider threat cases. The assumption also fails to consider the coerced insider, who, acting under duress and undue stress, may not make rational and logical decisions.

Assumption 3: The incident can be attributed to the offender(s)

Cyberattacks are notoriously challenging to attribute, largely explaining their pervasiveness. The estimated attribution and prosecution rate of cyberattacks in the United States in 2020 was 0.05% (World Economic Forum, 2020). While the statistic is not recent, the frequency of cyberattack has continued to rise, keeping pace with mitigation efforts. This phenomenon is partly caused by the

widespread availability of malicious coding knowledge, and the raise of AI as both a threat vector and a force multiplier.

3.4.2. Vulnerabilities Assessment

Each critical assets' relevant safeguards were mapped to threat activities. Vulnerabilities were identified for reach pairing, then scored using the HTRA evaluation criteria based on their ease of exploitation, ease of detection, probability and severity of compromise. At this point, the "research reactor" critical asset was divided in two categories: high-security, and non-high-security, due to the difference in applicable safeguards. The results were then averaged per threat activity, (see Appendix C). From the assessment emerged five highly exploitable vulnerability categories: poor cybersecurity security governance, human factors limitations, insufficient regulatory due diligence, lack of legal precedents, and limitations associated with third-party risk management.

3.4.2.1. Poor Cybersecurity Governance

As of 2025, there are no formal, dedicated cybersecurity legislations or regulation affecting the Canadian nuclear industry. There was a glimmer of hope between 2021 and 2024 from a legislative standpoint with Bill C-26[5], now reintroduced as Bill C-8. The Act is to provide legally binding cybersecurity and incident reporting requirements for four critical infrastructure sectors: telecommunication, finance, energy and transportation. However, caught in a political system rife with partisan politics, and delayed by a prorogation, it has taken more than four years to progress the act. Moreover, current proceedings suggest that the act will only apply to NPPs, limiting the breadth of its effectiveness given the close interdependence between the industry's assets (House of Commons Canada, 2024; Parliament of Canada, 2024; House of Commons Canada, 2025).

From a nuclear regulatory perspective, progress in promoting a robust cybersecurity posture is limited. The CNSC has been developing a cybersecurity regulation since 2016, following a recommendation from the IAEA International Physical Protection Advisory Service (IPPAS) Mission to Canada. The IAEA recommended mandating cybersecurity requirements for all at-risk activities such as non-power (research) reactors, nuclear fuel fabrication and processing, as well as transportation (International Atomic Energy Agency [IAEA], 2016). Nearly a decade later, there is no tangible, enforceable cybersecurity regulation for those at-risk licensees (CNSC, 2020b, 2021c, 2021d, 2022b, 2023b, 2024a, 2024b, 2025a).

As of 2025, the nuclear industry's cybersecurity protection rests on the implementation of CSA N290.7:21, on the nuclear licensee's reporting requirements, and on astute business decisions. The CSA N290.7:21 standard provides requirements for the five security functions and is loosely aligned with the National Institute of Standards and Technology (NIST) guidance. There are, however, two major vulnerabilities with the application of the standard. First, the mandatory requirements apply solely to operational technology (OT) systems and data that perform a nuclear safety, security, or emergency function. It fails to consider emerging technologies such as artificial intelligence (AI) and leaves the protection of critical information technology (IT) systems, business systems, intellectual property (IP), and trade secrets a voluntary business decision. These gaps overlook the increasingly exploited attack vectors between business and OT systems. A striking example of the critical role business systems play in the energy sector is the 2022 Colonial Pipeline ransomware attack. The incident demonstrated that a critical business system can be leveraged to carry out high impact cyberattacks. By incapacitating a

[5] *an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (House of Commons, 2024)

financial system, the cybercriminal group DarkSide was able to disrupt 45% of the fuel supply on the American East Coast, resulting in a five-day outage and a declaration of state of emergency (Walsh, 2021; The White House, 2021). The second vulnerability associated with the application of CSA N290.7:21 is that mandatory compliance with the standard is limited to a small number of nuclear licensees: high-security sites[6]. As of 2025, the implementation of cybersecurity measures is a discretionary business decision for the non-high security research reactors, uranium mines and mills, fuel processing facilities, medical and research facilities and the supporting supply chain (CNSC, 2021e).

The delay in developing nuclear cybersecurity regulations is partly due to a strategic decision made by the CNSC in 2021 to revise existing Nuclear Security Regulations (NSR) rather than introducing standalone regulations. The current NSRs date to 2015. In 2021, the CNCS initiated the process to amend the regulations, with a 2023 completion deadline. In 2024, the CNSC revised its deadline to 2026. While the proposed changes appear to be a step in the right direction, they represent meager progress in terms of securing Canada's nuclear IP, infrastructure, and in overall upholding national security.

As part of the amendment, the CNSC proposes expanding the requirements for the implementation of cybersecurity programs and the production of annual TRAs to all licensees subject to the NSR (CNSC, 2021b, 2022c, 2023c). The proposed change would only affect fuel fabrication facilities and university research reactors, as high security sites already meet these requirements. Moreover, the CNSC does not intend on extending the protective requirements to critical business systems or IP, or to include requirements related to the use of AI[7] as part of the amendment, thus partially addressing the current legislative and regulatory vulnerabilities.

The legislative and regulatory framework largely omit considerations for service level agreements or business continuity, which have a strong impact on national security. Within the framework, business continuity requirements are set forth by provincial legislation, and only apply to NPPs (Government of Ontario, 2023, 2024).

By imposing partial cybersecurity and business continuity requirements, the current legislative and nuclear regulatory framework overlooks the critical interdependencies within the digital ecosystems and among industry stakeholders. As the CARVER+Shock analysis confirmed, all licensee types present a comparable level of attractiveness from threat actors' perspective. For example, a cyberattack incapacitating one of the only two Canadian nuclear fuel manufacturing companies could affect national security[8] nearly as significantly as a direct attack on a NPP would. Meanwhile, this licensee is not subject to the same cybersecurity requirements. Given the ongoing geopolitical tensions with both adversarial and allied states, and the increasingly constrained nuclear supply chain, the Canadian nuclear industry cannot afford to compromise its sovereignty.

3.4.2.2. Human Factor Limitations

The current legislative and nuclear regulatory framework neglects human factors. This is primarily driven by the strong dependence on security screenings as preventative safeguards against insider threats. Inadvertent insiders account for the majority of insider threat incidents, and the ability to obtain security

[6] NPPs and the high-security research reactors license holders (Canadian Nuclear Laboratories).

[7] The CNSC, in collaboration with the United Kingdom and American nuclear regulators, produced study on the deployment of AI in the nuclear sector providing guidance and best practices (CNSC & al., 2024). While guidelines are valuable, they are not legally biding.

[8] And arguable international energy security, considering Cameco's mines produced 21% of the global supplies of Uranium in 2022 (WNA, 2024).

clearance is not a predicting indicator of mistakes and accidents. Effective cybersecurity and threat awareness are preventative methods. The current governance framework, through the implementation of CSA N290.7, only requires high-security sites to maintain cybersecurity training programs. Additionally, the governance framework completely omits requirements for the implementation of a formal insider threat mitigation program. These gaps leave the industry in a vulnerable and reactive position.

There are several vulnerabilities within the security screening process that undermine the effective prevention and detection of malicious insiders. In theory, the Government of Canada's (GoC) Directive on Security Screening stipulates that security clearances should undergo ongoing assessments (Treasury Board Secretariat [TBS], 2025). In practice, the process is performed as minimally as possible, providing only a snapshot of an individual circumstances at the time of application or renewal. Although employees are required to self-report changes in their personal circumstances and managers are required to report changes in their employees' behaviours, neither are common practices. This issue stems from a combination of complacency, employees' fear of reprisal, and from insufficient managerial awareness of insider threat key behavioural indicators. Under the NSRs, high-security sites are required to maintain a peer and supervisory behavioural observation program (CNSC, 2020a). In many cases, the program is approached as a routine administrative requirement rather than a meaningful analytical tool. The training is primarily delivered through computer-based modules, with little emphasis on comprehension, engagement, or regular updates to reflect evolving threats.

Adequate security screening hygiene was also identified as a challenge. Pervasive delays in processing screening requests in a context of labour shortage have pushed hiring managers to develop creative and risky workarounds. For more than five years, Canadian public safety agencies have carried large screening application backlogs, significantly impacting hiring timelines and the overall quality of the investigations (Bronskill, 2019; Department of Finance Canada, 2023; Department of National Defence [DND], 2023). To cut costs and fast track new employees onboarding, organizations have been revising their personnel security program, delaying renewals, and downgrading the security clearance requirements for key positions. Caught between a rock and a hard place, these business decisions represent exploitable vulnerabilities for threat actors. Regulatory audits and inspections related to personnel security are infrequent, allowing potential compliance breaches to go undetected for extended periods, thus jeopardizing the ongoing delivery of the industry's critical services.

