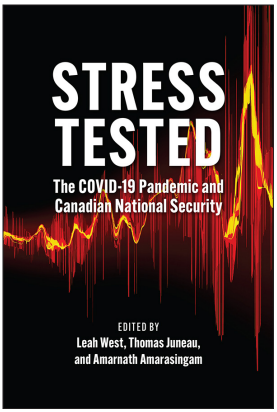
2021-11

Stress Tested: The COVID-19 Pandemic and Canadian National Security

University of Calgary Press

West, L., Juneau, T., & Amarasingam, A. (Eds.). (2021). Stress Tested: The COVID-19 Pandemic and Canadian National Security. University of Calgary Press.
http://hdl.handle.net/1880/114134
book

UNIVERSITY OF CALGARY
Press



STRESS TESTED: THE COVID-19 PANDEMIC AND CANADIAN NATIONAL SECURITY

Edited by Leah West, Thomas Juneau, and Amarnath Amarasingam

ISBN 978-1-77385-244-7

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

4

Getting the Politics of Protecting Critical Infrastructure Right

Bessma Momani and Jean-François Bélanger

Introduction

Canada has generally not been the target of cyber attacks, but these types of threats must become a concern in the post-COVID-19 digitized world. The digitalization of critical infrastructures should eliminate any sense of complacency the country once had. Critical infrastructures include energy and utilities, financial systems, food systems, transportation, government, information and communication technology, health systems, water, emergency services, and critical manufacturing (Public Safety Canada 2014); these are all vital components of our daily lives. Our move to a digitalized world has been rapidly accelerated by COVID-19, pushing Canada's national security and intelligence community to be even more vigilant about foreign and domestic cyber attacks. We note in this chapter that critical infrastructure can be particularly exposed to cyber attacks and therefore needs added policy attention. Some of these risks are further complicated by the fact that Canada's critical infrastructure has shifted from public to private ownership and control, thereby adding multiple operators, varied corporations with their own shareholder interests, and a vast number of asset owners. As the federal government often shares the public responsibility for keeping Canadians safe, getting the politics of critical infrastructure protection right falls in its remit.

A Case for Better Protection of Critical Infrastructure

Like many other aspects of our economy and society, critical infrastructure is increasingly hyperconnected and now vulnerable to malicious cyber attacks. While the universal challenge for many organizations is to secure their information technology systems, the added and most important concern from a critical infrastructure perspective is to ensure that the operational technology systems that effectively control their equipment become smart and remote-enabled. Moreover, these operational technology systems are now reliant on software and hardware that are more accessible and therefore penetrable by hackers (WEF 2020). Relying on hyperconnected operational technology systems is problematic when some critical infrastructure does not have manual backups. In a global survey of approximately a thousand businesses, academics, and government experts in 2020, cyber attacks on critical infrastructures ranked fifth on the list of global risks (WEF 2020). Moreover, in a survey of nearly two thousand global utilities' technicians and administrators, more than half expected a cyber attack on their systems within the year, a quarter reported having been attacked, likely by a state actor, and nearly a third noted that cyber attacks on their operational technology often goes undetected (Siemens and Ponemon Institute 2019). In other words, the increased connectedness of critical infrastructure to the Internet of Things and other digitized infrastructure will complicate things further (Khari et al. 2016). Critical infrastructure has become the soft underbelly of cyber attacks, with disproportionate impacts on citizens' lives.

The Canadian Centre for Cyber Security (often known as the Cyber Centre; see Robinson, this volume), in its 2020 National Cyber Threat Assessment, made a direct risk assessment of Canada's critical infrastructure (CI) and found that "foreign state-sponsored cyber programs are probing our critical infrastructure for vulnerabilities" (CCCS 2020a). The same assessment noted that CI operators may be willing to pay millions in ransom to resume operations—a not-so-subtle warning that CI systems are indeed being attacked. The Cyber Centre report goes further and notes that state-sponsored actors are "very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals" (CCCS 2020a, 5). While the threat is

constant, the Cyber Centre notes that the likelihood of state-sponsored cyber attacks against critical infrastructure is low as long as "international hostilities" are kept at bay (CCCS 2020a, 5). This is a crucial point. When international conflict flares or escalates, as has been the case recently between Canada and China over the arrest of a senior Huawei executive, the threat of an attack is then elevated. While state actors may not necessarily want to target Canada, they are acquiring the capability and know-how in case they need it in the future for political leverage. In light of increased global tensions, especially between the United States and China, and the rise of populist-nationalist regimes that have eroded international co-operation and multilateralism, one cannot discount the fact that such an uneasy context could spur a cyber attack on Canadian CI from vengeful state or state-sponsored actors (CCCS 2020a).

