A Cyber Risk Management Framework to Address Evolving Threats in U.S. and Canadian Critical Infrastructure

GIDEON OPEYEMI BABATUNDE[1], ABIDEMI ADELEYE ALABI[2], SIKIRAT DAMILOLA MUSTAPHA[3], ADEBIMPE BOLATITO IGE[4]
[1] *KPMG, Calgary, Canada*
[2] *Ericsson Telecommunications Inc., Lagos, Nigeria*
[3] *Kwara State University, Malete, Nigeria*
[4] *Independent Researcher, Canada*

Abstract- ***The growing reliance on interconnected systems has heightened the vulnerability of critical infrastructure in the U.S. and Canada to cyber threats. These threats, evolving in sophistication and frequency, underscore the urgent need for robust cyber risk management frameworks tailored to protect essential sectors such as energy, transportation, and healthcare. This paper proposes a comprehensive Cyber Risk Management Framework designed to address these emerging challenges, emphasizing resilience, adaptability, and cross-border collaboration. The framework integrates key elements, including proactive risk assessment, advanced threat intelligence, and real-time monitoring, to enhance the detection and mitigation of cyberattacks. It leverages cutting-edge technologies such as artificial intelligence (AI) and machine learning (ML) to predict and respond to threats with greater precision. Furthermore, the framework incorporates compliance with regulatory requirements in both countries, ensuring alignment with standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Canada's Cyber Security Strategy. A cornerstone of the proposed approach is fostering public-private partnerships to enable information sharing, joint incident response, and resource pooling. Recognizing the interconnected nature of critical infrastructure, the framework promotes a collaborative security posture across sectors and borders. Additionally, it addresses the human factor by advocating for continuous training programs to enhance cybersecurity awareness among stakeholders. Case studies highlight the framework's application in mitigating ransomware attacks and securing industrial control systems (ICS). The findings demonstrate improved resilience against cyber disruptions, reduced response times, and enhanced recovery processes. This work also identifies challenges, such as legal barriers to information sharing and the need for standardized metrics to measure effectiveness. In conclusion, this Cyber Risk Management Framework represents a strategic initiative to safeguard the critical infrastructure of the U.S. and Canada against evolving cyber threats. By leveraging technology, fostering collaboration, and ensuring regulatory compliance, the framework aims to enhance the resilience of critical systems and protect the economies and societies dependent on them.***

Indexed Terms- ***Cyber Risk Management, Critical Infrastructure, U.S., Canada, Cybersecurity Framework, Threat Intelligence, Public-Private Partnerships, AI, Machine Learning, Resilience***

I. INTRODUCTION

Critical infrastructure in the U.S. and Canada plays a pivotal role in supporting essential services such as energy, healthcare, finance, and communication, making it a prime target for cyber threats. The increasing reliance on interconnected systems has led to a more complex and vulnerable cyber landscape. As these systems become more integrated, the potential for cascading failures due to cyberattacks has escalated, putting not only national security but also economic stability at risk (Dalal, Abdul & Mahjabeen, 2016, Shafqat & Masood, 2016). The sophistication and frequency of cyberattacks targeting critical infrastructure have surged, with adversaries leveraging advanced techniques to breach defenses, compromise sensitive data, and disrupt operations. This growing threat necessitates a strategic approach to managing and mitigating cyber risks.

The objective of this paper is to propose a comprehensive Cyber Risk Management Framework

(CRMF) designed specifically for critical infrastructure in the U.S. and Canada. This framework seeks to address the unique challenges posed by the evolving cyber threat landscape. By focusing on resilience, the CRMF aims to enable organizations to better anticipate, prepare for, and recover from cyber incidents (Bodeau, McCollum & Fox, 2018, Georgiadou, Mouzakitis & Askounis, 2021). Adaptability is also a core principle, ensuring that the framework can evolve in response to emerging threats and technologies. Furthermore, the framework emphasizes collaboration, recognizing that the interconnected nature of critical infrastructure requires coordination across sectors and borders. It advocates for the sharing of threat intelligence and best practices to strengthen collective cybersecurity efforts (Elujide, et al., 2021). Through these guiding principles, the proposed framework will provide a robust, scalable approach to cyber risk management, enhancing the protection of critical infrastructure in both nations.

2.1. Overview of Critical Infrastructure in the U.S. and Canada

Critical infrastructure in both the United States and Canada is the backbone of essential services and is fundamental to the functioning of daily life. These critical sectors—ranging from energy to transportation, healthcare, and communications—are all deeply interconnected, making them vulnerable to various cyber threats that have grown in both frequency and sophistication. With the increasing reliance on digital systems and interconnected technologies, the protection of these vital sectors has become an urgent priority for both governments and private entities.

The energy sector, encompassing electricity, oil, and gas, is one of the most crucial components of critical infrastructure in both nations. It ensures that power is available for residential, industrial, and commercial purposes. The sector has become highly digitized, with power grids, pipelines, and electrical substations increasingly managed through sophisticated control systems like SCADA (Supervisory Control and Data Acquisition) (Buchanan, 2016, Clemente, 2018, Djenna, Harous & Saidouni, 2021). While these systems provide efficiency, they also create vulnerabilities. Cybercriminals or nation-state actors targeting power grids can cause extensive disruptions, leading to widespread power outages, economic losses, and even threats to national security. In 2015, a cyberattack in Ukraine demonstrated the potential impact on the energy sector, where hackers caused a major blackout by gaining control of electrical substations.

Similarly, the transportation sector, which includes air travel, rail systems, shipping, and road infrastructure, is another critical area of concern. Modern transportation systems rely on complex technologies for navigation, traffic control, and communication, many of which are vulnerable to cyberattacks. Transportation cybersecurity breaches can have severe consequences, including disruptions to daily commuting, supply chains, and the potential for physical damage (Aliyu, et al., 2020, Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). The 2017 ransomware attack on the shipping giant Maersk highlighted how interconnected global supply chains can be halted by cyberattacks. These disruptions also affect the healthcare sector, which is increasingly digital and reliant on interconnected systems for patient care, medical records, and operational management. The rise of ransomware attacks targeting healthcare organizations, such as the 2020 attack on Universal Health Services, underlined the vulnerabilities inherent in healthcare infrastructures. A cyberattack on hospitals can endanger lives by disrupting access to critical patient data, equipment, and operational systems, further exacerbating the strain on the healthcare system during emergencies. Boyson, 2014, presented a chart of Business ecosystem as shown in figure 1.

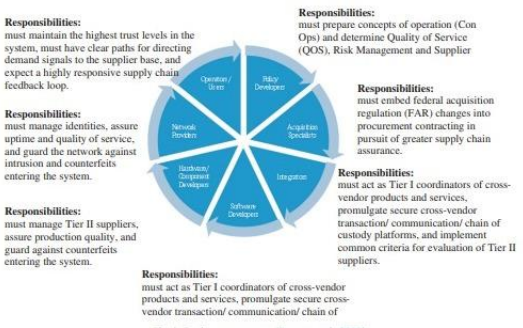

Figure 1: Business ecosystem (Boyson, 2014)

Other essential services, including finance, telecommunications, and water, also contribute to the larger ecosystem of critical infrastructure. These sectors underpin daily activities and are deeply interconnected with energy, transportation, and healthcare. A cyberattack on the financial sector can trigger cascading effects, leading to disruptions in payment systems, loss of financial data, and even undermining trust in the economy. Telecommunications, which provide the backbone for internet access, phone networks, and other communication channels, are similarly at risk (Djenna, Harous & Saidouni, 2021, Sabillon, Cavaller & Cano, 2016). Cyberattacks on these systems can affect national communication infrastructure, making it difficult for governments and businesses to communicate or coordinate responses during crises. Likewise, water systems that manage the distribution of clean water to communities can also be compromised, leading to significant health and environmental consequences.

These critical sectors share common vulnerabilities. First and foremost, the growing interconnectivity and digitization of infrastructure increase exposure to cyberattacks. Many of the control systems used in sectors such as energy and transportation were originally designed without cybersecurity considerations, making them susceptible to exploitation (Amin, 2019, Cherdantseva, et al., 2016, Dupont, 2019). These vulnerabilities are exacerbated by the use of legacy systems that are outdated and may no longer be supported or patched by manufacturers. Furthermore, the increasing use of third-party vendors and contractors to manage systems or provide services can introduce additional risks. Third-party vendors with weak cybersecurity measures can serve as gateways for attackers to gain access to critical systems, as demonstrated in the 2020 SolarWinds cyberattack, which affected multiple U.S. government agencies and private companies.