Three Canadian high-profile cases demonstrate the vulnerabilities associated with the overreliance on security clearances: Jeffrey Delisle, Sébastien Vachon-Desjardins, and the National Microbiology Laboratory (NML) couple Xiangguo Qiu and Kendig Cheng. Jeffrey Delisle had been a naval intelligence operator for over ten years when, in 2007, he walked in the Russian embassy offering to sell classified information. By 2009, Delisle had accumulated significant debts and was going through a painful divorce. Being part of the intelligence community, Delisle's personal situation should have been reported and have triggered a security clearance revalidation; it did not. Delisle was promoted in August 2011 and was reassigned to the Trinity intelligence centre, where he had access to more sensitive FIVE EYES intelligence. Delisle's top-secret security clearance had been expired for five months at the time of his promotion, and his transfer should have triggered a revalidation of his clearance. His clearance remained expired until December 2011, when the FBI reported his suspicious activities to the RCMP, triggering the revalidation process (Gordon, 2012). Delisle had the opportunity to pass classified information to Russian intelligence via floppy disks and USB for nearly five years before being apprehended. Most of the information the officer leaked were U.S. classified secrets, to which he had access but had no need to know (The Canadian Press, 2013). At the time of Delisle's trial in 2012, Canada had no legal precedent for

a case of this nature. He pleaded guilty to all charges and was sentenced to 20 years in prison, from which he was granted full parole in 2019 (Colley Borden, 2019).

Sébastien Vachon-Desjardins was a computer technician at the National Research Council of Canada (NRC) and held a security clearance before being arrested in 2015 on seven counts of drug possession for the purpose of trafficking (Woloshyn et al., 2022). He was sentenced to three and a half years in prison and released a year later. In 2016, while under conditional release, Vachon-Desjardins was again hired by the federal government as an IT analyst. It is unclear if the department, Public Services and Procurement Canada, validated his security screening before hiring him or if his NRC security clearance was still valid despite his criminal offence. In 2018, Vachon-Desjardins was arrested for a second time with drug trafficking and released while awaiting formal charges. He maintained his employment and a valid security clearance until January 2021, when he was again arrested, this time under a United States extradition order for ransomware crimes (Mandel, 2022; Woloshyn et al., 2022). Vachon-Desjardins was sentenced to 20 years in the United States, after being identified as one of the most prolific members of the Russian CaaS group NetWalker. At the time of his arrest, he had in his possession more than $700,000 in cash and US$21M in cryptocurrency.

Finally, one of the most recent and embarrassing cases of security clearance failure is that of the two researchers, Xiangguo Qiu and Kendig Cheng. Both researchers arrived in Canada in 1996 for their graduate studies and were subsequently hired at the NML, Canada's highest security laboratory which handles highly infectious and fatal diseases. Suspicions about Qiu first arose in 2018, when she was listed as an inventor on a Chinese patent believed to contain intellectual property owned by the NML. Both her and her husband were stripped of their access and security clearance in 2019, pending investigation. In early 2020, a CSIS investigation found the couple responsible for the breach of the lab's security policy but failed to action the evidence and granted the couple the benefit of the doubt on the espionage charges (Tunney, 2024). A few months later, however, the results of an independent fact-finding investigation required CSIS to reopen the case. This time, a more diligent investigation demonstrated that Qiu was part of the PRC's Thousand Talent Program and was using the NML to carry-out research on behalf of the PRC. The couple was dismissed and relocated before charges could be laid. They were recently found working under pseudonyms in a prestigious Chinese university connected to the state's military apparatus (Vanderklippe & al., 2024). The invocation of Articles 23 and 24 of the PRC's *National Intelligence Law* likely led to their relocation and employment.:

> "*When the personal safety of the staffs of national intelligence work institutions, personnel who have established cooperative relationships with national intelligence work institutions, or their close relatives, is threatened as a result of assisting national intelligence work, the relevant state departments shall employ the necessary measures to protect or rescue them*", and;
>
> "*The state shall arrange appropriate placements for persons who have made contributions to national intelligence efforts and require a placement*" (CSIS, 2025).

Given the alignment between Qiu's Ebola research timeline, the content of the Chinese patent, and the 2008 formal launch of the Thousand Talents Program, it is highly likely that Qiu had been acting on behalf of the PRC for over a decade (Shoham, 2020). At a minimum, one security clearance renewal cycle for Qiu and Cheng's top-secret clearance would have occurred. This suggests that both NML management and public safety agencies overlooked critical warning signs on two occasions: first during the 2020 investigation, and earlier during the renewal of the couple's security clearances.

This was not the first instance of the PRC exploiting federal government insiders to gain access to biological materials. In 2012, Klaus Nielsen and Wei Ling Yu, two Canadian Food Inspection Agency (CFIA) scientists with active security clearances were charged with breach of trust for attempting to provide the PRC with samples of live brucella, an infectious pathogen. Nielsen was sentenced to two years in prison, while his colleague and accomplice, Wei Ling Yu, is believed to have fled to China to avoid prosecution (Roman, 2015; Seymour, 2017). Nielsen and Yu had been working with the PRC for a minimum of seven years before being discovered (CBC News, 2014).

These two cases are excellent examples of the dire need to improve security screening hygiene and cybersecurity regulations in nuclear research and development. There are currently three operating research reactors (non-high security), and multiple nuclear and radiological research programs located on university campuses, hospitals and corporations. Due to the limited quantities of nuclear and radiological materials they handle, these organizations' physical, personnel, and cybersecurity are nominally regulated. Nonetheless, as these case studies indicate, they are actively targeted by threat actors (CSE, 2024). Canadian nuclear research centres engage in innovative research of economic value, dual-use research, and possess materials that could be used to build radioactive dispersal devices (dirty bombs). If these materials or IP were to fall into the wrong hands, the consequences could pose serious national and international security risks from a radiological and nuclear proliferation perspective and cause damage to the national economy.

3.4.2.3. Insufficient Regulatory Due Diligence

The Canadian Nuclear Safety Commission's objective is to prevent unreasonable risks to the health and safety of persons, the environment and national security (IAEA, 2020; CNSC, 2024b). Considering this objective, three regulatory vulnerabilities were identified: the upcoming NSR amendments introducing new security gaps, the irregular inspection of critical programs, and deficiencies with the application of the DBT process.

Nuclear Security Regulations Amendments

As discussed in section 3.4.2.1., the NSR are undergoing revision which include cybersecurity requirements for the licensees subject to it[9]. While providing supplementary requirements for the financial evaluation of personnel with Site Access Clearance, the proposed amendments are also introducing a new vulnerability exploitable by threat actors. The current NSRs personnel screening requirements override the TBS' *Directive on Security Screening* (Treasury Board Secretariat, 2025). The NSRs mandate a five-year security clearance revalidation cycle for insiders with Site Access Clearance, while the TBS requires a ten-year revalidation cycle (CNSC, 2022a). The amendment to the NSRs proposes to align its requirements to those of the TBS, effectively doubling the interval between security clearance revalidations. Site Access Clearance provides personnel, including vendors and contractors, with the authorized and unrestricted physical access to facilities, IT and OT systems necessary in the conduct of physical and digital espionage, sabotage, or fraudulent activities. The Canadian nuclear industry is highly dependent on vendors and contractors to maintain operations, especially in construction, project management, software implementation, and managed services. Given the current socioeconomic climate characterized by a rise in both malicious and inadvertent insider threats, increasingly aggressive actors with vested interests in nuclear, and the growing prevalence of supply

[9] Class I nuclear facilities: NPP, research reactors, nuclear fuel processing facilities, high-energy particle accelerators, and some long-term waste storage facilities.

chain attacks, extending the security clearance revalidation period for individuals with access to the industry's sensitive information and facilities is inherently imprudent.

Infrequent Inspection of Critical Programs

The second vulnerability stemming from insufficient regulatory due diligence is the infrequent inspections of programs relevant to insider threats mitigation. Inspections play a necessary role in validating license holder's accountability, yet inspections of cybersecurity and personnel security programs at nuclear facilities are far and few between. For example, only one inspection of the CNL cybersecurity program has been conducted since the implementation of CSA N290.7 became a regulatory requirement in 2018 (Dubé, 2024). Similarly, only one personnel security program inspection has been conducted at CNL in the past five years, which only targeted very specific roles. During an interview, the CNL's personnel security program manager recalled, however, that the inspection frequency used to be higher prior to 2018 (Durocher, 2024). Moreover, it was reported that CNL had never undergone an information management program inspection, leaving audits a voluntary business decision (Dubé, 2025).