Cyber attacks by malicious states or non-state actors on critical infrastructure could be catastrophic, potentially impacting millions. For example, Russian-sponsored cyber attacks attempted to penetrate American electrical systems in 2019 and have been tied to power outages in Ukraine in 2015 and 2016. Iranian operatives were reportedly able to infiltrate the computer system of a dam in New York in 2013. Perhaps the most famous cyber attack on CI is Stuxnet, a joint US-Israel effort that successfully inserted malware in Iranian nuclear infrastructures, damaging many centrifuges (Zetter 2014). The energy sector is not the only target, of course. North Korea, for example, attacked the SWIFT banking system, leading to millions of stolen dollars (Buchanan 2020). In late 2020, many news outlets reported that the United States suspected Russia had gained access to several US federal agencies' systems, which included access to a power grid. Russia was able to do so by operating a back door placed in a software widely used in the federal US government (Sanger, Perlroth, and Schmidtt 2021).

It is important to keep in mind that cyber attacks can have widely diffused consequences. Stuxnet's impact, for example, included Iranian critical infrastructure, but its spread infected other global systems as well. Even companies like Chevron in the United States found the same worm in their system (Kushner 2013). Stuxnet is not the only computer worm that spread beyond its intended target. NotPetya, the malware developed by Russia in the cyber attack against Ukraine, spread all over Europe, forcing

Denmark's largest export company, Maersk, to briefly shutdown its entire operation. In the end, the virus's path was wide, causing about $10 billion dollars (McQuade 2019). As nation-states increasingly use cyber weapons, we should therefore expect more spillover and collateral damage. As such, the thinking behind the defence of critical infrastructure cannot rest solely on expecting a direct attack from technologically capable adversaries or rivals.

While the most capable threat to CI comes from state actors, there is increasing concerns that cyber criminals are also interested and willing to attack CI for ransom. Sadly, a US Defense Information Systems Agency assessment noted that when they conducted war games to test the resiliency of their systems, only 4 per cent of operators had realized there was an attack, with just 1 in 150 reporting the attempted attack; more often than not, the phishing attempts were successful (Congressional Record 2000). This led Congressman Rob Andrews, Democrat of New Jersey, to conclude that

> a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos, strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees. Such a strategic attack mounted by a cyber-terrorist group, either sub-state or non-state actors, that is to say either terrorist groups that are not part of any state or terrorist groups that are sponsored by a rogue state, would shut down everything from electric power grids to air traffic control centers. (Congressional Record 2000)

Canada and the United States are increasingly adept at tracing the origins of an attack after the fact. The Cybersecurity and Infrastructure Security Agency (CISA) and the US Department of Defense (DoD), for example, are confident that they are able to trace back any cyber attack to its source if asked to do so by the relevant state actors and agencies.[1]

The question remains, however: What to do once the attacker is identified? Would Canada mount a counterattack against state or non-state actors? Even if the damages were significant, how to disentangle the web of actors involved? China, North Korea, and Russia, for example, use

various proxies in the form of state-funded hacking groups (Stevens 2021). While state agencies can likely pinpoint the origin of an attack, the chain of certainty breaks down afterwards as to whether it was an independent action from the group or commanded by state officials. When there is a high chance of plausible deniability, as is often the case with cyber attacks, states are less likely to want to counterattack.

As technological advancements in cyber capabilities progress and are increasingly available to non-state actors, vulnerabilities in Canada's CI increase (Majot and Yampolskiy 2015). This is further complicated by the move toward emerging technologies like quantum computing. While existing encryption methods can at times resist traditional cyber attacks, the future of quantum computing, which follows the rules of quantum physics, is making computers and cyber attacks more robust (Chen et al. 2016; Alagic et al. 2019). Quantum computers are faster and more sophisticated, speeding up the process of decoding security measures such as security keys. As some states develop their quantum capabilities sooner than others, this technology will represent a powerful advantage. Our critical infrastructure, and invariably our public safety and sense of national security, will be threatened by the "supercomputers" capable of quantum cyber attacks by either state adversaries or malicious actors (Herman and Friedson 2018). For example, if China or Russia develop quantum computers able to dismantle cybersecurity measures, Canada's CI system will be exposed. Patching these vulnerabilities through new and sophisticated cryptography will take considerable resources, expertise, and political commitment. Moreover, much of Canada's CI ecosystem is further exposed because its designs are retrofitted for connectivity and can be outdated (Ellinas et al. 2015, 5–6). In other words, these old systems are increasingly exposed in the era of quantum computing. While the risks are high, it is also essential to be mindful of an important and yet neglected concern that CI assets are often owned and supervised by multiple stakeholders with varied regulatory responsibility and governing authority (Slayton and Clark-Ginsberg 2018).