Another common vulnerability across critical sectors is the reliance on a centralized infrastructure model. This model can create single points of failure, where an attack on one critical component of the system can lead to cascading consequences. For instance, a disruption to the power grid could have far-reaching effects on transportation systems, telecommunications, and healthcare facilities (Kovacevic & Nikolic, 2015, Pomerleau, 2019). Additionally, critical sectors are often reliant on large amounts of sensitive data, which can become a target for cybercriminals seeking to steal intellectual property or personal information. Data breaches in the healthcare or financial sectors can have devastating impacts on individuals, leading to identity theft, financial loss, or compromised medical care (Elujide, et al., 2021). As the threat landscape evolves, these vulnerabilities become more pronounced, making it increasingly difficult to safeguard critical infrastructure against a wide array of cyberattacks. Figure 2 shows Risk transfer tools—the business of hazard insurance as presented by Schlegel & Trent, 2014.

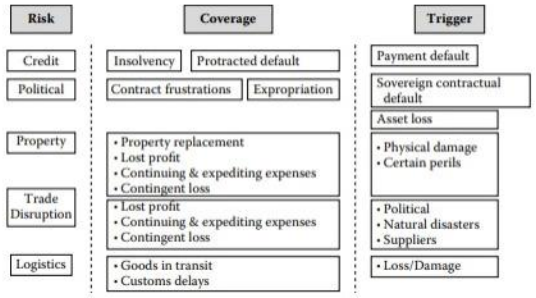

Figure 2: Risk transfer tools—the business of hazard insurance (Schlegel & Trent, 2014).

In response to these growing threats, both the U.S. and Canada have developed robust regulatory frameworks aimed at improving cybersecurity within critical infrastructure. In the U.S., the National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive approach to managing and reducing cybersecurity risks. The NIST framework is widely recognized and used by private companies and government entities across various sectors (Armenia, et al., 2021, Dupont, 2019). It focuses on five core functions—Identify, Protect, Detect, Respond, and Recover—that guide organizations through the process of managing cybersecurity risks. NIST emphasizes a risk-based approach, helping organizations prioritize resources and efforts according to the most critical assets and vulnerabilities.

Additionally, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) plays a crucial role in enhancing the security and resilience of critical infrastructure. CISA provides resources and guidance for sectors such as energy, transportation, and healthcare to bolster their cybersecurity posture. By working directly with private sector partners, CISA aims to identify risks, mitigate threats, and respond to incidents in real time (Armenia, et al., 2021, Dupont, 2019). The Federal Government also emphasizes the importance of information sharing between both private and public sectors to ensure a coordinated response to cyber threats. One such initiative is the Cybersecurity Information Sharing Act (CISA), which encourages private companies to share information about cyberattacks to improve the collective defense of critical infrastructure.

In Canada, the government's Cyber Security Strategy aims to strengthen the country's cyber resilience by fostering a coordinated, whole-of-government approach to cybersecurity. The strategy focuses on three key areas: securing critical infrastructure, increasing the resilience of the digital economy, and enhancing the ability to respond to cyber incidents. The strategy is designed to ensure that Canadian critical infrastructure is better protected against evolving cyber threats (Hussain, et al., 2021, Ike, et al., 2021). Canada's regulatory landscape also includes the Communications Security Establishment (CSE), which provides guidance and services to organizations on cybersecurity best practices. Furthermore, the Canadian Radio-television and Telecommunications Commission (CRTC) plays a key role in regulating the telecommunications industry, establishing standards for cybersecurity that ensure the protection of communications infrastructure.

While the regulatory frameworks in both countries are aligned in their goals of improving cybersecurity within critical sectors, there are differences in their specific approaches. The U.S. places significant emphasis on federal agencies like CISA and NIST to drive policy and implementation, whereas Canada's strategy is more decentralized, involving several government bodies and private entities in a collaborative approach (Austin-Gabriel, et al., 2021, Clarke & Knake, 2019, Oladosu, et al., 2021). Regardless, both nations recognize the importance of coordination between sectors and levels of government to ensure that critical infrastructure is protected against an evolving threat landscape.

In conclusion, critical infrastructure in both the U.S. and Canada is under increasing threat from cyberattacks that target interconnected and vulnerable systems across various sectors, including energy, transportation, healthcare, finance, and communications. The vulnerabilities present in these sectors are exacerbated by legacy systems, interdependencies, and reliance on third-party vendors (Austin-Gabriel, et al., 2021, Oladosu, et al., 2021). To combat these evolving threats, both nations have developed comprehensive regulatory frameworks to bolster cybersecurity and encourage cooperation between the private sector, government, and other stakeholders. By continuing to improve cybersecurity resilience, both countries can better protect their critical infrastructure from the growing cyber risk landscape.

2.2. Evolving Cyber Threat Landscape

The cyber threat landscape for critical infrastructure in the United States and Canada has evolved rapidly in recent years. As infrastructure systems become more interconnected and reliant on digital technologies, cybercriminals and state-sponsored actors have seized upon these vulnerabilities, devising increasingly sophisticated and targeted attacks. Critical infrastructure, such as energy grids, transportation systems, financial networks, and healthcare facilities, all form vital components of national security and economic stability. As such, these systems are prime targets for adversaries aiming to disrupt operations, steal sensitive data, or cause widespread damage (Aaronson & Leblond, 2018, Newlands, et al., 2020). The evolution of cyber threats poses significant challenges in safeguarding these critical systems, demanding the development of comprehensive risk management frameworks to address these growing risks.

Ransomware has emerged as one of the most prevalent and disruptive cyber threats targeting critical infrastructure. In these types of attacks, malicious actors infiltrate a system, encrypt critical files or systems, and demand payment, typically in

cryptocurrency, in exchange for the decryption key. Ransomware attacks can severely disrupt operations and cause extensive financial losses, as evidenced by the 2021 attack on the Colonial Pipeline in the U.S., which led to fuel shortages and logistical challenges (Igo, 2020). These attacks have grown in sophistication, with attackers not only encrypting data but also threatening to release sensitive information publicly, a tactic known as double extortion. This dual-pronged approach increases the pressure on organizations to comply with demands, as failure to do so may result in reputational damage and loss of customer trust in addition to operational disruption. Schlegel & Trent, 2014, presented Scenario and risk response planning as shown in figure 3.

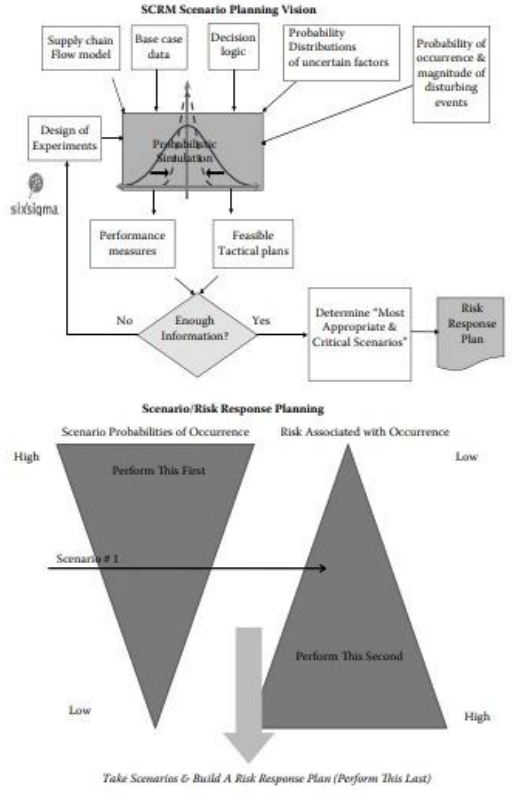

Figure 3: Scenario and risk response planning (Schlegel & Trent, 2014).

Another growing threat is supply chain attacks, which target third-party vendors or contractors that have access to critical infrastructure systems. In these attacks, cybercriminals compromise a trusted vendor, leveraging their access to infiltrate the networks and systems of their clients. The SolarWinds attack, discovered in late 2020, serves as a stark example of the devastating impact of supply chain breaches (Dwivedi, et al., 2020, Feng, 2019). This attack, believed to be perpetrated by a nation-state actor, compromised the software supply chain by inserting a backdoor into a widely used network management tool. The attack affected thousands of organizations, including U.S. government agencies and major corporations. The interconnectedness of modern supply chains means that an attack on one vendor can have far-reaching consequences, impacting multiple sectors of critical infrastructure simultaneously. This type of attack underscores the importance of rigorous vetting processes, continual monitoring of third-party vendors, and an emphasis on supply chain cybersecurity.