An educated assumption regarding the root cause of this issue is that the international and national regulatory framework is primarily focused on the physical protection of nuclear materials, affecting the prioritization of security inspections. Based on this assumption, personnel security, cybersecurity, and information security program inspections would not be considered a high priority. Adequate resourcing also appears to be a contributing factor. The 2019 IAEA Integrated Regulatory Review Service (IRRS) mission to Canada report outlined the CNSC's challenge in recruiting and training inspectors specialized in cybersecurity (IAEA, 2020b). It is unclear, at the time of this research, if the regulator has taken the appropriate measures to address this gap, in the context of a nation-wide cybersecurity talent crisis (Guay, 2024; ICS2, 2024).

Deficiencies with the Application of the Design Basis Threat Process

IAEA member states commonly employ the DBT framework to identify credible threats to their nuclear industry by evaluating threat actors' motivations, intentions, and capabilities. The DBT defines worst-case security scenarios that both current and prospective nuclear licensees must use as the basis for designing and implementing their security programs. The DBT is typically produced by the state's nuclear regulator and is derived from a national nuclear security threat assessment, performed by the national public safety stakeholders. The DBT is the CNSC's only threat assessment instrument. It is a reliable threat assessment methodology, but a poor risk assessment tool. Although high-security site licensees are mandated to conduct annual TRAs, there is no risk assessment performed at the industry-wide level. This translates into an inefficient, impulsive approach to security risk management with no long-term, concerted strategy. In short, a chaotic fertile ground for threat actors to operate.

The CNSC has historically renewed the DBT on a five-year cycle. While a five-year revision cycle may have been adequate for the post-9/11 threat landscape, the rapid evolution and sophistication of cyber threats calls for a more frequent and agile re-assessment[10]. This assumes, of course, that the renewal cycle is adhered to in the first place. As of 2025, the regulator is actively revising its DBT, with the most recent approved version dating back to 2014. (Nuclear Security Summit, 2016). A DBT was produced in 2020 but never officially approved. Major geopolitical events and technological advances have affected the nuclear threat landscape in the ten years since the official DBT, especially in matters related to

[10] As a comparison, the United States Interagency Security Committee (from which the Department of Energy and Nuclear Regulatory Commission are part of) updates theirs every bi-annually. (Interagency Security Committee, 2024)

cybersecurity and industrial espionage. The geopolitical context and the new techniques, tactics and procedures are not reflected in the official version. Decade-long delays in releasing a DBT is irresponsible and represents a major vulnerability for the industry. The situation equally denotes a lack of oversight and accountability on the part of Parliament in conducting its own compliance verification and ensuring that the Canadian nuclear regulator is held to account.

Currently, the DBT is shared only with high-security site license holders, on a need-to-know basis, as to inform their mandated annual TRAs. The upcoming NSRs amendments propose to extend the distribution to nuclear fuel processing facilities and research reactors. Once again, a small step in the right direction, but insufficient in assuring the security of the industry as a whole. Uranium mines and mills, research facilities, and the broader supply chain face comparable, if not greater, cyber threats, given the absence of legally binding cybersecurity requirements. An attack compromising their ability to deliver critical services would ultimately disrupt uranium production, NPP daily operations and maintenance, leading to serious national and international security and reputational consequences.

3.4.2.4. Lack of Legal Precedents

Beyond the burden of proof that makes attributing and prosecuting cyberattacks exceptionally difficult, the limited operational experience and legal precedents in enforcing legislation protecting against insider threat generates additional challenges. Some legislation, such as the *Nuclear Terrorism Act*, the *Ontario Electricity Act,* and the *Emergency Management and Civil Protection Act* have never been put to test in the context of theft of nuclear material, or the failure to maintain business continuity. The number of prosecutions under the SOIA can be counted on one hand, amid the growing number of cases. Delisle was the first individual to be prosecuted under the Act in 2012. In 2013, Qing Quentin Huang, a subcontractor of Irving Shipbuilding, the company then responsible for the construction and maintenance of the Royal Canadian Navy fleet, was charged under the act. Huang was accused of attempting to transmit classified information to the PRC. In late 2021, the court stayed his charges due to the unreasonable delays in bringing the case to trial (Bronskill, 2021). Since then, only one conviction has been secured under the SOIA: Cameron Ortis. In 2019 the ex-RCMP intelligence officer was arrested and charged under the Act for unlawfully disclosing special operational information to members of criminal organizations (R v. Cameron Ortis, 2023, ONSC 3113, 2023). Ortis' trial exposed vulnerabilities within the legislative text and legal proceedings, which an interview with Ortis' defence lawyer, Jon Doody, clarified.

Doody explains that the SOIA was amended hastily after 9/11 and indicated that some of the legal text lacked clarity (Doody, 2023). The criminal nature of Ortis' actions rests in the unauthorized disclosure of the special operational information. The SOIA, however, does not define what constitutes "authority," which blurs the line of the criminality of the actions (Applicant's Factum: Constitutional Challenge to Section 14 of the Security of Information Act, 2023). Moreover, Doody outlines that Ortis was permanently bound to secrecy due to the highly classified nature of his work. This prevented the accused from disclosing some of the very highly classified evidence that would have been key to his defence[11].

The shortage of legal precedents has made the Canadian judiciary system reticent in enforcing the SOIA. While none of the nuclear workforce members are bound to permanent secrecy, the absence of operational experience in enforcing the legislation leaves plenty of grey areas for malicious insiders to exploit. Klaus Nielsen and Wei Ling Yu from the CFIA, as well as Qiu and Cheng from the NML laboratory

[11] Four of the ten charges against Ortis were dropped due to the court's inability to conduct a fair trial, stemming from restricted access to highly classified information.

were not charged under the SOIA, when public safety agencies had probable cause to do so. As of 2025, former energy workers Yue-Sheng Wang (Hydro-Québec researcher) and James Mousaly (OPG operator), along with ex-RCMP officer William Majcher, are on trial facing charges under the SOIA (RCMP, 2023, 2023, 2024).

3.4.2.5. Limitations with Third-Party Risk Management

As identified in the threat assessment, threat actors are increasingly turning to the supply chain to conduct their operations. This exploitation is performed through the merger and acquisition of key companies, the recruitment or introduction of malicious insiders[12], or by simply leveraging cyberattacks against supply chain vendors to affect their CI sector clients[13].

In 2018, a PRC state-owned company attempted to acquire AECON, the Canadian construction titan. At the time, AECON held multiple contracts with nuclear operators, including the Darlington and Bruce Power nuclear refurbishment projects (AECON, 2018). The sale was blocked with the Canadian government. Since then, the PRC has continuously attempted to acquire key enterprises, including several critical mineral companies such as Solaris Resources Inc., First Quantum Minerals Ltd., and SRG Mining Inc. (Rajagopal, 2024).

Most legislative and nuclear regulatory safeguards do not extend to the supply chain, regulators and inspectors, or collaborators. Rather, there are a few mandatory standards[14], that licensees must abide by in managing third parties. The requirements within these standards are, however, predominantly oriented toward quality assurance. The NSRs, supported by *REGDOC-2.12.2, Site Access Security Clearance* (CNSC, 2014), are the only safeguards that provide actionable requirements for mitigating third-party insider threats, through contractor vetting. These requirements, however, apply only to individuals with *direct* access to the licensee's physical or digital infrastructure. They overlook broader supply chain elements such as materials traceability, software development personnel, and other contributors involved in the manufacturing process or managed services.

The requirements also overlook vulnerabilities arising from unintentional insider threats. The standards do not require licensees to verify vendors', contractors', or even governmental regulatory agencies' cybersecurity programs, although they may possess critical and sensitive information such as engineering designs, or the quantities of nuclear materials held at a site. It is ultimately the license holder's business decision to implement rigorous security risk assessments within their procurement and collaborations practices. This rigorous approach is neither widely nor consistently adopted given the insufficient third-party risk awareness and training, and the absence of legally binding requirements. For decades, decision-makers have underestimated the strategic value of robust conventional and cybersecurity programs, often dismissing them as non-revenue-generating expenses, or cost centers. While this mindset is slowly shifting, the absence of legally biding requirements indicates that legislative and regulatory framework is ill adapted to the current threat landscape. It suggests that third-party security risk management is a low priority, leaving the industry highly susceptible to insider threat incidents.