While citizens require access to critical infrastructure, the increasing complexity of these systems requires improved government coordination. Ensuring technical resilience to a potential cyber attack requires a multi-stakeholder approach synchronizing multiple levels of government,

policy-makers from difference agencies, scientific and academic experts, and the private sector. Indeed, Canadians' well-being, as well as the Canadian government's effectiveness and cyber defences, are locked in relationships of interdependence.

The pandemic provides the necessary disruption to attract policy-makers' attention and to challenge conventional thinking about threats to critical infrastructure. We have already seen that the pandemic has exposed how the health sector is subject to cyber attacks, thereby noting the gaps in the security of vital systems and information. Canadians expect governments to be well-coordinated when responding to potential cyber attacks and well-prepared to prevent exposure to critical infrastructure systems' technical vulnerabilities (CIRA 2018). Canadians presume that they will have reliable and uninterrupted service and that governments will maintain the integrity of CI systems. If a CI sector is disrupted, the negative economic, political, and socio-psychological impact on Canadians would be broad and impact millions (see Dynes, Goets, and Freeman 2008, 15–16, for an American study of this issue). Officials need to bridge the potential gaps in preparedness to withstand a cyber attack on Canadian CI by working better with diverse communities of technical, policy, and industry professionals. This includes identifying vulnerabilities and developing intervention opportunities to pre-empt malicious actors who would use cyber attacks to harm people living in Canada.

Getting the Politics of Protecting Critical Infrastructure Right

Canada's history of governing critical infrastructure is unique and unlike our southern neighbour, where many tend to look at the federal government with skepticism. As Boyle and Speed (2018) note, Canada's constitutional framework has empowered the federal government to be more active in coordinating a response to emergencies and external attacks. This is an advantage Canada has over other federal systems. In this context, Canada's national security and intelligence community has an important role to play in ensuring the resilience of its interconnected critical infrastructure.

Public Safety Canada is tasked by the National Cross Sector Forum's 2018–2020 Action Plan for Critical Infrastructure and by the *Emergency*

Management Act to take the lead. Public Safety has the necessary legislative authority and is in the process of reviewing CI resilience, as per the 2018–2020 Action Plan. However, it is hobbled by the fact that the National Strategy for Critical Infrastructure was published in 2010 and is, therefore, outdated. One way to secure Canadian infrastructure would be to take stock of the rapid advances in technology and techniques developed in the last ten years and to revise the strategy accordingly.

Protecting critical infrastructure is also riskier because of the challenges of policy coordination among multiple government agencies, gaps in varying levels of authority and responsibility, and the information asymmetry among various stakeholders. As former Assistant Deputy Minister Andrew Graham, writing on Canadian critical infrastructure, put it, "research to date would indicate that the federal government, while trying to provide a form of general leadership and sharing platforms, lacks most of the policy and operational clout to impose solutions, even when they are known. It therefore tries to provide leadership in partnership with many actors, a nascent effort" (Graham 2012, 2). In other words, there are limits to what a solely technical solution can provide, as stakeholders often face imperfect information, cognitive biases, and attribution and detection failures. This is further complicated when stakeholders such as CI operators experience two-level problems, whereby organizational preferences to stay quiet can be incompatible with the need to alert authorities (Bellé, Cantarelli, and Belardinelli 2018; Head and Alford 2015).

In addition to the threat of cyber attacks by state adversaries and malicious non-state actors, the complex network of stakeholders and decision-makers with varied levels of responsibility and authority also creates vulnerabilities in Canada's CI ecosystem (Bernstein 2009). This is compounded by the diffuse nature of responsibility and authority over many systems, as there is no centralization of control over a wide number of stakeholders, from private industry owners/operators to provincial and federal governments and regulatory bodies. This division of authority and the multiple layers of responsibility challenge Canada's emergency preparedness to prevent and respond to cyberattacks (Boyle and Speed 2018).

