Centre for International Governance Innovation

Policy Brief No. 178 — October 2023

Addressing Canada's Exposure to Space-Cyber Threats

Eytan Tepper

Key Points

→ Canada relies on critical space-based infrastructure for its security and economy, yet the 2018 National Cyber Security Strategy does not address threats to that infrastructure.

→ In cooperation with industry, Canada should launch a national effort on space-cyber security, to include adopting legislation and policy, developing defensive capabilities, and introducing best practices to protect space assets.

→ Already a leader in cybersecurity, Canada should encourage the establishment of a Canadian space-cyber security sector and the training of its workforce. In doing so, Canada can not only mitigate risk but also create significant economic opportunity.

→ At the global level, Canada has the capacity — and, arguably, the responsibility — to promote international norms of behaviour for the space-cyber nexus.

Introduction: The Missing Space-Cyber Policy

The war in Ukraine demonstrated that cyberattacks on space systems and their terrestrial components (space-cyber attack) are a low-risk, high-yield tool already in use that can affect both national security and civil society (Tepper 2022). On the eve of the Russian invasion, a cyberattack associated with Russia disrupted the services of Viasat, a US commercial satellite internet company, in Ukraine, which "plunged tens of thousands of people into internet darkness. Among them were parts of Ukraine's defenses" (Burgess 2022). The effects were felt far into Europe, where even a month later wind turbines in Germany remained offline (ibid.). Moreover, criminal organizations and terrorist groups have also already launched cyberattacks on space-based services (Tepper 2022).

As a highly developed country, Canada is reliant on space-based infrastructure, notably satellites providing communication, positioning, navigation, timing and remote sensing. Nearly a decade ago, US Lt. Gen. John A. Toolan Jr., then the commanding general of I Marine Expeditionary Force, noted that operations in Iraq and Afghanistan had made the Marines "addicted to... space-based systems," and that US forces realized they needed to develop systemic resilience and readiness to meet the very real risk of "a day without space" (Magnuson 2014). The Canadian Forces have equally

About the Author

Eytan Tepper is research coordinator and lecturer, space governance, at the Graduate School of International Studies, Laval University, and a visiting assistant professor at Indiana University Bloomington and director of its Space Governance Lab. He teaches and leads a research project on space-cyber security governance.

Eytan earned his doctorate from the McGill University Faculty of Law, where he was affiliated with the Institute of Air and Space Law, and subsequently pursued a post-doctoral fellowship at the New York University School of Law. As a lawyer, he had a career spanning the public and private sectors, resolving issues related to international trade and cooperation and financial and industrial policy. His work in the private sector included representing Fortune 500 companies (among them, Johnson & Johnson, Pfizer, Merck, Eli Lilly) and working on Albert Einstein's estate.

become reliant on their space capabilities.[1] Space systems have also become an essential part of the civilian infrastructure. A "day without space" would mean outages and disruptions across essential systems: the internet and cellphone networks, television and radio broadcasting, banking and payment systems and, possibly, electricity and water supply (Hollingham 2013; Magnuson 2014; Ogden 2023). In other words, disruption of select space-based applications could bring an economy to a standstill. In Germany, the point of departure of the national space-cyber security strategy from the Federal Office for Information Security is that "satellite applications are now a virtually indispensable part of day-to-day life. Space-based systems are also especially relevant for national security" (Bundesamt für Sicherheit in der Informationstechnik [BSI], n.d.).

Policy makers and space companies around the world are increasingly aware of the threats, but governments' response is either incipient, as in the United States and Germany, or non-existent, as in Canada. In the United States, several instruments of policy and standards are in the works or were introduced by the president, Congress, the Infrastructure Security Agency or the Space Force. Germany's Federal Office for Information Security adopted a national space-cyber security strategy and introduced standards, in cooperation with the industry (BSI, n.d.; 2022). However, neither Canada's most recent National Cyber Security Strategy (Public Safety Canada 2018) nor its international cyber policy[2] addresses the space-cyber nexus. This gap is a major limitation of Canada's approach, which stands in stark contrast to our allies' initiatives.

Space-cyber threats are reshaping the nature of national defence and economic resilience, and Canada should adopt a dedicated policy and allocate sufficient resources to address these threats. This policy brief sketches several steps Canada can take to prepare for and defend its security and economy against space-cyber attacks.

[1] See www.canada.ca/en/air-force/corporate/space/capabilities.html#.

[2] See www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=eng.

Fortress Canada in Space

To face the challenge, Canada should fortify its space infrastructure, including those assets operated by commercial companies, against cyberattacks. Further, unlike traditional fortress strategy, which aims to block all infiltration attempts, the process of fortifying Canada's space-cyber defences should take into account that some space-cyber attacks *will* be successful. Thus, in addition to building defences, we must employ detection and mitigation measures — that is, build *resilience* into the use of critical space assets, to minimize the impact of any disruption. Doing so requires launching a national effort on the space-cyber nexus, in terms of capabilities and governance, coordinated across several government ministries and in close cooperation with the private sector and academe. Such a comprehensive effort needs to include governance aspects, the development of domestic capabilities, engagement with and support for the private sector, and the promotion of international norms.