---

[12] Such as Qing Quentin Huang, or the North Korean IT worker scheme.

[13] As seen with the 2020 SolarWinds attack, the 2023 Johnson Controls and MOVEit attacks affecting multiple high-security public safety and energy agencies in North America.

[14] CSA N286 *Management system requirements for nuclear facilities*, and *REGDOC-2.1.1, Management System* (CSA, 2022; CSA, 2021b; CNSC, 2019)

3.4.3. Residual Risk Assessment

To initiate the residual risk assessment, each critical asset was paired to each threat activities. The residual risk was calculated by multiplying the critical asset value, the threat score and the vulnerability score for each paring. The residual risk scores were subsequently categorized into high, medium, low, and very-low risk levels, using the HTRA conversion chart. A heatmap was developed to provide a visual representation of the synthetized information (see Table 4).

The results of the computation, presented in heatmap show an average residual risk score of *HIGH* across all critical assets, effectively demonstrating that the legislative and nuclear regulatory framework fails to adequately protect the industry from insider threats.

The assessment shows that NPPs and uranium mines and mills face a very high risk of insider-initiated cyberattacks, espionage, theft of IP (trade secrets), and data leaks. For NPPs these results are driven by the continent-wide impacts associated their disruption, due to the integration of the north American grid, making them highly attractive targets to threat actors. The uranium mines and mills results are primarily driven by the absence of applicable, legally binding cybersecurity, threat and risk assessments, continuous behavior monitoring, and business continuity requirements.

The assessment shows that nuclear power plants (NPPs) and uranium mines and mills face a very high risk of insider-initiated cyberattacks, espionage, IP or trade secret theft, and data leaks. For NPPs, this risk rating is largely driven by the continent-wide impacts of disruptions, given the interconnected nature of the North American power grid, which makes them especially attractive targets for threat actors. The elevated risk ratings for uranium mines and mills are primarily driven by their disruption's impact on the global uranium market, and the absence of legally binding requirements for cybersecurity programs, threat and risk assessments, continuous behavior monitoring, and business continuity planning.

The medium residual risk scores for subversion and MDM across all critical assets reflect the lesser immediate impacts of such attacks, as operational continuity can generally be maintained. However, these activities pose a long-term, chronic risk. While they may only mildly disrupt daily operations through internal personnel grievances, they can fuel anti-nuclear activism, increase the frequency of anti-nuclear conventional and cyberattacks, and, ultimately, undermine the industry's reputation and public support.

The medium residual risk levels associated with sabotage in research reactors, medical and research facilities, and the supply chain are attributed to the relatively lower critical impacts associated with disruptions, and the broader availability of alternative service providers.

Finally, the high residual risks levels across the other critical assets related to cyberattacks, espionage, data leak, procurement or installation of compromised equipment and software, and fraud are driven by several factors:

- The substantial consequences for national and international security if nuclear fuel fabrication, NPP maintenance, radioisotope production, or operational support are disrupted;
- The weak cybersecurity governance, stemming from the absence of legally binding cybersecurity regulations;
- The inadequate personnel security governance, marked by the absence of legally binding requirements for third-party security risk assessments and behavioural monitoring of insiders with access to facilities, materials, and sensitive nuclear and business information;
- The inherent deficiencies with the current personnel vetting process.

Table 4
Heat Map of averaged Residual Risk of Insider Threat Activities per Critical Asset

Threat Activity	NPP	Uranium Mines & Mills	Fuel Processing Facilities	Research Reactors (H.S.)	Research Reactors (NHS)	Research & Medical Facilities	Supply Chain
Cyberattack	V. High	V. High	High	High	High	High	High
Espionage/ Theft of IP/ Data Leak	V. High	V. High	High	High	High	High	High
Procurement or Installation of Counterfeit or Compromised (bugged) IT/OT Equipment or Software	High	High	High	High	High	High	High
Fraud	High	High	High	High	High	High	High
Sabotage	High	V. High	High	Med	Med	Med	Med
Subversion/ MDM	Med	Med	Med	Med	Med	Med	Med
Average Residual Risk	High	High	High	High	High	High	High

4. Recommendations

Seven risk mitigation recommendations were developed to promote adequate legislative and nuclear regulatory protection against insider threat in the Canadian nuclear industry. These recommendations offer pragmatic, resource-efficient means to directly address the identified vulnerabilities. They leverage existing legislative and regulatory instruments as well as industry standards to streamline their implementation. These measures are expected to reduce the residual risk level to the *MEDIUM* target. A revision of the TRA will be required upon implementation to assess the effectiveness of the recommendations.

Recommendation 1: The House of Commons should revise Bill C-8 to extend its application to all nuclear license holders to account for critical asset interdependency and adequately protect the nuclear supply chain.

Recommendation 2: The CNSC should leverage existing best practices and standards such as Systems and Organization Controls 2 (SOC2), IAEA nuclear security publications, and Carnegie Mellon's *Common Sense Guide to Mitigating Insider Threats* as the basis for a cybersecurity regulation and compliance framework (Software Engineering Institute, 2022).

Recommendation 3: The CNSC should amend the NSR and associated regulatory documents to:

a. Include business continuity requirements
b. Require the implementation of CSA N290.7 for all nuclear license holders

c. Maintain the five-year Site Access Clearance renewal cycle
d. Integrate TBS' *Directive on Security Screening* financial evaluation requirement for employees with Site Access Clearance.

Recommendation 4: CSA should amend:

a. CSA N290.7 to mandate the protection of critical business systems and information
b. CSA N286 to include security requirements such as supply chain and third-party risk assessments, as well as traceability requirements for the procurement of materials, equipment, software, and services.

Recommendation 5: The CNSC should develop, or collaborate with a trusted organization to develop, an annual cyber DBT and an industry-wide TRA.

Recommendation 6: The GoC should legislate and audit the mandatory development, approval and release of the physical security and cybersecurity DBTs, as well as their respective revision cycle.

Recommendation 7: CSIS and the CNSC should increased skilled staffing levels in key high-risk areas such as personnel security screening, nuclear threat intelligence, as well as personnel and cybersecurity program inspections.

5. References

Aecon. (2018). *Focused; 2018 annual report*. https://www.aecon.com/docs/default source/investorbriefcase/financial-reports/2018/annual-report.pdf?sfvrsn=c0106daf_2

Applicant's Factum: Constitutional Challenge to Section 14 of the Security of Information Act, Court File No.: 19-20044 (Superior Court of Justice (East Region) July 20, 2023).

Bae, S. (2025). *Deterrence Under Pressure: Sustaining U.S.–ROK Cyber Cooperation Against North Korea*. Center for Strategic & International Studies. https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea

Baweja, J.A., Burchett, D., Taylor, C., Katana, F.S., Nelson, L. (2023, July). *The Dark Triad: Considerations in Hiring, Employment, and Termination.* The Threat Lab. U.S. Department of Defense. https://www.hsdl.org/c/view?docid=889468#:~:text=%E2%80%9CThe%20Dark%20Triad%3A%20Considerations%20in,to%20maximize%20employees'%20positive%20contributions.

BBC. (2012). *Anti-Israel group hacks UN nuclear agency server*. https://www.bbc.com/news/world-middle-east-20522585

Beuth, P. (2024). Der Mann, der Stuxnet nach Natanz schmuggelte, ist angeblich identifiziert. *Der Spiegel*. https://www.spiegel.de/netzwelt/netzpolitik/stuxnet-der-mann-der-stuxnet-nach-natanz-schmuggelte-ist-angeblich-identifiziert-a-8d12b0fa-db78-4120-bf53-17f131323392

Bronskill, J. (2019). RCMP struggled with security-clearance backlogs at time of Cameron Ortis' alleged leaks, internal audit shows. *The Globe and Mail. https://www.theglobeandmail.com/canada/article-rcmp-struggled-with-security-clearance-backlogs-at-time-of-cameron/*

Bronskill, J. (2021). Hamilton man charged in 2013 with trying to leak secrets to China no longer being prosecuted. *CBC News*. https://www.cbc.ca/news/canada/hamilton/hamilton-secrets-law-huang-case-stayed-1.6289933

Bunn, M., Sagan, S. (2014). *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes.* American Academy of Arts and Sciences. Cambridge University. https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf

Cameco. (2023). *Corporate profile.* https://www.cameco.com/sites/default/files/documents/CCO-2023-corporate-profile.pdf

Cameco. (2024). *Annual highlights*. https://www.cameco.com/invest/financial-information/annual-highlights

Canada Labour Code, R.S.C. (1985). c. L-2.