Critical infrastructure insecurity also opens the door to cascading failures. These governance challenges can further undermine Canada's ability to prevent and respond to cyber attacks. This is where the national

security and intelligence community needs to ensure that gaps in governance do not expose systems to foreign attacks. While citizens require access to critical infrastructure to live secure and prosperous lives, the increasing complexity of these systems means that stakeholders cannot respond to threats without proper coordination. Moreover, threats are distributed asymmetrically: some groups and communities are more vulnerable to critical infrastructure failures than others. Only governments can best protect the most vulnerable from these failures.

COVID-19 and Critical Infrastructure

The COVID-19 pandemic, and the digital transformation it has accelerated, means that policy-makers must contend with a new landscape in which non-state actors, both violent and peaceful, have access to technology that can disrupt social, political, and economic life. Moreover, the pandemic makes it necessary for the Canadian government to further assess the impact of exogenous shocks on critical infrastructure, the opportunities this type of event creates to attack CI, and the proper tactics to maintain security. Large-scale disasters are often exploited for cyber attacks, for example, and COVID-19 is a case in point. Recent meta-analyses have demonstrated a significant increase of cybercrimes and more advanced attacks since the start of the pandemic (Aladenusi 2020; Williams et al. 2020). Attacks on banking infrastructure have multiplied, for example, since the UK government announced relief funding for its citizens (Lallie et al. 2020, 6). The health-care system in Canada, as in other nations, has been the target of ransomware attacks during the pandemic (CCCS 2020b). Given the seriousness of the situation and what it would mean for patients to delay their treatments and the potential reputational damage hospitals would accrue, many hospitals opt to pay the ransom (Hijji and Alam 2020, 7160; Lallie et al. 2020, 13).

As cyber capabilities advance and as the connectedness of critical infrastructure opens new vulnerabilities, threats increase. Some of these risks are further complicated by the fact that Canada's critical infrastructure has shifted from public ownership and control to more private control, adding multiple operators, varied corporations with their own shareholder interests, and a vast number of asset owners. Private-sector

operators, for example, may agree to pay small ransomware requests to get their data returned or to access their systems if, from their perspective, the cost-benefit calculation makes complying with the demands less costly. Moreover, there is an impulse in the normative shift toward building resiliency by encouraging operators to self-govern. Governments are increasingly investing in raising awareness and self-reporting but are less interested in playing a heavy hand in terms of enforcement. As Boyle (2019) explains, since Public Safety Canada started its Regional Resilience Assessment Program, CI operators are asked to voluntary self-assess their operations using a US-designed critical infrastructure resilience tool (CIRT). This CIRT helps operators measure their own security, preparedness, and mitigation strategies, and then compare these to other operators, who could see how they measure up without disclosing potentially embarrassing vulnerabilities (also see Quigley, Bisset, and Mills 2017, 66–70).

The COVID-19 pandemic has also highlighted other difficulties in securing and governing CI. Specifically, it has made salient the issue of low-tech methods putting infrastructure at risk. The pandemic has forced a massive and rapid shift of work and operations online for most private and public entities. Companies, like Zoom, that were previously relatively unknown outside of the business world are now household names. Concurrently, this has led to an increase in the use of social-engineering techniques to access critical infrastructure through the most vulnerable access point: individuals operating from home. These are techniques where the user, rather than the system, is the primary target (Carrapico and Farrand 2020, 1111–12). Almost 80 per cent of known cyber attacks during the pandemic have involved social-engineering techniques, which include phishing and other email scams (Hijji and Alam 2020, 7153). The most secure system is only as secure as the computer literacy and digital hygiene of its operators. In other words, the more access points that cyber attackers have to inflict damage on CI operators, the more the CI is at risk. Platforms like Zoom and Microsoft Teams, for example, have been targeted in part due to the lack of users' vigilance (Matthews 2020). Other factors are at play as well. Online video conferencing such as Zoom, for example, have a lot of their traffic directed through Chinese servers. This has raised Western government and corporate fears that using Zoom might expose their data and information to the Chinese government or corporate espionage.

Conclusion

The federal government is in charge of, and accountable for, keeping Canada's critical infrastructure safe. In this context, there is a need for better coordination across departments and agencies within the national security and intelligence community, and between the public and private sectors. A lack thereof has proven time and again to be the vulnerable point in many attacks on critical infrastructure.