Industrial Control Systems (ICS) breaches are also an area of growing concern, particularly within the energy and manufacturing sectors. ICS systems, which are responsible for monitoring and controlling physical processes, are increasingly connected to broader IT networks, making them vulnerable to cyberattacks. Attacks targeting ICS infrastructure can result in physical damage to equipment, disruptions to essential services, or even safety hazards (Bamberger & Mulligan, 2015, Voss & Houser, 2019). One prominent example of such an attack occurred in 2010 when the Stuxnet worm targeted Iranian nuclear facilities, causing significant damage to centrifuges used for uranium enrichment. ICS breaches can have devastating consequences, especially when attackers seek to manipulate or disable critical infrastructure components. These types of attacks highlight the need for tailored cybersecurity solutions that specifically address the unique vulnerabilities of ICS systems.

In the face of these and other emerging threats, there are significant challenges to effectively mitigating cyber risks to critical infrastructure. One of the primary challenges is the rapid evolution of tactics employed by malicious actors. Cybercriminals and nation-state actors are constantly adapting and refining their techniques, making it increasingly difficult for organizations to stay ahead of the threat curve. Attackers leverage a wide range of tools, such as advanced malware, phishing schemes, and social engineering tactics, to gain access to systems and networks (Jathanna & Jagli, 2017). Moreover, the rise

of automation and artificial intelligence has enabled attackers to scale their operations, increasing the speed and volume of attacks. This constant evolution of threat tactics requires organizations to remain vigilant and proactive in their cybersecurity efforts, continuously updating defense mechanisms and threat detection systems to stay one step ahead.

The speed with which cyber threats evolve is further compounded by the challenges of maintaining effective cybersecurity across multiple sectors and jurisdictions. Many critical infrastructure systems span across national borders, with assets, services, and information shared between organizations in different countries. This interconnectedness can complicate efforts to prevent or respond to cyberattacks, particularly when adversaries operate from outside a given jurisdiction (Bello, et al., 2021, Yang, et al., 2017). In the U.S. and Canada, while there are efforts to enhance collaboration between government agencies, private sector entities, and international partners, there are still significant gaps in coordination and information-sharing. Cyberattackers often take advantage of these gaps, exploiting the lack of synchronized efforts to respond to threats in real time.

Cross-border collaboration is critical in addressing cyber risks, as cybercriminals frequently operate in a decentralized and borderless environment. However, differences in regulatory frameworks, data protection laws, and national priorities can hinder effective cooperation. For example, while both the U.S. and Canada emphasize the need for enhanced cybersecurity resilience, their regulatory approaches differ in key areas, such as data breach notification requirements and incident response procedures (Cherdantseva, et al., 2016, Kaplan & Mikes, 2016, Yang, et al., 2017). This lack of harmonization can create confusion for organizations that operate across both countries and may result in delays in responding to cyber threats. Additionally, international cooperation remains a challenge when it comes to prosecuting cybercriminals or holding state-sponsored actors accountable for their actions.

Sectoral collaboration also remains a challenge in improving cybersecurity readiness. While there are some efforts to facilitate cooperation within specific sectors—such as energy, healthcare, or transportation—these efforts are often fragmented. Organizations in critical sectors may be hesitant to share threat intelligence or cooperate in cybersecurity initiatives due to concerns about the sharing of sensitive information or the potential reputational risks of acknowledging vulnerabilities (Atkins & Lawson, 2021, Robinson, 2020). In some cases, businesses may prioritize protecting their own operations over collective efforts to safeguard the broader infrastructure ecosystem. This siloed approach can leave critical gaps in overall cybersecurity resilience, as a failure to coordinate across sectors increases the likelihood of systemic vulnerabilities being exploited by cyber adversaries.

Furthermore, there is a significant gap in the ability of many organizations to effectively implement robust cybersecurity measures. While large organizations and government entities may have the resources to invest in cutting-edge cybersecurity technologies and specialized personnel, smaller organizations, particularly in sectors such as healthcare and energy, often lack the capacity to adequately defend themselves. Small and medium-sized enterprises (SMEs) face particular challenges in adopting best practices and securing their systems, leaving them vulnerable to cyberattacks (Lanz, 2022, Shackelford, Russell & Haut, 2015, Shackelford, et al., 2015). Addressing these disparities in cybersecurity preparedness is essential to strengthening overall infrastructure resilience and ensuring that all components of the critical infrastructure ecosystem are protected.

To effectively mitigate the risks posed by the evolving cyber threat landscape, organizations in both the U.S. and Canada must adopt a proactive, risk-based approach to cybersecurity. This includes not only improving internal security measures but also enhancing collaboration across sectors and jurisdictions. Additionally, governments must prioritize the development of policies and regulatory frameworks that facilitate greater information sharing, promote best practices, and provide support to organizations facing resource constraints. By fostering a collaborative, adaptive, and forward-thinking cybersecurity culture, the U.S. and Canada can better

safeguard their critical infrastructure against the rapidly evolving cyber threat landscape.

2.3. Proposed Cyber Risk Management Framework

The need for a comprehensive and adaptive cyber risk management framework for critical infrastructure in the U.S. and Canada has become more pressing as cyber threats continue to evolve in sophistication and scale. These threats, targeting sectors such as energy, transportation, healthcare, and financial systems, can result in widespread disruptions, economic losses, and national security risks. To address these growing concerns, a robust cyber risk management framework must be developed, incorporating a variety of core components designed to proactively identify, assess, and mitigate risks while ensuring a rapid and effective response to any cyber incidents.

One of the key components of an effective cyber risk management framework is a proactive risk assessment approach. This entails regularly evaluating the potential risks to critical infrastructure systems and identifying vulnerabilities before they can be exploited by malicious actors. Proactive risk assessment involves the use of both qualitative and quantitative techniques to understand the likelihood and potential impact of cyber threats on infrastructure (Atkins & Lawson, 2021, Cohen, et al., 2022, Sabillon, Cavaller & Cano, 2016). This assessment should encompass all aspects of infrastructure, including hardware, software, and human factors, to ensure a comprehensive understanding of potential weaknesses. The use of risk assessment tools, such as vulnerability scanning, penetration testing, and threat modeling, can help identify critical vulnerabilities in systems and networks that may be exploited by attackers. This proactive approach allows organizations to address vulnerabilities before they are targeted and strengthens the overall security posture of critical infrastructure.

An essential part of this framework is the integration of advanced threat intelligence and real-time monitoring. Given the dynamic and ever-changing nature of cyber threats, relying solely on traditional security measures is insufficient to protect critical infrastructure. Threat intelligence provides organizations with up-to-date information about the tactics, techniques, and procedures (TTPs) used by adversaries, enabling them to better prepare for potential attacks (Abraham, Chatterjee & Sims, 2019, Raveling, 2023, Ustundag, et al., 2018). Real-time monitoring allows organizations to detect and respond to cyber threats as they occur, minimizing the potential impact of an attack. Advanced monitoring systems, such as Security Information and Event Management (SIEM) tools, enable organizations to analyze vast amounts of data from across their networks to identify signs of suspicious activity or emerging threats. These systems leverage machine learning and artificial intelligence (AI) to analyze patterns in network traffic and detect anomalies that could signal a potential breach. By incorporating real-time monitoring into the cyber risk management framework, organizations can identify and mitigate threats in their early stages, reducing the overall risk to critical infrastructure.

In the event that a cyberattack bypasses preventive measures, an effective incident response and recovery plan is crucial. This component of the cyber risk management framework outlines the steps organizations must take in response to a cyberattack, with the goal of containing the threat, mitigating its impact, and recovering normal operations as quickly as possible. A well-structured incident response plan includes clearly defined roles and responsibilities, communication protocols, and procedures for identifying, containing, and neutralizing the threat (Ani, He & Tiwari, 2017, Djenna, Harous & Saidouni, 2021, Judijanto). The plan should also involve collaboration with external stakeholders, such as government agencies and industry partners, to share information about the attack and coordinate response efforts. Furthermore, the recovery process must focus on restoring affected systems, data, and services, as well as conducting a thorough post-incident analysis to understand the root cause of the attack and improve future defenses. Incident response and recovery planning are critical to minimizing the long-term effects of a cyberattack on critical infrastructure.

As cyber threats continue to evolve, the integration of advanced technologies plays a crucial role in enhancing the effectiveness of the cyber risk management framework. Artificial intelligence (AI) and machine learning (ML) technologies are

particularly valuable in predictive analysis and automated responses. AI and ML can analyze vast amounts of data from multiple sources to identify patterns and trends that indicate emerging threats (Smart, 2017, Yeung, et al., 2017). By leveraging these technologies, organizations can develop predictive models that forecast potential cyberattacks, allowing them to implement preventive measures before a breach occurs. Additionally, AI-powered tools can automate responses to certain types of threats, reducing the time it takes to contain and neutralize an attack. For example, machine learning algorithms can detect malicious network traffic and automatically isolate affected systems, preventing the spread of the attack across the network. The use of AI and ML in cyber risk management enhances the ability of organizations to stay ahead of evolving threats and respond more effectively to incidents.