Canadian Centre for Cyber Security. (2020). *National cyber threat assessment 2020*. Communications Security Establishment.

Canadian Centre for Cyber Security. (2022). *National cyber threat assessment 2023-2024*. Communications Security Establishment.

Canadian Centre for Cyber Security. (2024). *National cyber threat assessment 2025-2026*. Communications Security Establishment.

Canadian Nuclear Safety Commission. (2014a). *REGDOC-2.12.2, Site Access Security Clearance*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-12-2/

Canadian Nuclear Safety Commission. (2014b). *REGDOC-3.1.1, Reporting Requirements for Nuclear Power Plants.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc3-1-1/

Canadian Nuclear Safety Commission. (2015) *REGDOC-2.2.4, Fitness for Duty.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/comment/regdoc2-2-4-b/

Canadian Nuclear Safety Commission. (2018a). *REGDOC-2.13.1, Safeguards and Nuclear Material Accountancy*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-13-1/

Canadian Nuclear Safety Commission. (2018db). *REGDOC-3.1.2, Reporting Requirements, Volume I: Non-Power Reactor Class I Nuclear Facilities and Uranium Mines and Mills.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc3-1-2-v1/

Canadian Nuclear Safety Commission. (2019). *REGDOC-2.1.1, management system*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-1-1/

Canadian Nuclear Safety Commission. (2020a, March). *Fitness for Duty, Volume II: Managing Alcohol and Drug Use, version 3.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/comment/regdoc2-2-4-ver3/review/#sec3-6

Canadian Nuclear Safety Commission. (2020b). CNSC departmental results report 2019–20. https://nuclearsafety.gc.ca/eng/resources/publications/reports/departmental/drr-2019-2020/index.cfm

Canadian Nuclear Safety Commission. (2020c). *REGDOC-3.1.3, reporting requirements for waste nuclear substance licensees, Class II nuclear facilities and users of prescribed equipment, nuclear substances and radiation devices.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc3-1-3/

Canadian Nuclear Safety Commission. (2021a). *DIS-21-03, cyber security and the protection of digital information*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/history/cyber-security-and-the-protection-of-digital-information-dis-21-03/

Canadian Nuclear Safety Commission. (2021b). *Discussion paper DIS-21-02, proposals to amend the Nuclear Security Regulations*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/history/proposals-to-amend-the-nuclear-security-regulations-dis-21-02/

Canadian Nuclear Safety Commission. (2021c). 2021–22 departmental plan. https://nuclearsafety.gc.ca/eng/resources/publications/reports/rpp/dp-2021-2022/index.cfm

Canadian Nuclear Safety Commission. (2021d). *CNSC departmental results report 2020–21*. https://nuclearsafety.gc.ca/eng/resources/publications/reports/departmental/drr-2020-2021/index.cfm

Canadian Nuclear Safety Commission. (2021e). *DIS-21-03, Cyber Security and the Protection of Digital Information.* https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/history/cyber-security-and-the-protection-of-digital-information-dis-21-03/

Canadian Nuclear Safety Commission. (2022a). *DIS-22-02, proposals to amend the REGDOC 2.12 nuclear security series*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/consultation/dis-22-02/

Canadian Nuclear Safety Commission. (2022b). CNSC departmental results report 2021–22 . https://nuclearsafety.gc.ca/eng/resources/publications/reports/departmental/drr-2021-2022/index.cfm

Canadian Nuclear Safety Commission. (2022c, November). *Canada Gazette, Part I, Volume 156, Number 46: Nuclear Security Regulations, 2023*. https://gazette.gc.ca/rp-pr/p1/2022/2022-11-12/html/reg1-eng.html

Canadian Nuclear Safety Commission. (2023a). *Changes to regulation of cyber security for Canadian nuclear facilities and activities*. https://www.cnsc-ccsn.gc.ca/eng/resources/research/technical-papers-and-articles/2023/changes-to-regulation-of-cyber-security-for-canadian-nuclear-facilities-and-activities/

Canadian Nuclear Safety Commission. (2023b). CNSC departmental results report 2022–23. https://nuclearsafety.gc.ca/eng/resources/publications/reports/departmental/drr-2022-2023/index.cfm

Canadian Nuclear Safety Commission. (2023c). *Changes to regulation of cyber security for Canadian nuclear facilities and activities*. https://www.cnsc-ccsn.gc.ca/eng/resources/research/technical-papers-and-articles/2023/changes-to-regulation-of-cyber-security-for-canadian-nuclear-facilities-and-activities/

Canadian Nuclear Safety Commission. (2024a). *Canadian Nuclear Safety Commission 2024–25 Departmental Plan.* https://www.cnsc-ccsn.gc.ca/eng/resources/publications/reports/rpp/dp-2024-2025/

Canadian Nuclear Safety Commission. (2024b). *CNSC forward regulatory plan: 2024–2026*. https://www.cnsc-ccsn.gc.ca/eng/acts-and-regulations/regulatoryplan/forward-regulatory-plan-details/

Canadian Nuclear Safety Commission, UK Office for Nuclear Regulation, US Nuclear Regulatory Commission. (2024). *Considerations for Developing Artificial Intelligence Systems in Nuclear Applications.* https://www.nrc.gov/docs/ML2424/ML24241A252.pdf

Canadian Nuclear Safety Commission. (2025a). *Canadian Nuclear Safety Commission 2023–24 Departmental Results Report*. https://www.cnsc-ccsn.gc.ca/eng/resources/publications/reports/departmental/drr-2023-2024/

Canadian Security Intelligence Service. (2025). *China's intelligence law and the country's future intelligence competitions*. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html

Canadian Standards Association. (2021). *N290.7-14 (R2021) Cyber security for nuclear power plants and small reactor facilities.*

Canadian Standards Association. (2022). *CSA N286:12 (R2022) Management system requirements for nuclear facilities.*

CBC News. (2014). *Klaus Nielsen pleads guilty to trying to export infectious agent.* https://www.cbc.ca/news/canada/ottawa/klaus-nielsen-pleads-guilty-to-trying-to-export-infectious-agent-1.2735012

Charney, D.L. (2010). True Psychology of the insider spy. *Intelligencer: Journal of U.S. Intelligence Studies*. P.47-54.

Class I Nuclear Facilities Regulations (SOR/2000-204)

Class II Nuclear Facilities and Prescribed Equipment Regulations (SOR/2000-205)

Colley Borden, S. (2019). Convicted spy Jeffrey Delisle released on full parole. *CBC News.* https://www.cbc.ca/news/canada/nova-scotia/convicted-spy-russians-canadian-armed-forces-parole-1.5049166#:~:text=Convicted%20spy%20Jeffrey%20Delisle%20has,and%20its%20allies%20to%20Russia.

Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology TRA-1.* https://www.cyber.gc.ca/sites/default/files/cyber/publications/tra-emr-1-e.pdf

Criminal Code, R.S.C. (1985). c. C-46.

Cybersecurity & Infrastructure Security Agency. (2024, July). *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Program*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

Dahl, F. (2014, June). *Seized nuclear material in Iraq "low grade" - U.N. agency.* Reuters. https://www.reuters.com/article/world/seized-nuclear-material-in-iraq-low-grade-u-n-agency-idUSKBN0FF0TB/

De Falco. M. (2012). *Stuxnet Facts Report. A Technical and Strategic Analysis*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Department of Finance. (2023). *Internal audit of the personnel security screening process - Internal audit report*. Government of Canada. https://www.canada.ca/en/department-finance/corporate/transparency/audits-evaluations/2023/audit-personnel-security-screening-process.html

Department of Justice. (2025). *Nuclear security regulations (SOR/2000-209)*. Government of Canada. https://laws.justice.gc.ca/eng/regulations/sor-2000-209/page-1.html

Department of National Defence. (2023). *Security woes in a fish generation world: CAF security clearance process is unfit for purpose*. Canadian Forces College. https://www.cfc.forces.gc.ca/259/290/49/192/Anon903.pdf

Dias, T., Hakmeh, J., & Messmer, M. (2024). *Cybersecurity of the civil nuclear sector threat landscape and international legal protections in peacetime and conflict*. Chatham House. https://www.chathamhouse.org/2024/07/cybersecurity-civil-nuclear-sector

Diller, S. J., Czibor, A., Szabo, Z., Restas, P., Jonas, E., & Frey, D. (2021). The positive connection between dark triad traits and leadership levels in self- and other- ratings. *Leadership, Education, Personality: An Interdisciplinary Journal*. Volume 3, 117–131.

