Testimony

Cyber Threats to Canada's Defence Infrastructure

Quentin E. Hodgson

CT-A2682-1

Testimony presented before the Canadian Senate Standing Committee on National Security, Defence and Veterans Affairs on March 20, 2023.

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/CTA2682-1.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Limited Print and Electronic Distribution Rights

www.rand.org

Cyber Threats to Canada's Defence Infrastructure

Testimony of Quentin E. Hodgson[1]
The RAND Corporation[2]

Before the Standing Committee on National Security, Defence and Veterans Affairs
Senate of Canada

March 20, 2023

Thank you for the opportunity to participate in this hearing on the important topic of cyber threats to Canada's defence infrastructure. My name is Quentin Hodgson, and I am a senior international and defense researcher at the RAND Corporation, a nonprofit, nonpartisan public policy research organization.

My work at the RAND Corporation encompasses the issues of cybersecurity, cyberspace operations, risk management, and critical infrastructure protection. For my testimony today, I will briefly touch on three issues: the nature of threats in cyberspace; the potential impacts those threats can have for the security of North America; and what the governments of Canada and the United States can do to address those threats.

The Nature of the Threat

Cyber threats to critical infrastructure have been a concern for at least three decades. The report of the U.S. President's Commission on Critical Infrastructure Protection in 1997 highlighted that there was no expectation of impending cyberattack but "did find widespread

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

capability to exploit infrastructure vulnerabilities."[3] Since that time, we have seen growth in the sophistication and skill of both nation-state and non-nation-state cyber actors.[4] At the same time, the vulnerabilities these actors exploit endure for long periods.[5] Cyber threats affect not just business information communication technology; increasingly, operational technology—the hardware and software that control physical processes—is also subject to a variety of threats, from the manufacturing sector, to electricity generation and distribution, to water treatment plants.[6]

Cyber threats encompass compromise of sensitive information, cyber espionage, ransomware that costs businesses millions of dollars a year, and potentially more-destructive attacks. We have also seen how cyberspace can be harnessed to spread misinformation and disinformation that undermine confidence in public institutions and sow discord among the people in democratic nations.[7] So the threats we face as democracies continue to grow.

The Potential Impact of the Cyber Threat on National Security and Defence

The ongoing conflict in Ukraine provides an interesting case study of how an adversary could employ cyber capabilities in the context of military operations. There has been considerable debate about Russia's use of cyber in the Ukraine conflict, prompting questions as to why we did not see more use of cyber, why the cyberattacks we did see appeared marginally effective, and what the implications for future conflict are.[8] Some, including Canada's Centre for Cyber Security, believe that Russian cyber activity has been greater than publicly reported.[9] What we have seen is that Russia has used cyber operations to target government institutions, media, and telecommunications in Ukraine, including a widely reported cyberattack on the satellite

---

[3] Robert T. Marsh, *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, May 1997.

[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 6, 2023.

[5] Jonathan Greig, "Average Time to Fix High Severity Vulnerabilities Grows from 197 Days to 246 Days in 6 Months: Report," ZDNET, July 27, 2021, https://www.zdnet.com/article/average-time-to-fix-high-vulnerabilities-grows-from-197-days-to-246-days-in-6-months-report/.

[6] Dragos, *ICS/OT Cybersecurity Year in Review 2022*, 2023; Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," *Wired*, February 8, 2021.

[7] Elias Groll, "US Intel: Chinese Influence Operations Are Growing More Aggressive, More Similar to Russia's," CyberScoop, March 8, 2023, https://cyberscoop.com/china-worldwide-threats-cyber/.

[8] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influence, and Implications," Carnegie Endowment for International Peace, December 16, 2022. As of March 15, 2023: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

[9] Canadian Centre for Cyber Security, "Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine," updated July 14, 2022, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine.

communications system provided by Viasat that affected customers across Europe.[10] The Ukrainian government, however, has clarified that the Viasat attack had a marginal effect on military communications when it occurred in February 2022.[11]

The Russian invasion of Ukraine is an ongoing conflict, and we do not yet know how it will end. Some observers expect Russian cyber activity to expand as the conflict drags on.[12] Further, we should not expect that future conflicts or crises will entail the same types of cyber operations as those Russia has already employed.

We should consider how an adversary in a crisis or emerging conflict could employ cyber capabilities to impede the ability to deploy and support military forces, degrade or deny the ability to command and control those forces, and create circumstances in which militaries have less trust in their systems' abilities to operate as needed. Cyber-enabled espionage affects our economies as intellectual property is stolen to enable the growth of industry that can undercut North American businesses. This espionage is not just an economic threat, however, because it also provides adversaries with insights into North American military capabilities and support infrastructure.