Blockchain technology also offers significant potential for enhancing cybersecurity within critical infrastructure. Blockchain provides a decentralized, immutable ledger for recording transactions, which can be used to ensure the integrity and security of data exchanges across multiple parties. By utilizing blockchain for secure data exchange, organizations can enhance the transparency, traceability, and accountability of their cybersecurity operations. For instance, blockchain can be employed to secure communications between critical infrastructure systems and external partners, such as third-party vendors, service providers, and government agencies (Flores, 2019, Park, 2015). It can also be used to authenticate the integrity of software updates and patch management processes, ensuring that no malicious code is introduced into the system during updates. The decentralized nature of blockchain makes it highly resistant to tampering, ensuring that data is secure even in the event of a cyberattack. By incorporating blockchain into their cyber risk management framework, organizations can further strengthen the security of their critical infrastructure and reduce the risk of data breaches or unauthorized access.

The proposed cyber risk management framework should also prioritize collaboration across sectors and jurisdictions. Given the interconnected nature of critical infrastructure systems, cyber threats to one sector or region can have cascading effects on others. A coordinated approach to cybersecurity across the U.S. and Canada, as well as with international partners, is essential to effectively mitigate cyber risks. This collaboration can take many forms, including the sharing of threat intelligence, joint incident response exercises, and the development of standardized cybersecurity policies and best practices (Callaghan, 2018, Trew, 2021). Governments, industry groups, and private sector organizations should work together to create a unified cybersecurity strategy that strengthens the resilience of critical infrastructure systems and ensures a rapid, coordinated response to cyberattacks.

In addition to cross-sector collaboration, it is important to focus on training and education to build a cybersecurity-aware workforce. Employees at all levels of an organization must be trained to recognize potential cyber threats and follow best practices for preventing cyberattacks. This includes regular cybersecurity training programs, simulations of common attack scenarios, and the implementation of security awareness campaigns (Al-Hassan, et al., 2020, Haugh, 2018, Zaccari, 2016). By fostering a culture of cybersecurity awareness and accountability, organizations can reduce the risk of human error, which remains one of the most common causes of security breaches. Furthermore, the use of advanced technologies, such as AI and blockchain, should be accompanied by a continuous investment in research and development to explore new ways to improve the cybersecurity resilience of critical infrastructure systems.

Ultimately, the proposed cyber risk management framework provides a comprehensive, proactive approach to addressing the evolving threats facing critical infrastructure in the U.S. and Canada. By incorporating core components such as proactive risk assessment, advanced threat intelligence, incident response planning, and the use of advanced technologies like AI, ML, and blockchain, organizations can better protect their systems from cyberattacks. Collaboration, training, and continuous improvement are essential to ensuring the long-term resilience of critical infrastructure and minimizing the risks posed by the growing cyber threat landscape. As cyber threats continue to evolve, this framework must

remain flexible and adaptable, allowing organizations to respond effectively to new and emerging risks.

2.4. Methodology

The methodology for developing a comprehensive cyber risk management framework to address evolving threats in U.S. and Canadian critical infrastructure involves a multi-step approach, incorporating an in-depth literature review, comparative analysis, case studies, stakeholder interviews, and the establishment of evaluation metrics to assess the framework's effectiveness. This process is designed to provide a robust, adaptable, and scalable solution that can address the complex and ever-changing cyber threat landscape.

The first step in developing the framework is conducting a thorough literature review to identify existing cyber risk management frameworks, best practices, and lessons learned from past incidents. This review encompasses academic research, industry reports, governmental publications, and cybersecurity guidelines from both the U.S. and Canada. The goal is to build on proven methodologies, identify gaps in current approaches, and understand the different strategies implemented across various sectors, particularly within the energy, transportation, healthcare, and other critical industries (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). The literature review also includes an analysis of international cybersecurity frameworks to ensure that the proposed framework aligns with global standards and regulations, while also considering unique regional requirements in the U.S. and Canada. By examining these existing models, the framework development process can draw from the strengths of previous efforts, ensuring that it is grounded in the most effective cybersecurity practices while being flexible enough to accommodate the rapidly changing threat environment.

Once the foundational understanding of existing frameworks is established, the next stage involves conducting a comparative analysis of U.S. and Canadian cybersecurity approaches. The U.S. has various cybersecurity initiatives, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and guidelines from the Cybersecurity and Infrastructure Security Agency (CISA). In contrast, Canada has its own cybersecurity initiatives, including the Cyber Security Strategy, which provides guidelines for improving the security and resilience of critical infrastructure (Recor & Xu, 2016, Sanaei, et al., 2016, Sikdar, 2021). The comparative analysis explores the similarities and differences between these frameworks, focusing on the strengths and weaknesses of each. By evaluating the regulatory and policy frameworks in both countries, it becomes clear where they align and where additional collaboration or modifications might be necessary. This analysis helps to ensure that the proposed framework addresses the unique needs of both nations, promoting cross-border cooperation and sharing of best practices while accounting for differences in regulatory environments, governance structures, and stakeholder responsibilities.

Data collection plays a crucial role in shaping the framework, particularly in terms of identifying real-world challenges and providing context for the proposed solutions. One of the primary methods of data collection is through the analysis of case studies of past cyber incidents targeting critical infrastructure. These case studies offer invaluable insights into the tactics, techniques, and procedures used by malicious actors in breaching critical systems. By studying notable incidents, such as the 2015 Ukraine power grid attack or the 2017 NotPetya attack, it is possible to gain a better understanding of the vulnerabilities in critical infrastructure and the effectiveness of previous response strategies (Govindji, Peko & Sundaram, 2018023). Analyzing the outcomes of these incidents—such as response times, containment strategies, and recovery efforts—provides critical data to inform the framework development. Case studies also help identify recurring patterns of vulnerabilities and attack vectors that organizations can address through proactive cybersecurity measures.

In addition to case studies, stakeholder interviews are an essential part of the data collection process. These interviews provide a direct line to individuals with practical experience and expertise in managing cyber risks in critical infrastructure sectors. The stakeholders interviewed include government representatives, private sector leaders, cybersecurity experts, and representatives from critical infrastructure industries.

These discussions yield valuable insights into the challenges faced by organizations in protecting their systems from cyber threats, as well as the current gaps in cybersecurity strategies (Fefer, 2019, Sullivan, 2019, Voss, 2019). Interviews with government representatives help identify the regulatory landscape and the challenges that organizations face when trying to comply with evolving policies. Private sector leaders, on the other hand, provide a practical perspective on how businesses are addressing cybersecurity challenges within their sectors, including the resource constraints and operational limitations they face. Cybersecurity experts contribute technical insights into the latest tools and technologies for mitigating cyber risks and offer recommendations on how these can be integrated into the proposed framework. Through this multi-stakeholder approach, the methodology ensures that the proposed cyber risk management framework is grounded in real-world experience and aligns with the needs of all relevant parties.

The next step in the methodology is the development of evaluation metrics, which are essential for assessing the effectiveness of the cyber risk management framework once it is implemented. These metrics focus on several critical aspects, including threat detection capabilities, response times, and overall system resilience. Threat detection is a key area of evaluation, as the ability to quickly identify and assess cyber threats is essential for preventing or minimizing damage. The framework should be evaluated based on its ability to integrate advanced threat intelligence tools and real-time monitoring systems that allow organizations to detect emerging threats early on (Minssen, et al., 2020, Tian, 2016). This includes assessing the effectiveness of machine learning algorithms, artificial intelligence tools, and automated systems in recognizing patterns and anomalies in network traffic, system behavior, and user activity that may indicate an attack.

Another critical evaluation metric is response time. The ability to quickly and effectively respond to cyber incidents is crucial for minimizing the impact on critical infrastructure. The framework will be assessed based on its ability to support rapid incident detection, containment, and remediation efforts. This includes evaluating the efficiency of the incident response processes, the clarity of communication channels, and the coordination between different stakeholders (e.g., private sector organizations, government agencies, and industry partners) in responding to an attack (Celeste & Fabbrini, 2020, Mattoo & Meltzer, 2018, Tehrani, Sabaruddin & Ramanathan, 2018). Key performance indicators (KPIs) for response time might include the time taken to detect a breach, the time taken to mitigate the attack, and the time required to fully recover affected systems.