Doody, J. (2023). Discussion on the *Security of Information Act* legal and enforcement challenges. (A. Crowe, Interviewer)

Dubé, Y. (2024). Discussion on frequency of regulatory inspections of cybersecurity program. (A. Crowe, Interviewer)

Dubé, Y. (2025). Discussion on frequency of regulatory inspections of information security program. (A. Crowe, Interviewer)

Durocher, W. (2024). Discussion on the frequency of regulatory inspections of personnel security program. (A. Crowe, Interviewer)

Emergency Management and Civil Protection Act (R.S.O., 1990, c. E.9)

G7. (2025). *G7 leaders' statement on transnational repression.* G7 2025 Kananaskis. https://g7.canada.ca/en/news-and-media/news/g7-leaders-statement-on-transnational-repression/

General Nuclear Safety and Control Regulations (SOR/2000-202)

George Washington Program on Extremism. (2025, August). *Atomwaffen Division (AWD)*. George Washington University. https://extremism.gwu.edu/atomwaffen-division-awd

Global Affairs Canada. (2023). *Canada signs deal to refurbish CANDU reactor at Cernavoda Nuclear Power Plant in Romania.* Government of Canada. https://www.canada.ca/en/global-affairs/news/2023/11/canada-signs-deal-to-refurbish-candu-reactor-at-cernavoda-nuclear-power-plant-in-romania.html

Gordon, R. (2012). Early clues to navy spy Delisle's guilt overlooked. *CBC News*. https://www.cbc.ca/news/canada/early-clues-to-navy-spy-delisle-s-guilt-overlooked-1.1235506

Government of Canada. (2022). *Canada Gazette, Part I, Volume 156, Number 46: Nuclear Security Regulations, 2023.* https://gazette.gc.ca/rp-pr/p1/2022/2022-11-12/html/reg1-eng.html

Government of Ontario. (2023). *Emergency Management and Civil Protection Act, R.S.O. 1990, c. E.9*. https://www.ontario.ca/laws/statute/90e09

Government of Ontario. (2024). *Electricity Act, 1998, S.O. 1998, c. 15, Sched. A*. https://www.ontario.ca/laws/statute/98e15

Greig, J. (2022). *US Nuclear Security Administration criticized by watchdog over cybersecurity failures.* The Record. Recorded Future. https://therecord.media/us-nuclear-security-administration-criticized-by-watchdog-over-cybersecurity-failures

Greig, J. (2024). *North Korean hacking group targeted weapons blueprints, nuclear facilities in cyber campaigns.* Recorded Future. https://therecord.media/north-korea-andariel-apt45-weapons-systems-nuclear-facilities

Guay, F. (2024). The cybersecurity skills crisis: Canada's call to action. *Financial Post*. https://financialpost.com/technology/tech-news/the-cybersecurity-skills-crisis-canadas-call-to-action

Harms, P.D., Marbut, A., Johnston, A.C., Lester, P., Fezzey, T. (2022). Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats. *Journal of Information Security and Applications*. Volume 71, Issue C.

Hobbs, C., Pope, N. (2015). *Insider Threat Case Studies at Radiological and Nuclear Facilities*. Los Alamos National Laboratories. https://www.osti.gov/servlets/purl/1177991/

House of Commons Canada. (2024). *Bill C-26 an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts adopted by the House on June 19, 2024, report and government response*. *https://www.ourcommons.ca/committees/en/SECU/StudyActivity?studyActivityId=12223563*

House of Commons Canada. (2025). *Bill C-8 an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, first reading June 18, 2025.* https://www.parl.ca/DocumentViewer/en/45-1/bill/C-8/first-reading

IBM & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.

IBM Security. (2024). *Cost of a Data Breach Report 2024.* IBM Corporation.

ICS2. (2024). *Employers must act as cybersecurity workforce growth stalls and skills gaps widen.* https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

Institute for Economics & Peace. (2025). *Global Terrorism Index 2025.* http://visionofhumanity.org/resources

Interagency Security Committee. (2024). *The risk management process for federal facilities: an interagency security committee standard*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2024-07/The_Risk_Management_Process_2024_Edition.pdf

International Atomic Energy Agency. (2016). *International physical protection advisory service mission report: Canada.*

International Atomic Energy Agency. (2020a*). Nuclear security series No. 8-G – Preventive and protective measures against insider threats.*

International Atomic Energy Agency. (2020b). *Integrated regulatory review service (IRSS) to Canada*. https://www.iaea.org/sites/default/files/documents/review-missions/irrs_canada_2019_final_report.pdf

International Energy Agency. (2024). *World Energy Outlook 2024*. https://iea.blob.core.windows.net/assets/140a0470-5b90-4922-a0e9-838b3ac6918c/WorldEnergyOutlook2024.pdf

International Monetary Fund. (2025). *A critical juncture amid policy shifts.* https://www.imf.org/en/Publications/WEO/Issues/2025/04/22/world-economic-outlook-april-2025

International Trade Administration. (2023). *Canada – country commercial guide*. https://www.trade.gov/country-commercial-guides/canada-energy

Jonason, P.K., Davis, M.K. (2018). A gender role view of the Dark Triad traits. *Personality and Individual Differences Volume 125,* 102-105.

Kenyon, J., Baker-Beall, C., & Binder, J. (2021). Lone-Actor Terrorism – A Systematic Literature Review. *Studies in Conflict & Terrorism*, 46(10), 2038–2065.

Lang, E. (2022). Seven (Science-Based) Commandments for Understanding and Countering Insider Threats. *Counter-Insider Threat Research and Practice.* https://citrap.scholasticahq.com/article/37321-seven-science-based-commandments-for-understanding-and-countering-insider-threats

Mailey., J. R. (2024). *Iran's criminal statecraft – How Theran weaponizes illicit markets*. Global Initiative Against Transnational Organized Crime. Geneva. https://globalinitiative.net/wp-content/uploads/2024/10/JR-Malley-Irans-critical-statecraft-How-Tehran-weaponizes-illicit-markets-GI-TOC-October-2024.pdf

Mandel, M. (2022). MANDEL: One of the world's most active cyberpirates pleads guilty. *Toronto Sun*. https://torontosun.com/news/local-news/mandel-one-of-the-most-active-cyberpirates-in-the-world-pleads-guilty-in-brampton

Miller, M., Nickel, D. (2025). *Tech companies have a big remote worker problem: North Korean operatives*. POLITICO. https://www.politico.com/news/2025/05/12/north-korea-remote-workers-us-tech-companies-00340208

New Jersey Cybersecurity and Communication Cell. (2025, August). *Nuclear Reactors, Materials, and Waste Sector Threat Analysis Report*. https://www.cyber.nj.gov/grants-and-resources/critical-infrastructure-cybersecurity-outreach-program/sector-threat-analysis-reports/nuclear-reactors-materials-and-waste-sector-threat-analysis-report

Nord, M., Angiolillo, F., Goof God, A., Lindberg, S.I. (2025, March). State of the world 2024: 25 years of autocratization – democracy trumped? *Democratization*. Volume 32, Issue 4, 839–864.

Nuclear Security Summit. (2016, March). *National Progress Report: Canada. https://www.nss2016.org/document-center-docs/2016/4/5/national-progress-report-canada*

Nuclear Security Regulations (SOR/2000-209)

Ontario Electricity Act (R.S.O., 1998)

Parliament of Canada. (2024). Bill *C-26 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. https://www.parl.ca/legisinfo/en/bill/44-1/c-26

Ponemon Institute & DTEX. (2025). *Cost of insider risks – global report 2025*.

Public Safety Canada. (2022). *Enhancing Canada's critical infrastructure resilience to insider risk*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx

R v. Cameron Ortis, 2023 ONSC 3113, 19-20044 (Ontario Superior Court of Justice May 24, 2023).