The COVID-19 pandemic has rung the alarm bell: we are, willingly or not, moving online (Murugesan 2020). We are already at the next frontier; it is now a question of how the Canadian government, and others, will react. Another recommendation is, therefore, to leverage the pandemic to reorganize how national security and intelligence departments and agencies engage with the private sector. Canadians as a whole have a tendency to think of cybersecurity in remote terms, something that is applicable elsewhere but not here. Yet too many Canadians have been the victim of Canada Emergency Response Benefit (CERB) fraud, for example, or have had their information stolen from their banks. Cyber attacks are no longer a faraway or speculative threat: they are now affecting us in the present (Quigley, Bisset, and Mills 2017, 187). The current trend toward greater privatization, on the one hand, and the distrust of government action, on the other, must be bridged. Moreover, moving toward a more coordinated and centralized cyber-response capability may be even more necessary moving forward, given the reluctance of the private sector to adequately invest in risk management (59–60). Lastly, we recommend the mandatory use of tabletop exercises on attacks against CI to better inform operators and governments of gaps in preparedness. While these are voluntary for now, a greater uptake and involvement of CI operators would help keep Canadians safe.

NOTE

1 This was discussed by officials from both agencies during the 2020 Homeland Defense Academic Symposium, held by the North American Aerospace Defense Command and US Northern Command from 1 to 3 December 2020.

REFERENCES

Aladenusi, Tope. 2020. "COVID-19's Impact on Cybersecurity." *Deloitte*, March 2020. https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html.

Alagic, Gorjan, Jacob M. Alperin-Sheriff, Daniel Apon, David Cooper, Quynh H. Dang, Carl A. Miller, Dustin Moody, Rene C. Peralta, Ray A. Perlner, Angela Y. Robinson, Daniel Smith-Tone, and Vi-Kai Liu. 2019. "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process." *National Institute of Standards and Technology*, report no. 8240 (January). https://doi.org/10.6028/NIST.IR.8240.

Bellé, Nicola, Paola Cantarelli, and Paolo Belardinelli. 2018. "Prospect Theory Goes Public." *Public Administration Review* 78, no. 6 (June): 828–40. https://doi.org/10.1111/puar.12960.

Bernstein, Daniel J. 2009. "Introduction to Post-Quantum Crytography." In *Post Quantum Cryptography*, edited by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, 1–14. Berlin: Springer.

Boyle, Philip J. 2019. "Building a Safe and Resilient Canada: Resilience and the Mechanopolitics of Critical Infrastructure." *Resilience* 7, no. 1 (October): 59–82. https://doi.org/10.1080/21693293.2018.1531476.

Boyle, Philip J., and Shannon T. Speed. 2018. "From Protection to Coordinated Preparedness: A Genealogy of Critical Infrastructure in Canada." *Security Dialogue* 49 (3): 217–31. https://doi.org/10.1177/0967010617748541.

Buchanan, Ben. 2020 "How North Korea Hackers Rob Banks Around the World." *Wired*, 28 February 2020. https://www.wired.com/story/how-north-korea-robs-banks-around-world/.

Carrapico, Helena, and Benjamin Farrand. 2020. "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy." *Journal of European Integration* 42 (8): 1111–26. https://doi.org/10.1080/07036337.2020.1853122.

CCCS (Canadian Centre for Cyber Security). 2020a. "National Cyber Threat Assessment." Government of Canada, last modified 16 November 2020. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

———. 2020b. "Renewed Cyber Threats to Canadian Health Organizations." Government of Canada, 30 October 2020. https://cyber.gc.ca/en/alerts/renewed-cyber-threats-canadian-health-organizations.

Chen, Lily, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. 2016. "Report on Post-Quantum Cryptography." *National Institute of Standards and Technology*, report 8105 (April). http://dx.doi.org/10.6028/NIST.IR.8105.

CIRA (Canadian Internet Registry Authority). 2018. "Canadian Cybersecurity Survey." Canadian Internet Registry Authority, Spring 2018. https://www.cira.ca/resources/cybersecurity/report/2018-canadian-cybersecurity-survey-spring-edition.

Congressional Record. 2000. "Cyber Terrorism, a Real Threat to Society." *Congressional Record* 146, no. 28 (14 March): H974–9. https://www.govinfo.gov/content/pkg/CREC-2000-03-14/html/CREC-2000-03-14-pt1-PgH974.htm.