Lastly, the framework will be evaluated based on the overall resilience of the critical infrastructure systems it protects. System resilience refers to an organization's ability to maintain operational continuity during and after a cyberattack. The evaluation process will assess how well the framework helps organizations strengthen their resilience, ensuring that even in the event of an attack, critical systems can continue to operate or quickly recover with minimal disruption (Malhotra, 2018, McCubbrey, 2020). This includes evaluating the effectiveness of business continuity planning, disaster recovery measures, and the integration of redundancy and backup systems into critical infrastructure. The overall goal is to ensure that the framework not only reduces the likelihood of a successful cyberattack but also enables organizations to recover quickly and resume normal operations when an attack occurs.

The methodology for developing the cyber risk management framework relies on a combination of qualitative and quantitative approaches, ensuring that the final product is both evidence-based and aligned with the practical needs of stakeholders. By synthesizing insights from literature, case studies, stakeholder interviews, and evaluation metrics, the framework aims to address the evolving cyber threats facing critical infrastructure in the U.S. and Canada. This structured, multi-faceted approach ensures that the proposed framework is comprehensive, adaptable, and capable of evolving alongside the growing sophistication of cyber threats.

2.5. Implementation Strategies

Implementing a cyber risk management framework to address the evolving threats in U.S. and Canadian critical infrastructure requires a multi-layered

approach that emphasizes collaboration, proactive risk management, and a skilled workforce. These strategies are essential to ensuring that critical sectors such as energy, healthcare, transportation, and communications remain resilient in the face of increasingly sophisticated cyber threats (Aboelfotoh & Hikal, 2019, Garrett, 2018, Shackelford, et al., 2015). The successful implementation of the framework hinges on the involvement of public and private sector stakeholders, continuous development of cybersecurity capabilities, and close cooperation between the U.S. and Canadian governments.

One of the foundational strategies for the implementation of a robust cyber risk management framework is fostering strong public-private partnerships. In both the U.S. and Canada, the private sector plays a vital role in the operation and maintenance of critical infrastructure. Government agencies, such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Canada's Centre for Cyber Security, must work closely with private organizations to ensure that cybersecurity strategies are not only comprehensive but also adaptable to evolving threats (Georgiadou, Mouzakitis & Askounis, 2021, Knowles, et al., 2015). Public-private partnerships can facilitate the sharing of threat intelligence, which is crucial for detecting and mitigating cyber risks in real-time. Information sharing initiatives, such as the Information Sharing and Analysis Centers (ISACs) in both countries, can serve as platforms for exchanging cyber threat data, vulnerability reports, and mitigation strategies. By sharing information in a secure and timely manner, both sectors can be better prepared for cyber attacks and can work collaboratively to develop effective responses.

In addition to information sharing, joint incident response mechanisms are critical for minimizing the impact of cyber attacks on critical infrastructure. When a cyber attack occurs, a swift and coordinated response is necessary to prevent further damage and restore services. A clear and agreed-upon incident response plan, developed through collaboration between the public and private sectors, can ensure that resources are allocated efficiently, and communication channels remain open between key stakeholders (Sabillon, et al., 2017, Shackelford, Russell & Haut, 2015). This joint response can include a combination of cybersecurity experts, legal teams, law enforcement agencies, and government representatives, all working together to mitigate the effects of an attack and prevent future breaches.

Another essential aspect of the framework's implementation is workforce development. As the threat landscape evolves, so too must the cybersecurity skills of the workforce tasked with defending critical infrastructure. Continuous training and awareness programs are essential to ensure that individuals at all levels of an organization are prepared to recognize and respond to cyber risks. These programs must be tailored to the specific needs of each sector within critical infrastructure, providing industry-specific knowledge and practical skills for employees to manage cyber threats (Burke, et al., 2019, Demchak, et al., 2016, Kour, Karim & Thaduri, 2020). In the energy sector, for example, workers may require training in securing Industrial Control Systems (ICS) against cyber intrusions, while in healthcare, the focus may be on safeguarding patient data and protecting against ransomware attacks. Cybersecurity training should be an ongoing process, rather than a one-time event, as the tactics and techniques used by cybercriminals evolve over time. This ensures that the workforce remains prepared and responsive to emerging threats.

Moreover, raising awareness about cybersecurity risks within the workforce is equally important. Employees should be aware of potential vulnerabilities, such as phishing emails or social engineering attacks, and should know how to respond to these threats. Public awareness campaigns can also play a role in educating the broader population about the importance of cybersecurity and safe online behaviors. By creating a culture of cybersecurity within organizations, workers become more vigilant and proactive in protecting critical infrastructure (Aliyu, et al., 2020, Brown, 2018, Miron, 2015).

Cross-border collaboration between the U.S. and Canada is another critical strategy for effectively addressing cyber threats to critical infrastructure. As cyber threats often originate from outside national borders, it is essential that both countries work

together to harmonize their cybersecurity practices, policies, and regulations. This collaboration can take the form of aligning regulatory standards and frameworks, ensuring that both nations adopt similar approaches to cybersecurity. This helps eliminate gaps that malicious actors might exploit to target critical infrastructure in one country while bypassing protections in the other (Kumar, Himes & P. Kritzer, 2014, Monaghan & Walby, 2017).

Harmonizing regulatory standards also simplifies compliance for multinational organizations that operate across both the U.S. and Canada. For example, both countries could align their approaches to cybersecurity incident reporting, ensuring that companies in both jurisdictions follow the same procedures when a breach occurs. This standardization improves transparency and efficiency, making it easier to coordinate responses to cross-border cyber incidents. It also ensures that the regulatory environment is clear and consistent, making it easier for organizations to comply with legal requirements related to cybersecurity (Gow, 2019, Pomerleau & Lowery, 2020).

In addition to harmonizing regulations, joint exercises and simulations for coordinated responses are vital for enhancing cross-border collaboration. These exercises can simulate real-world cyber incidents and test the effectiveness of joint response strategies. Both U.S. and Canadian officials can participate in these exercises to evaluate how well they can work together during a cyber attack, identify areas for improvement, and refine response protocols (Miron & Muita, 2014). These simulations help build trust and cooperation between governments, critical infrastructure operators, and cybersecurity professionals, ensuring that all parties know their roles and responsibilities during a crisis. Regular cross-border exercises also help organizations stay current with new threats and vulnerabilities and allow them to practice integrating new technologies and strategies into their response plans.

Furthermore, regular communication and collaboration between U.S. and Canadian law enforcement agencies, cybersecurity experts, and industry leaders are critical for addressing cybercrime that spans both countries. Joint task forces, such as the U.S.-Canada Cybersecurity Partnership, facilitate information sharing and ensure that both governments are aligned in their efforts to combat cybercrime. By working together, these entities can investigate cross-border cybercriminal activities and take coordinated actions against cyber threats targeting critical infrastructure.

Finally, the implementation of the cyber risk management framework requires strong leadership and governance. Both U.S. and Canadian governments must provide clear direction and support for the cybersecurity efforts of critical infrastructure sectors. This includes providing adequate funding for cybersecurity initiatives, establishing clear lines of accountability, and ensuring that organizations within critical sectors have access to the resources they need to bolster their cybersecurity posture (Burns, 2019, Shackelford & Bohm, 2016, Stoddart, 2016). Leadership at the highest levels of government and industry is essential for driving the implementation of the framework and ensuring that cybersecurity remains a top priority.

The implementation strategies for a cyber risk management framework aimed at addressing the evolving threats to U.S. and Canadian critical infrastructure are multifaceted and require collaboration across sectors and borders. By fostering public-private partnerships, investing in workforce development, and promoting cross-border cooperation, both countries can strengthen their resilience against cyber threats (Rass, et al., 2020, Stellios, et al., 2018). These strategies not only improve the ability to detect and respond to cyber incidents but also ensure that critical infrastructure remains operational and secure, even in the face of increasingly sophisticated cyber threats. Through these efforts, the U.S. and Canada can protect their critical infrastructure from evolving cyber risks and ensure the continued safety, stability, and prosperity of their societies.

2.6. Case Studies

Case studies play a crucial role in understanding the real-world application of a cyber risk management framework to address evolving threats to critical

infrastructure. The experiences of U.S. and Canadian organizations in responding to various cyber incidents provide valuable insights into the effectiveness of current cybersecurity strategies and highlight areas for improvement. In particular, two case studies—one focusing on the successful mitigation of ransomware attacks in the Canadian energy sector and the other on securing Industrial Control Systems (ICS) in the U.S. transportation sector—offer key lessons for addressing the evolving cyber threat landscape in critical infrastructure.