Rabson, M. (2023). Canada signs $3B nuclear deal with Romania, as Europe aims to wean off Russian energy. *CTV News*. https://www.ctvnews.ca/business/article/canada-signs-3b-nuclear-deal-with-romania-as-europe-aims-to-wean-off-russian-energy/

Rajagopal, D. (2024). Chinese money still chasing Canadian critical mining deals despite Ottawa's scrutiny. *Reuters*. https://www.reuters.com/markets/commodities/chinese-money-still-chasing-canadian-critical-mining-deals-despite-ottawas-2024-02-27/

Research and Markets. (2024). *Canadian Nuclear Medicine Market Analysis Report 2024-2030.* GlobeNewswire. https://www.globenewswire.com/news-release/2024/01/24/2814965/28124/en/Canada-Nuclear-Medicine-Market-Analysis-Report-2024-2030-Featuring-Nordion-Lantheus-Medical-Imaging-Cardinal-Health-Jubilant-Life-Sciences-Isologic-Innovative-Radiopharmaceuticals-.html

Reuters. (2013). *UN nuclear agency says malware infected some computers*. https://www.reuters.com/article/nuclear-iaea-malware-idUSL5N0IC1HN20131022/

Reuters. (2021). *Brazil's Eletrobras says nuclear unit hit with cyberattack. https://www.reuters.com/business/energy/brazils-eletrobras-says-nuclear-unit-hit-with-cyberattack-2021-02-04/*

Roman, K. (2015). Klaus Nielsen, scientist who tried to smuggle contagious bacteria, begins sentencing hearing. *CBC News.* https://www.cbc.ca/news/canada/ottawa/klaus-nielsen-scientist-who-tried-to-smuggle-contagious-bacteria-begins-sentencing-hearing-1.3124559

Royal Canadian Mounted Police. (2022). *Hydro-Québec employee charged with espionage.* https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage

Royal Canadian Mounted Police. (2023). *Retired RCMP officer charged with foreign interference*. https://www.rcmp-grc.gc.ca/en/news/2023/retired-rcmp-officer-charged-foreign-interference

Royal Canadian Mounted Police. (2024). *RCMP arrests one individual for communicating safeguarded information in relation to critical infrastructure*. https://www.rcmp-grc.gc.ca/en/news/2024/rcmp-arrests-individual-communicating-safeguarded-information-relation-critical

Sapien Labs. (2025). *Mental State of the World in 2024*. https://sapienlabs.org/wp-content/uploads/2025/02/Mental-State-of-the-World-2024-Online-Feb-26.pdfs

Security of Information Act (R.S.C., 1985, c. O-5)

Seymour, A. (2017). Canadian government scientist who smuggled bacteria in carry-on luggage gets prison time. *Ottawa Citizen*. https://ottawacitizen.com/news/local-news/canadian-government-scientist-who-smuggled-bacteria-in-carry-on-luggage-gets-prison-time

Scharff, C. (2024). *Dix ans après, le sabotage de Doel 4 toujours pas élucidé*. L'Écho.

https://www.lecho.be/economie-politique/belgique/general/dix-ans-apres-le-sabotage-de-doel-4-toujours-pas-belucide/10558774.html

Sharwood, S. (2022). *Hacktivists say they stole 100,000 emails from Iran's nuclear energy agency.* The Record. https://www.theregister.com/2022/10/24/black_reward_iran_nuclear_leak/

Shoham, D. (2020). China and Viruses: The Case of Dr. Xiangguo Qiu*. The COVID-19 Crisis: Impact and Implications*. Begin-Sadat Center for Strategic Studies. http://www.jstor.org/stable/resrep26356.30

Statistics Canada. (2023). *Study: Mental disorders and access to mental health care*. https://www150.statcan.gc.ca/n1/daily-quotidien/230922/dq230922b-eng.htm

Statistics Canada. (2024). *Energy-related research and development expenditures, 2022.* https://www150.statcan.gc.ca/n1/daily-quotidien/240919/dq240919b-eng.htm

Software Engineering Institute (2022). *Common Sense Guide to Mitigating Insider Threats, Seventh Edition*. https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

Strider. (2022). "*The Los Alamos Club:" New Report Details China's Efforts to Recruit Leading U.S. Department of Energy Scientists to Advance Defense Technology Programs for the People's Republic of China.* https://www.striderintel.com/newsroom/the-los-alamos-club-new-report-details-chinas-efforts-to-recruit-leading-u-s-department-of-energy-scientists-to-advance-defense-technology-programs-for-the-people/

The Canadian Press. (2013). CSIS knew of navy spy's activity, left RCMP in the dark. *CBC News*. https://www.cbc.ca/news/canada/nova-scotia/csis-knew-of-navy-spy-s-activity-left-rcmp-in-the-dark-1.1312803#:~:text=Canada's%20spy%20agency%20clandestinely%20watched,could%20have%20been%20arrested%20sooner.

The White House. (2021). *FACT SHEET: The Biden-Harris Administration has launched an all-of government effort to address colonial pipeline incident*. https://www.whitehouse.gov/briefingroom/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-haslaunched-an-all-of-government-effort-to-address-colonial-pipeline-incident/

Treasury Board Secretariat. (2025). *Directive on Security Screening*. Government of Canada. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32805#appG

Tunney, C. (2024). Lies and scandal: How two rogue scientists at a high-security lab triggered a national security calamity. *CBC News. https://www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7130284*

Twenge, J. M., Miller, J. D., & Campbell, W. K. (2014). The *narcissism epidemic: Commentary on Modernity and narcissistic personality disorder*. Personality Disorders: Theory, Research, and Treatment, 5(2), 227–229.

Uranium Mines and Mills Regulations (SOR/2000-206)

U.S. Department of Justice. (2016). *Former U.S. Nuclear Regulatory Commission Employee Sentenced to Prison for Attempted Spear-Phishing Cyber-Attack On Department of Energy Computers.*

U.S. Department of Justice. (2018). *Neo-Nazi Leader Sentenced to Five Years in Federal Prison for Explosives Charges.* https://www.justice.gov/archives/opa/pr/neo-nazi-leader-sentenced-five-years-federal-prison-explosives-charges

U.S. Department of Justice. (2021). *Iranian National Charged with Illegally Exporting Laboratory Equipment from the United States to Iran*. https://www.justice.gov/usao-dc/pr/iranian-national-charged-illegally-exporting-laboratory-equipment-united-states-iran

U.S. Department of Justice. (2023). *Justice Department Announces Charges and Sentence in Connection with Iranian Procurement Network's Attempts to Acquire Sophisticated Military Technology.*

U.S. Department of Justice. (2025a). *Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes.* https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

U.S. Department of Justice. (2025b). *Arizona Woman Sentenced in $17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea. https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north*

U.S. Department of Justice. (2025c). *Japanese Yakuza Leader Pleads Guilty to Nuclear Materials Trafficking, Narcotics, and Weapons Charges*. [Archived]. https://www.justice.gov/archives/opa/pr/japanese-yakuza-leader-pleads-guilty-nuclear-materials-trafficking-narcotics-and-weapons

U.S. Department of Justice. (2025d). *White Supremacist Leader Found Guilty of Conspiring to Destroy Regional Power Grid*. https://www.justice.gov/usao-md/pr/white-supremacist-leader-found-guilty-conspiring-destroy-regional-power-grid

Vanderklippe, N., Chase, S., Fife, R. (2024). Fired Winnipeg scientists use pseudonyms in China as RCMP probe continues. *The Globe and Mail*. https://www.theglobeandmail.com/politics/article-fired-winnipeg-scientists-china/

Walsh, J. (2021). Ransomware attack shuts down massive east coast gasoline pipeline. *Forbes*. https://www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/

Woloshyn, R., Denis, M.-M., & Guerriero, L. (2022). Taking down a ransomware hacker. *CBC News - The Fifth Estate.* https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker

World Bank. (2025). *Global Economy Set for Weakest Run Since 2008 Outside of Recessions*. https://www.worldbank.org/en/news/press-release/2025/06/10/global-economic-prospects-june-2025-press-release

World Economic Forum. (2020). *Partnerships are our best weapon in the fight against cybercrime. Here's why.* https://www.weforum.org/stories/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/

World Health Organization. (2022). *World Mental Health Report*. United Nations. https://iris.who.int/bitstream/handle/10665/356119/9789240049338-eng.pdf?sequence=1

World Nuclear Association. (2022). *World energy needs and nuclear power*. https://worldnuclear.org/information-library/current-and-future-generation/world-energy-needs-andnuclearpower.aspx#:~:text=In%20IEO%2D2016%2C%20nuclear%20power,2.3%20PWh%20to%204.5%20PWh.

World Nuclear Association. (2024). *World Uranium mining production*. https://world nuclear.org/information-library/nuclear-fuel-cycle/mining-of-uranium/world-uranium-mining-production

Yrondi, A., Rouyre, P., Schmitt, L. (2015). La personnalité narcissique devient-elle plus fréquente? Fait culturel ou fait clinique? *Annales Médico-psychologiques, revue psychiatrique.* Volume 173, Issue 4, 331-334.

Zul-Azri, I., Fiza, A., Anis, A., Norziana, J., & Harisk Iskandar Mohd, A. (2022). Insider threats: profiling potential malicious attacks, severity and impact. *Journal of Theoretical and Applied Information Technology.* Volume 100, Issue 13, 4827-4838.

Zweig, D., Kang, S. (2020). *America challenges China's National Talent Programs*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20505_zweig_AmericaChallenges_v6_FINAL.pdf

6. Appendix A – Threat Assessment Results

The results of the threat assessment are presented in the table below.