Dynes, Scott, Eric Goetz, Eric, and Michael Freeman. 2008. "Cyber Security: Are Economic Incentives Adequate?" In *Critical Infrastructure Protection*, edited by E. Goetz and E. Shenoi, 15–28. New York: Springer.

Ellinas, Georgios, Christos Panayiotou, Elias Kyriakides, and Marios Polycarpou. 2015. "Critical Infrastructure Systems: Basic Principles of Monitoring, Control, and Security." In *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, edited by E. Kyriakides and Marios Polycarpou, 1–30. Berlin: Springer.

Graham, Andrew. 2012. "Canada's Critical Infrastructure: When Is Safe Enough Safe Enough?" *Macdonald-Laurier Institute*, 7 December 2011. https://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf.

Head, Brian W., and John Alford. 2015. "Wicked Problems: Implications for Public Policy and Management." *Administration and Society* 47, no. 6 (March): 711–39. https://doi.org/10.1177/0095399713481601.

Herman, Arthur, and Idalia Friedson. 2018. *Quantum Computing: How to Address the National Security Risk*. Washington, DC: Hudson Institute. https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf

Hijji, Mohammad, and Gulzar Alam. 2021. "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions." *IEEE Access* 9:7152–69. DOI: 10.1109/ACCESS.2020.3048839.

Khari, Manju, Manoj Kumar, Sonakshi Vij, Priyank Pandey, and Vaishali. 2016. "Internet of Things: Proposed Security Aspects for Digitizing the World." 3rd International Conference on Computing for Sustainable Global Development, 31 October 2016. https://ieeexplore.ieee.org/document/7724648.

Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum*, 26 February 2013. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Lallie, Harjinder Singh, Lynsay A. Shepard, Jason R. C. Nurse, Arnau Erola, Gregory Epiphanio, Carsten Maple, and Xavier Bellekens. 2020. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." *arViv* (June): 1–20. https://arxiv.org/abs/2006.11929.

Majot, Andy, and Roman Yampolskiy. 2015. "Global Catastrophic Risk and Security Implications of Quantum Computers." *Future: The Journal of Policy, Planning, and Futures Studies*, no. 72 (December): 17–26. https://doi.org/10.1016/j.futures.2015.02.006.

Matthews, Lee. 2020. "500,000 Hacked Zoom Accounts Given Away for Free on the Dark Web." *Forbes*, 13 April 2020. https://www.forbes.com/sites/leemathews/2020/04/13/500000-hacked-zoom-accounts-given-away-for-free-on-the-dark-web/?sh=29b9e89c58c5.

McQuade, Mike. 2008. "The Untold Story of NotPetya, the Most Devasting Cyberattack in History." *Wired*, 22 August 2008. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Murugesan, San. 2020. "IT Risk and Resilience—Cybersecurity Response to COVID-19." *IT Professional* 22 (3): 12–18. DOI: 10.1109/MITP.2020.2988330.

Public Safety Canada. 2014. "Critical 5: Forging a Common Understanding for Critical Infrastructure." Government of Canada, March 2014. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr-en.pdf.

Quigley, Kevin, Ben Bisset, and Bryan Mills. 2017. *Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure*. Montreal: McGill-Queen's University Press.

Sanger, David E., Nicole Perlroth, and Eric Schmidtt. 2020. "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit." *New York Times*, 14 December 2020. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Siemens and Ponemon Institute. 2019. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" *Siemens and Ponemon Institute*, 4 October 2019. https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf.

Slayton, Rebecca, and Aaron Clark-Ginsberg. 2018. "Beyond Regulatory Capture: Coproducing Expertise for Critical Infrastructure Protection." *Regulation and Governance* 12 (1): 115–30. https://doi.org/10.1111/rego.12168.

Stevens, Corbin. 2021. "Cyber Doctrines and the Risk of Nuclear Crisis Instability Part 2: Russian and Chinese Use of Proxy." *Council on Foreign Relation*, 25 January 2021. https://www.cfr.org/blog/cyber-doctrines-and-risk-nuclear-crisis-instability-part-2-russian-and-chinese-use-proxies.

WEF (World Economic Forum). 2020. *The Global Risks Report 2020*. Insight Report, 15th ed. Geneva: World Economic Forum. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

Williams, Meilee Christina, Rahul Chaturvedi, and Krishnan Chakravarthy. 2020. "Cybersecurity Risks in a Pandemic." *Journal of Medical Internet Research* 22 (9): 1–4. https://doi.org/10.2196/23692.

Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, 11 March 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.