Ransomware attacks have emerged as one of the most prevalent and disruptive forms of cyber threat in recent years, particularly targeting critical infrastructure sectors. In Canada, the energy sector has been a primary target for such attacks, with several high-profile incidents underscoring the vulnerability of the sector to ransomware. One such case occurred when a major Canadian energy provider experienced a ransomware attack that disrupted its operations, leading to significant financial losses and operational downtime. The attack involved the encryption of critical data, leaving the energy company with limited access to its internal systems and data (Burns, 2019, Shackelford & Bohm, 2016, Stoddart, 2016). In response, the organization quickly activated its incident response plan, which included isolation of affected systems, engagement with cybersecurity experts, and communication with government agencies and law enforcement.

The success of the response can be attributed to several key factors within the cyber risk management framework. First, the organization had a proactive risk assessment process in place, identifying the energy sector as a high-value target for ransomware attacks. This foresight allowed the company to implement robust preventative measures, such as regular data backups, network segmentation, and the use of advanced threat detection tools. Additionally, the energy provider had established strong partnerships with governmental bodies and private cybersecurity firms, ensuring that it had the necessary expertise and resources to address the incident (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). The use of advanced threat intelligence tools enabled the company to identify the attack's origin and nature, helping to prevent further damage. Furthermore, the organization's focus on real-time monitoring allowed for the rapid detection of the ransomware attack, minimizing the scope of the incident and reducing recovery time.

Following the incident, the company conducted a thorough post-attack analysis, identifying areas for improvement in its cyber risk management framework. Lessons learned from the attack included the importance of having a comprehensive cybersecurity strategy that incorporates both technical and human elements. The company recognized the need to provide ongoing cybersecurity training for its workforce, particularly for employees who may be vulnerable to phishing attacks, a common vector for ransomware (Burke, et al., 2019, Demchak, et al., 2016, Kour, Karim & Thaduri, 2020). The organization also enhanced its threat intelligence capabilities, allowing for more proactive identification of emerging threats and better collaboration with public and private sector stakeholders.

In addition to mitigating ransomware attacks, securing Industrial Control Systems (ICS) has become a top priority for critical infrastructure sectors in both the U.S. and Canada. ICS are vital to the functioning of essential services, such as energy production, transportation, and water treatment (Rass, et al., 2020, Stellios, et al., 2018). However, these systems are often vulnerable to cyber threats due to their reliance on legacy technologies, lack of robust security measures, and the convergence of operational technology (OT) with information technology (IT). A significant case study of securing ICS comes from the U.S. transportation sector, where the need to protect transportation systems from cyber threats became increasingly urgent as cyberattacks targeting ICS grew more sophisticated.

One notable example of ICS vulnerability in the U.S. transportation sector occurred when a cyberattack targeted the control systems of a major metropolitan transit system. The attack exploited vulnerabilities in the transit system's outdated ICS, compromising the ability to control trains and signaling systems (Kumar, Himes & P. Kritzer, 2014, Monaghan & Walby, 2017). This incident caused significant disruption to transportation services, affecting thousands of

commuters and raising concerns about the safety and reliability of critical transportation infrastructure. In response, the transit system's cybersecurity team worked closely with federal agencies, such as the U.S. Department of Homeland Security (DHS) and the Federal Transportation Administration (FTA), as well as private cybersecurity firms, to contain the attack and mitigate its impact.

The response to the ICS attack in the U.S. transportation sector highlighted several critical elements of an effective cyber risk management framework. The first lesson learned was the importance of regular vulnerability assessments and system updates. The attack was successful, in part, because the ICS had not been adequately updated to address known vulnerabilities. As a result, the transportation agency implemented a more aggressive patch management strategy, ensuring that all systems were regularly updated and tested for vulnerabilitie (Burns, 2019, Shackelford & Bohm, 2016, Stoddart, 2016)s. The agency also began conducting more frequent risk assessments to identify potential gaps in its cybersecurity posture and to prioritize remediation efforts.

Another key lesson from the transportation sector case study was the importance of segmentation and isolation of ICS from IT networks. The convergence of OT and IT has created new attack vectors, allowing cybercriminals to move laterally within an organization's networks. In response to this, the transportation agency implemented stricter network segmentation measures, ensuring that ICS were isolated from IT systems. This made it more difficult for attackers to move between the two networks, thereby limiting the potential impact of future attacks (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). Additionally, the agency invested in advanced threat monitoring and detection tools that could quickly identify unusual behavior or potential intrusions within ICS.

The U.S. transportation sector also recognized the need for cross-sector collaboration in securing ICS. The incident underscored the importance of information sharing between government agencies, critical infrastructure operators, and private sector stakeholders (Rass, et al., 2020, Stellios, et al., 2018). The transportation agency participated in information-sharing platforms, such as the Transportation Systems Sector Coordinating Council (TSSCC), to gain access to real-time threat intelligence and best practices for securing ICS. These collaborative efforts helped the agency stay informed about emerging threats and improve its response capabilities.

Finally, the transportation sector case study demonstrated the importance of having a robust incident response and recovery plan. The agency's ability to quickly contain the attack and restore services was due in large part to its well-defined incident response procedures. These procedures included clear communication channels, coordination with law enforcement agencies, and a focus on rapid recovery to minimize operational downtime. Following the attack, the agency conducted a comprehensive post-incident review to identify areas for improvement and to enhance its ICS security posture (Burke, et al., 2019, Demchak, et al., 2016, Kour, Karim & Thaduri, 2020).

Both the Canadian energy sector's response to ransomware attacks and the U.S. transportation sector's efforts to secure ICS highlight the importance of a proactive and multi-faceted approach to cyber risk management. Successful mitigation of cyber threats requires a combination of advanced threat intelligence, real-time monitoring, vulnerability management, and collaboration between public and private sector stakeholders. Furthermore, these case studies demonstrate the value of post-incident analysis in identifying weaknesses and refining cybersecurity strategies to address evolving threats.

In conclusion, the experiences of both the Canadian energy sector and the U.S. transportation sector offer valuable insights into the challenges and successes of implementing a cyber risk management framework for critical infrastructure. By continuously adapting to the changing cyber threat landscape, organizations in these sectors can improve their resilience and protect critical infrastructure from increasingly sophisticated cyber threats (Burns, 2019, Shackelford & Bohm, 2016, Stoddart, 2016). These case studies underscore the need for ongoing investment in cybersecurity

technologies, workforce development, and cross-sector collaboration to effectively address the evolving nature of cyber risks to critical infrastructure in both the U.S. and Canada.

2.7. Challenges and Limitations

The implementation of a cyber risk management framework to address the evolving threats to critical infrastructure in the U.S. and Canada presents a complex set of challenges and limitations that need to be overcome. These barriers, stemming from legal, resource, and operational issues, hinder the effectiveness of cybersecurity measures and often complicate the establishment of a unified and comprehensive framework. While the critical infrastructure sectors in both countries have made significant progress in strengthening their cybersecurity, these challenges continue to be significant impediments that demand focused attention.

One of the primary challenges facing the successful implementation of a cyber risk management framework in the U.S. and Canada is the legal barriers to cross-border information sharing. Critical infrastructure is inherently interconnected across borders, and cyber threats to one sector or region can have significant impacts on neighboring sectors or even international partners. However, the legal frameworks governing information sharing between the U.S. and Canada are complex and often hinder the timely exchange of critical cybersecurity intelligence. In both countries, regulatory and privacy laws can create significant barriers to collaboration. For instance, concerns over national security, data sovereignty, and privacy laws limit the ability of private sector organizations to share sensitive data, including threat intelligence, with foreign governments and companies (Rass, et al., 2020, Stellios, et al., 2018). As a result, when cyber threats evolve rapidly or attacks occur across jurisdictions, organizations are often left to act in isolation rather than cooperating with international partners who could provide critical insights or resources to mitigate the impact of the attacks.

The legal complexities surrounding cross-border data sharing are further exacerbated by the differing regulatory approaches between the U.S. and Canada. While both countries have established frameworks to address cybersecurity in critical infrastructure, the regulatory requirements and expectations can vary significantly. For example, the U.S. relies heavily on guidelines and frameworks from agencies such as the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), while Canada has its own set of regulations and strategies, such as the Canadian Cyber Security Strategy and the Canadian Radio-television and Telecommunications Commission (CRTC) regulations (Cantelmi, Di Gravio & Patriarca, 2021, Carter & Sofio, 2017). This divergence in regulatory approaches complicates efforts to establish a cohesive cyber risk management framework, especially when both countries are dealing with similar threats to critical infrastructure.