Threat Assessment - Insider Threat in the Canadian Nuclear Industry					
Threat Actor Category	Threat Activity	Threat Impact	Likelihood	Threat Level	Threat Score
State or State-Sponsored Actors	Cyberattack	High	High	V. High	5
State or State-Sponsored Actors	Espionnage/Theft of IP/Data Leak	High	High	V. High	5
State or State-Sponsored Actors	Sabotage	High	High	V. High	5
Criminal Organizations	Cyberattack	High	High	V. High	5
Criminal Organizations	Espionnage/Theft of IP/Data Leak	Medium	V. Low	V. High	5
Criminal Organizations	Sabotage	High	High	V. High	5
State or State-Sponsored Actors	Procurement or Installation of Counterfeit or Compromised Equipment or Software	High	Medium	High	4
Lone-Wolf Insider	Sabotage	High	Medium	High	4
IMVE	Cyberattack	Medium	High	High	4
State or State-Sponsored Actors	Fraud	High	Low	Medium	3
State or State-Sponsored Actors	Subversion/MDM	Medium	Medium	Medium	3
Lone-Wolf Insider	Cyberattack	Medium	Medium	Medium	3
Lone-Wolf Insider	Espionnage/Theft of IP/Data Leak	Medium	Medium	Medium	3
Lone-Wolf Insider	Fraud	Medium	Medium	Medium	3
IMVE	Fraud	Medium	Medium	Medium	3
IMVE	Sabotage	Medium	Medium	Medium	3
Criminal Organizations	Procurement or Installation of Counterfeit or Compromised Equipment or Software	Medium	V. Low	Medium	3
Lone-Wolf Insider	Procurement or Installation of Counterfeit or Compromised Equipment or Software	Medium	Low	Low	2
IMVE	Espionnage/Theft of IP/Data Leak	Medium	Low	Low	2
IMVE	Subversion/MDM	Medium	Low	Low	2
Criminal Organizations	Fraud	Medium	Medium	Low	2
Lone-Wolf Insider	Subversion/MDM	V. Low	Low	V. Low	1
IMVE	Procurement or Installation of Counterfeit or Compromised Equipment or Software	Low	V. Low	V. Low	1
Criminal Organizations	Subversion/MDM	Low	V. Low	V. Low	1

7. Appendix B – Legislative and Nuclear Regulatory Safeguards

The 25 legislative and nuclear regulatory safeguards below were assessed as part of the TRA.

Current and upcoming legislation:

1. Bill C-25, now bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (Bill-C26, 2024)
2. *Canada Labour Code (R.S.C., 1985, c. L-2), Section 143* (False Information)
3. *Criminal Code (R.S.C., 1985, c. C-46), Section 342.1* (Unauthorized Use of Computer)
4. *Criminal Code (R.S.C., 1985, c. C-46), Section 372* (False Information)
5. *Criminal Code (R.S.C., 1985, c. C-46), Section 380* (Fraud)
6. *Criminal Code (R.S.C., 1985, c. C-46) Part II, Section 83* (Nuclear Terrorism)
7. *Criminal Code (R.S.C., 1985, c. C-46), Section 391* (Trade Secret)
8. Emergency Management and Civil Protection Act (R.S.O., 1990, c. E.9)
9. *Ontario Electricity Act* (R.S.O., 1998)
10. *Security of Information Act* (R.S.C., 1985, c. O-5)

Nuclear legislation and regulations:

11. *General Nuclear Safety and Control Regulations (SOR/2000-202)*
12. *Class I Nuclear Facilities Regulations (SOR/2000-204)*
13. *Class II Nuclear Facilities and Prescribed Equipment Regulations (SOR/2000-205)*
14. *Uranium Mines and Mills Regulations (SOR/2000-206)*
15. *Nuclear Security Regulations (SOR/2000-209)*

Nuclear regulatory documents and regulatory activities:

16. *REGDOC-2.1.1, Management System* (CNSC, 2019)
17. *REGDOC-2.2.4, Fitness for Duty* (CNSC, 2015)
18. *REGDOC-2.12.2, Site Access Security Clearance* (CNSC, 2014a)
19. *REGDOC-2.13.1, Safeguards and Nuclear Material Accountancy* (CNSC, 2018a)
20. *REGDOC-3.1.1 Reporting Requirements for Nuclear Power Plants* (CNSC, 2014b)
21. *REGDOC-3.1.2, Reporting Requirements, Volume I: Non-Power Reactor Class I Nuclear Facilities and Uranium Mines and Mills* (CNSC, 2018b)
22. *REGDOC-3.1.3, Reporting Requirements for Waste Nuclear Substance Licensees, Class II Nuclear Facilities and Users of Prescribed Equipment, Nuclear Substances and Radiation Devices* (CNSC, 2020c)
23. Regulatory and/or IAEA Inspections

Mandatory standards:

24. *CSA N286, Management system requirements for nuclear facilities* (CSA, 2022)
25. *CSA N290.7, Cyber security for nuclear facilities* (CSA, 2021)

8. Appendix C - Residual Risk Computation

The results of the residual risk computation if threats, vulnerabilities, and impact scores are shown in the table below.

Critical Asset	Asset Score (impact)	Threat Activity	Threat Score	Vulnerability Score	Residual Risk Score	Residual Risk Level
Nuclear Power Plants	5	Cyberattack	5	4	91	Very High
Nuclear Power Plants	5	Espionage/Theft of IP/Data Leak	5	4	88	Very High
Uranium Mines & Mills	4	Cyberattack	5	4	87	Very High
Uranium Mines & Mills	4	Espionage/Theft of IP/Data Leak	5	4	82	Very High
Uranium Mines & Mills	4	Sabotage	5	4	82	Very High
Nuclear Fuel Processing Facilities	4	Cyberattack	5	4	78	High
Nuclear Fuel Processing Facilities	4	Espionage/Theft of IP/Data Leak	5	4	76	High
Nuclear Power Plants	5	Sabotage	5	3	75	High
Nuclear Fuel Processing Facilities	4	Sabotage	5	4	74	High
Supply Chain	3	Cyberattack	5	5	69	High
Supply Chain	3	Sabotage	5	5	68	High
Supply Chain	3	Espionage/Theft of IP/Data Leak	5	4	66	High
Research Reactors Non-High Security	3	Cyberattack	5	4	65	High
Class II Medical and Research Facilities	3	Cyberattack	5	4	65	High
Research Reactors Non-High Security	3	Espionage/Theft of IP/Data Leak	5	4	63	High
Research Reactor High Security	3	Cyberattack	5	4	63	High
Nuclear Power Plants	5	Procurement or Installation of Counterfeit or Compromised Equipm	4	3	62	High
Class II Medical and Research Facilities	3	Espionage/Theft of IP/Data Leak	5	4	62	High
Class II Medical and Research Facilities	3	Sabotage	5	4	61	High
Uranium Mines & Mills	4	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	60	High
Research Reactors Non-High Security	3	Sabotage	5	4	60	High
Research Reactor High Security	3	Espionage/Theft of IP/Data Leak	5	4	60	High
Nuclear Fuel Processing Facilities	4	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	59	High
Research Reactor High Security	3	Sabotage	5	4	59	High
Supply Chain	3	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	53	High
Research Reactors Non-High Security	3	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	45	High
Nuclear Power Plants	5	Fraud	3	3	45	High
Class II Medical and Research Facilities	3	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	45	High
Research Reactor High Security	3	Procurement or Installation of Counterfeit or Compromised Equipm	4	4	42	High
Uranium Mines & Mills	4	Fraud	3	3	38	High
Nuclear Fuel Processing Facilities	4	Fraud	3	3	36	High
Supply Chain	3	Fraud	3	4	35	Medium
Class II Medical and Research Facilities	3	Fraud	3	3	30	Medium
Nuclear Power Plants	5	Subversion/MDM	3	2	30	Medium
Nuclear Fuel Processing Facilities	4	Subversion/MDM	3	2	29	Medium
Uranium Mines & Mills	4	Subversion/MDM	3	2	28	Medium
Research Reactors Non-High Security	3	Fraud	3	3	28	Medium
Supply Chain	3	Subversion/MDM	3	3	27	Medium
Research Reactor High Security	3	Fraud	3	3	27	Medium
Class II Medical and Research Facilities	3	Subversion/MDM	3	2	21	Medium
Research Reactors Non-High Security	3	Subversion/MDM	3	2	20	Medium
Research Reactor High Security	3	Subversion/MDM	3	2	20	Medium