At this point, I want to emphasize that government and the private sector should and must take the threat of cyberattack on critical infrastructure seriously. At the same time, we should also understand that executing a destructive cyberattack, particularly one that would have significant impacts on operations and cascading effects in other sectors, is difficult. For example, the ransomware attack on Colonial Pipeline in May 2021 had widespread effects in the United States, including long lines at gas stations for fuel, but the ransomware attack itself affected business information systems that monitored the pipelines, not the operational technology directly. The company decided to take the pipelines offline to prevent the ransomware from spreading, but the ransomware did not directly affect operational systems.[13]

What Can We Do to Address These Threats?

Governments have developed an array of tools and relationships to address these threats. They have made attempts to agree norms of behavior in cyberspace.[14] Leaders have sought to signal that cyberattacks on critical infrastructure will not be tolerated.[15] In addition, there is a

---

[10] Viasat, "KA-SAT Network Cyber Attack Overview," March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

[11] Kim Zetter, "Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," *Zero Day*, September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.

[12] Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare in Ukraine: What We Have Learned About Nation State Tactics So Far and What May Be on the Horizon," Microsoft, March 15, 2023.

[13] Colonial Pipeline, "Media Statement Update: Colonial Pipeline System Disruption," press release, updated May 17, 2021, https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

[14] United Nations Office for Disarmament Affairs, "Group of Governmental Experts," webpage, undated, https://www.un.org/disarmament/group-of-governmental-experts/.

[15] Vladimir Soldatkin and Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off-Limits,'" Reuters, June 16, 2021.

vibrant and growing private sector providing cybersecurity services to critical infrastructure entities, including vulnerability assessments, penetration testing, "hunt" operations to actively identify malicious cyber activity, and incident response. We have seen the development of better and more-actionable intelligence sharing about cyber threats from government and through bodies such as Information Sharing and Analysis Organizations.[16] Companies now understand not only what the threat is but how it can affect them and their operations. But the largest companies are not the whole story; small and medium-sized businesses play a critical role in our economies and in supporting the defence sector, which makes them a target for exploitation.

In the United States, government has sought to encourage a largely voluntary approach to adopting cybersecurity standards, rather than imposing regulations. More recently, the government has moved to leverage existing powers, such as issuing additional guidance and regulatory power, since the voluntary approach is seen as insufficient. For example, the U.S. Environmental Protection Agency issued guidance to the states on including cybersecurity as part of sanitary surveys of public water systems.[17] Similarly, the U.S. Transportation Security Administration revised its cybersecurity requirements for oil and gas pipelines because of the Colonial Pipeline incident.[18]

In the U.S. Department of Defense, there are several programs that are attempting to address the concerns over the cybersecurity of the defence industrial base and military weapon systems and installations. The first is the Cybersecurity Maturity Model Certification (CMMC) program, which is designed to bring more clarity and confidence to the security of sensitive but unclassified information processed on nonfederal networks. The CMMC program has experienced challenges in getting off the ground, not least due to concerns about costs and the role that third-party assessors will play in certifying companies' cybersecurity programs.[19] The second initiative is the Strategic Cybersecurity Program that the U.S. Congress has mandated. The Strategic Cybersecurity Program is intended to institutionalize and expand efforts to identify and address cyber threats to military systems and critical infrastructure.[20]

Despite the challenges in implementation, these are laudable efforts, and the broad goals are welcome. But we also need to address resiliency for when things inevitably go wrong. The common refrain in cybersecurity is that defenders have to defend everywhere, while the attacker only has to be successful once. Although this is somewhat hyperbole, the sentiment stands that we should expect that in a crisis or conflict our adversaries will find ways to employ cyber to

---

[16] See the ISAO Standards Organization website, https://www.isao.org.

[17] Radhika Fox, "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process," U.S. Environmental Protection Agency, memorandum to state drinking water administrators and water division directors, March 3, 2023.

[18] U.S. Transportation Security Administration, "TSA Revises and Reissues Cybersecurity Requirements for Pipeline Owners and Operators," press release, July 21, 2022, https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners.

[19] Meredith Roaten, "Defense Base Prepares for New CMMC Rules (Updated)," *National Defense*, November 28, 2022, https://www.nationaldefensemagazine.org/articles/2022/11/28/defense-base-prepares-for-new-cmmc-rules.

[20] Public Law 116-283, National Defense Authorization Act for Fiscal Year 2021, Section 1712, Modification of Requirements Relating to the Strategic Cybersecurity Program and the Evaluation of Cyber Vulnerabilities of Major Weapon Systems of the Department of Defense.

degrade our ability to respond. Government must be prepared for those eventualities and work with the defence sector and supporting infrastructure to develop contingency plans to overcome those challenges, to develop redundancy in critical systems, and ensure that systems degrade gracefully—and not catastrophically—when attacked.

Thank you for this opportunity. I look forward to your questions.