Another significant challenge that limits the effectiveness of a cyber risk management framework is the resource constraints faced by small and medium-sized infrastructure providers. While large organizations in critical sectors such as energy, transportation, and healthcare have the financial resources and technical expertise to implement sophisticated cybersecurity measures, small and medium-sized enterprises (SMEs) often lack the necessary funding and personnel to address cyber risks adequately (Bridge & Bradshaw, 2017, Papert & Pflaum, 2017). These smaller organizations often operate on tight budgets and struggle to invest in the tools and technologies needed to protect their infrastructure from advanced threats. Furthermore, they may not have dedicated cybersecurity teams, making them more vulnerable to cyberattacks, especially as the complexity of threats continues to evolve.

The resource gap between large and small infrastructure providers is particularly evident in the implementation of advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) for threat detection and mitigation. These technologies require substantial investments in both infrastructure and expertise, and many SMEs in the critical infrastructure sectors cannot afford them. As a result, they rely on basic cybersecurity measures, which may not be sufficient to defend against

increasingly sophisticated cyberattacks (Chen, Zhang & Delaurentis, 2014, Urciuoli, et al., 2014). Additionally, many smaller organizations lack the capacity to conduct regular cybersecurity audits or to develop comprehensive incident response plans, which leaves them ill-prepared when attacks occur.

Moreover, the lack of skilled cybersecurity professionals exacerbates the resource constraints faced by smaller organizations. The cybersecurity workforce in both the U.S. and Canada is in high demand, with many companies struggling to find qualified professionals to fill positions. As a result, SMEs often face significant difficulties in attracting and retaining skilled cybersecurity experts who can help them develop and implement effective risk management strategies (Kumar, Himes & P. Kritzer, 2014, Monaghan & Walby, 2017). This shortage of talent further undermines the ability of these organizations to build and maintain robust cybersecurity frameworks, leaving critical infrastructure vulnerable to attack.

A third challenge in implementing an effective cyber risk management framework for critical infrastructure is the need for standardized metrics to evaluate the success of the framework. While many organizations have adopted cyber risk management frameworks based on industry best practices and regulatory guidelines, there remains a lack of standardized metrics to measure their effectiveness (Gao, et al., 2020, Schlegel & Trent, 2014). This lack of clear metrics makes it difficult for organizations to assess whether their cybersecurity measures are achieving the desired outcomes, such as reducing the number of successful attacks, minimizing the impact of incidents, or enhancing system resilience. Without standardized metrics, it is also challenging for organizations to compare their performance against industry benchmarks or to determine areas where they need to improve.

The absence of standardized evaluation metrics also complicates the task of measuring the return on investment (ROI) for cybersecurity initiatives. Organizations often struggle to justify the costs associated with cybersecurity investments without clear, quantifiable outcomes. As cyber threats become more complex and expensive to mitigate, the need for standardized metrics becomes even more critical. These metrics would allow organizations to better understand the effectiveness of their cybersecurity investments and make informed decisions about where to allocate resources (Hobbs, 2020, Lawrence, et al., 2020). Additionally, standardized metrics would facilitate greater collaboration between sectors, enabling organizations to share best practices and benchmark their performance against others in the industry.

Another limitation is that the absence of standardized metrics hinders the development of universal cybersecurity standards across different sectors. While certain sectors, such as the financial industry, have well-defined cybersecurity standards and metrics, other sectors, like energy and transportation, have less clearly defined metrics (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). This lack of uniformity makes it difficult to create a comprehensive, cross-sector cyber risk management framework that addresses the unique needs and challenges of each sector. It also limits the ability of regulators to enforce cybersecurity standards consistently across critical infrastructure sectors, leading to potential gaps in security and oversight.

In addition to these challenges, the constantly evolving nature of cyber threats presents an ongoing hurdle in managing risk to critical infrastructure. Cybercriminals, state-sponsored actors, and hacktivists continuously adapt their tactics, techniques, and procedures to bypass security measures and exploit vulnerabilities. The rapid pace of technological change, particularly in areas such as automation, cloud computing, and the Internet of Things (IoT), also creates new vulnerabilities that must be addressed (Kumar, Himes & P. Kritzer, 2014, Monaghan & Walby, 2017). As cyber threats continue to evolve, organizations must remain agile and adapt their cybersecurity strategies to stay ahead of potential attacks. However, resource limitations, regulatory barriers, and the lack of standardized metrics make it challenging for many organizations to keep up with the pace of change and to implement adaptive risk management strategies effectively.

In conclusion, the challenges and limitations of implementing a cyber risk management framework to address evolving threats to U.S. and Canadian critical infrastructure are substantial and multifaceted. Legal barriers to cross-border information sharing, resource constraints for small and medium-sized infrastructure providers, and the need for standardized evaluation metrics are just a few of the key issues that hinder the effectiveness of cybersecurity efforts (Boyson, 2014, Linkov, et al., 2014). Overcoming these challenges will require coordinated efforts across both countries, as well as investment in advanced technologies, workforce development, and standardized regulatory approaches. Only by addressing these limitations can the U.S. and Canada hope to enhance the resilience of their critical infrastructure and effectively mitigate the risks posed by evolving cyber threats.

2.8. Conclusion and Recommendations

In conclusion, the proposed cyber risk management framework aims to enhance the resilience and security of critical infrastructure across the U.S. and Canada, addressing the increasing frequency and sophistication of cyber threats. The framework's primary objectives are to proactively identify risks, implement advanced threat intelligence, strengthen incident response mechanisms, and foster a collaborative approach between the public and private sectors. By focusing on key components such as real-time monitoring, predictive analytics using artificial intelligence (AI), and the integration of blockchain for secure data exchange, the framework seeks to provide a comprehensive and adaptable solution to the evolving cyber threat landscape. This approach ensures that both countries can not only respond to immediate threats but also build long-term resilience within critical infrastructure sectors like energy, healthcare, transportation, and beyond.

The benefits of such a framework are far-reaching. First, it provides a structured methodology for identifying and mitigating risks before they become catastrophic, minimizing the potential for disruption to essential services. Second, it encourages the adoption of cutting-edge technologies, such as AI and machine learning, which allow for faster detection and automated responses to cyber incidents. Additionally, by facilitating information sharing and joint incident response efforts, the framework promotes collaboration across sectors and borders, ensuring that organizations are better equipped to deal with cyberattacks that cross national and sectoral boundaries.

However, the implementation of this framework faces numerous challenges, including legal and resource barriers, especially when it comes to cross-border information sharing and the limitations faced by small and medium-sized infrastructure providers. To overcome these challenges, a series of policy improvements and strategic investments are necessary. Policymakers must focus on harmonizing regulatory standards across both the U.S. and Canada, especially when it comes to information sharing, to ensure smoother collaboration between public and private entities. It is also crucial to increase investment in advanced cybersecurity technologies that can enhance threat detection, automated response, and recovery planning.

Furthermore, fostering a culture of collaboration across sectors—especially between governments, private enterprises, and critical infrastructure providers—is essential. Governments should incentivize private sector investment in cybersecurity and encourage the sharing of best practices through joint exercises, simulations, and real-time threat intelligence exchanges. In addition, supporting workforce development initiatives to train a new generation of cybersecurity professionals will ensure that organizations have the skilled talent necessary to implement and maintain these advanced risk management frameworks.

By addressing these recommendations and taking a proactive approach to cybersecurity, the U.S. and Canada can significantly enhance the security of their critical infrastructure, protecting them from evolving cyber threats that could have wide-ranging consequences for national security, the economy, and public safety. A concerted effort toward collaboration, investment, and continuous adaptation will ultimately ensure that both nations remain resilient in the face of growing cyber risks.

REFERENCES

[1] Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245-272.

[2] Aboelfotoh, S. F., & Hikal, N. A. (2019). A review of cyber-security measuring and assessment methods for modern enterprises. *JOIV: International Journal on Informatics Visualization*, *3*(2), 157-176.

[3] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.

[4] Al-Hassan, A., Burfisher, M. E., Chow, M. J. T., Ding, D., Di Vittorio, F., Kovtun, D., ... & Youssef, K. (2020). *Is the whole greater than the sum of its parts? Strengthening caribbean regional integration*. International Monetary Fund.

[5] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

[6] Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32-43.

[7] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74.

[8] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

[9] Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847-861.

[10] Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024.

[11] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[12] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[13] Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.

[14] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[15] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. *Mitre Corp, Mclean*, 2021-11.

[16] Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

[17] Bridge, G., & Bradshaw, M. (2017). Making a global gas market: Territoriality and production networks in liquefied natural gas. *Economic Geography*, *93*(3), 215-240.

[18] Brown, R. D. (2018). Towards a Qatar cybersecurity capability maturity model with a legislative framework. *International Review of Law*.

[19] Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

[20] Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019, January). Cybersecurity indexes for eHealth. In *Proceedings of the australasian computer science week multiconference* (pp. 1-8).

[21] Burns, M. G. (2019). *Managing energy security: an all hazards approach to critical infrastructure*. Routledge.

[22] Callaghan, R. (2018). *The impact of protectionism on the completion and duration of cross-border acquisitions* (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

[23] Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, *41*(3), 341-376.

[24] Carter, W. A., & Sofio, D. G. (2017). Cybersecurity legislation and critical infrastructure vulnerabilities. *Foundations of Homeland Security: Law and Policy*, 233-249.

[25] Celeste, E., & Fabbrini, F. (2020). Competing jurisdictions: Data privacy across the borders. *Data Privacy and Trust in Cloud Computing*, 43-58.

[26] Chen, C., Zhang, J., & Delaurentis, T. (2014). Quality control in food supply chain management: An analytical model and case study of the adulterated milk incident in China. *International Journal of Production Economics*, *152*, 188-199.

[27] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

[28] Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

[29] Clemente, J. F. (2018). *Cyber security for critical energy infrastructure* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[30] Dalal, A., Abdul, S., & Mahjabeen, F. (2016). Leveraging Artificial Intelligence for Cyber Threat Intelligence: Perspectives from the US, Canada, and Japan. *Revista de Inteligencia Artificial en Medicina*, *7*(1), 18-28.

[31] Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2016). Cyber readiness at a glance. *Potomac Institute for Policy Studies*, 1-44.

[32] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

[33] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

[34] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, *55*, 102211.

[35] Ele, S. I., & Oko, J. O. (2016). Governance, risk and compliance (Grc): a. *Journal of Integrative Humanism*, *6*(1), 161.

[36] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Application of deep and machine learning techniques for multi-label classification performance on psychotic

disorder diseases. Informatics in Medicine Unlocked, 23, 100545.

[37] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Informatics in Medicine Unlocked.

[38] Fefer, R. F. (2019). Data flows, online privacy, and trade policy. *Congressional Research Service*.

[39] Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, *27*(1), 62-82.

[40] Flores, M. C. (2019). Challenges for Macroprudential Policy in the Euro Area: Cross-Border Spillovers and Governance Issues.

[41] Gao, Q., Guo, S., Liu, X., Manogaran, G., Chilamkurti, N., & Kadry, S. (2020). Simulation analysis of supply chain risk management system based on IoT information platform. *Enterprise Information Systems*, *14*(9-10), 1354-1378.

[42] Garrett, G. A. (2018). *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices*. Aspen Publishers.

[43] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

[44] Govindji, S., Peko, G., & Sundaram, D. (2018). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication: 6th International Conference, ICCASA 2017, and 3rd International Conference, ICTCC 2017, Tam Ky, Vietnam, November 23-24, 2017, Proceedings 6* (pp. 14-24). Springer International Publishing.

[45] Gow, G. A. (2019). *Policymaking for critical infrastructure: a case study on strategic interventions in public safety telecommunications*. Routledge.

[46] Haugh, T. (2018). Harmonizing governance, risk management, and compliance through the paradigm of behavioral ethics risk. *U. Pa. J. Bus. L.*, *21*, 873.

[47] Hobbs, J. E. (2020). Food supply chains during the COVID-19 pandemic. *Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie*, *68*(2), 171-176.

[48] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2021.2.2.0059

[49] Igo, S. E. (2020). *The known citizen: A history of privacy in modern America*. Harvard University Press.

[50] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), 074–086. https://doi.org/10.30574/msarr.2021.2.1.0032

[51] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, *7*(6), 31-38.

[52] Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

[53] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.

[54] Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the institution of*

mechanical engineers, Part F: Journal of Rail and Rapid Transit, *234*(10), 1129-1148.

[55] Kovacevic, A., & Nikolic, D. (2015). Cyber attacks on critical infrastructure: Review and challenges. *Handbook of research on digital crime, cyberspace security, and information assurance*, 1-18.

[56] Kumar, S., J. Himes, K., & P. Kritzer, C. (2014). Risk assessment and operational approaches to managing risk in global supply chains. *Journal of Manufacturing Technology Management*, *25*(6), 873-890.

[57] Laidlaw, E. (2021). Privacy and cybersecurity in digital trade: The challenge of cross border data flows. *Available at SSRN 3790936*.

[58] Lawrence, J. M., Hossain, N. U. I., Jaradat, R., & Hamilton, M. (2020). Leveraging a Bayesian network approach to model and analyze supplier vulnerability to severe weather risk: A case study of the US pharmaceutical supply chain following Hurricane Maria. *International Journal of Disaster Risk Reduction*, *49*, 101607.

[59] Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature climate change*, *4*(6), 407-409.

[60] Malhotra, Y. (2018). Bridging networks, systems and controls frameworks for cybersecurity curriculums and standards development. *Journal of Operational Risk*, *13*(1).

[61] Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

[62] McCubbrey, D. S. (2020). *Cybersecurity Penetration Assessments in the Context of a Global Cybersecurity Skills Gap* (Doctoral dissertation, Capella University).

[63] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE.

[64] Minssen, T., Seitz, C., Aboy, M., & Compagnucci, M. C. (2020). The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?. *EPLR*, *4*, 34.

[65] Miron, W. R. (2015). *Adoption of Cybersecurity Capability Maturity Models in Municipal Governments* (Doctoral dissertation, Carleton University).

[66] Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, *4*(10), 33.

[67] Monaghan, J., & Walby, K. (2017). Surveillance of environmental movements in Canada: Critical infrastructure protection and the petro-security apparatus. *Contemporary Justice Review*, *20*(1), 51-70.

[68] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

[69] Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017, September). Managing information security risk using integrated governance risk and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56-66). IEEE.

[70] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and*

Reviews. https://doi.org/10.30574/msarr.2021.3.2.0086

[71] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.1.0076

[72] Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, 1251-1263.

[73] Papert, M., & Pflaum, A. (2017). Development of an ecosystem model for the realization of internet of things (IoT) services in supply chain management. *Electronic Markets*, *27*(2), 175-189.

[74] Park, S. K. (2015). Special economic zones and the perpetual pluralism of global trade and labor migration. *Geo. J. Int'l L.*, *47*, 1379.

[75] Pomerleau, P. L. (2019). Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection. *Order*, (27540959).

[76] Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*. Springer.

[77] Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-security in critical infrastructures* (Vol. 297). Springer International Publishing.

[78] Recor, J., & Xu, H. (2016). GRC technology introduction. In *Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (pp. 305-331). New York: Palgrave Macmillan US.

[79] Robinson, R. (2020). *Exploring strategies to ensure United States critical infrastructure of the water sector maintains proper cybersecurity* (Doctoral dissertation, Colorado Technical University).

[80] Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

[81] Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

[82] Sanaei, M. R., Movahedi Sobhani, F., & Rajabzadeh, A. (2016). Toward An E-business Governance Model Based on GRC Concept. *The International Journal of Humanities*, *23*(3), 71-85.

[83] Schlegel, G. L., & Trent, R. J. (2014). *Supply chain risk management: An emerging discipline*. Crc Press.

[84] Shackelford, S. J., & Bohm, Z. (2016). Securing North American critical infrastructure: A comparative case study in cybersecurity regulation. *Can.-USLJ*, *40*, 61.

[85] Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

[86] Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, 217.

[87] Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of*

Computer Science and Information Security, *14*(1), 129-136.

[88] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30.

[89] Sikdar, P. (2021). *Strong Security Governance Through Integration and Automation: A Practical Guide to Building an Integrated GRC Framework for Your Organization*. Auerbach Publications.

[90] Smart, C. (2017). Regulating the Data that Drive 21st-Century Economic Growth.

[91] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.

[92] Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), 1079-1105.

[93] Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *computer law & security review*, *35*(4), 380-397.

[94] Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, *34*(3), 582-594.

[95] Tian, G. Y. (2016). Current issues of cross-border personal data protection in the context of cloud computing and trans-Pacific partnership agreement: join or withdraw. *Wis. Int'l LJ*, *34*, 367.

[96] Trew, S. J. (2021). *International Regulatory Cooperation and the Making of "Good" Regulators: A Case Study of the Canada–US Regulatory Cooperation Council* (Doctoral dissertation, Carleton University).

[97] Urciuoli, L., Mohanty, S., Hintsa, J., & Gerine Boekesteijn, E. (2014). The resilience of energy supply chains: a multiple case study approach on oil and gas supply chains to Europe. *Supply Chain Management: An International Journal*, *19*(1), 46-63.

[98] Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*, 267-284.

[99] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485.

[100] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

[101] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.

[102] Yeung, M. T., Kerr, W. A., Coomber, B., Lantz, M., & McConnell, A. (2017). *Declining international cooperation on pesticide regulation: frittering away food security*. Springer.

[103] Zaccari, L. (2016). Addressing a successful implementation of a governance, risk and compliance management system.