Aspects of Space-Cyber Governance

Declaring Space Infrastructure as Critical Infrastructure

The US Department of Homeland Security defines *critical infrastructure* as physical or cyber systems or assets "so vital...that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[3] Canada sees systems, facilities, technologies, services, networks and assets that are essential to the well-being of Canadians and the Government of Canada as critical infrastructure.[4] Space infrastructure — from satellites to the ground stations and relay stations that transfer data up and down to satellites — falls within these definitions, although neither country has yet declared space infrastructure as critical. The United States may be the first to do so, as a bipartisan bill introduced in Congress proposes (Bennet 2023). Space infrastructure enables key economic and security functions, and we can consider free and secure space operations as vital to advancing "security, economic prosperity, and scientific knowledge" in Canada as in the United States (White House 2020, sec. 1). If Canada were to declare space infrastructure as critical infrastructure, it would facilitate and mandate the allocation of proper attention and resources to the protection of this infrastructure.

Establishing a Task Force and Introducing National Policy and Regulation

Canada should establish a dedicated task force of leading experts within the space-cyber nexus, to identify and explore the underlying policy gaps, challenges and considerations as space-cyber security pertains to Canada, and to suggest ways to address them in a detailed report. The task force should engage with public and private sector leaders on the nature of the threats, the available policy options, and the limitations and drawbacks of each option, and also solicit their suggestions for an adequate national policy and regulatory framework.

Public Safety Canada's mid-term review of Canada's National Cyber Security Strategy referred to the prime minister's committment to developing and implementing "a renewed National Cyber Security Strategy, which will articulate Canada's long-term strategy to protect our national security and economy, deter cyber threat actors, and promote norms-based international behavior in cyberspace."[5] This promised revamping of the strategy should address issues related to threats to space-based infrastructure and applications. Developing a robust national policy is necessary for a coordinated effort. Regulation may be needed to prescribe authority and set basic, legally binding rules. Preparation of the policy and regulation should be informed by the United States' and Germany's initiatives, as outlined in the next section.

[3] See www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[4] See www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx.

[5] See www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx#.

Models of Guidelines and Best Practices from the United States and Germany

The United States and Germany have adopted several guidelines and best practices on space-cyber security, namely:

- the US Space Policy Directive-5: Cybersecurity Principles for Space Systems (SPD-5), adopted in 2020 by then president Donald Trump, and providing a set of best practices for government agencies and commercial companies;[6]
- guidance published in December 2022 by the US National Institute of Standards and Technology (NIST): *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control* (Lightman, Suloway and Brule 2022);
- the Cybersecurity Advisory on securing communication satellites from cyberattacks, published by the US Cybersecurity & Infrastructure Security Agency (CISA) with the Federal Bureau of Investigation (CISA 2022);
- the work in progress of the US Space Force on new satellite cybersecurity standards that will apply to the private sector satellite communication providers working with the military (Waterman 2021);
- the Department of Homeland Security's Space Policy (Mayorkas 2022);
- a bipartisan bill introduced in May 2023, the Satellite Cybersecurity Act;[7] and
- Germany's national space cybersecurity strategy (BSI, n.d.), and the standards introduced by the Federal Office for Information Security, in cooperation with the industry, on "IT baseline protection profile for space infrastructures" (BSI 2022).

Canada may similarly introduce guidelines and recommend best practices modelled on the US and German ones. The principles and guidelines in the next four subsections are based on a synthesis of takeaways from the documents listed above, and several draw, in particular, from language in SPD-5 and a related memorandum.[8]

Umbrella Strategy

- As articulated in SPD-5, "effective cybersecurity practices arise out of cultures of prevention, active defense, risk management, and sharing best practices."[9]
- In addition, the government should adopt a multi-stakeholder approach by which it will work together with the industry and other non-governmental organizations on space-cyber security.
- Finally, the government, together with the industry, should build resilience into the use of critical space assets to minimize the impacts of any disruption.

Design Principles for Space Systems

The design of space systems should use the "secure by design" approach, namely, that security is considered and embedded at the design phase and not as an afterthought.[10] Thus, the design takes into account not only the functions the system should perform but also that it should be foundationally secure, as free of vulnerabilities and impervious to attack as possible. With this in mind, key takeaways from SPD-5 are:

- Space systems should be designed to be able to continuously monitor, anticipate and adapt so that they can effectively respond to evolving malicious cyber activities that could manipulate, disrupt, disable or surveil space system operations.
- Space systems should be designed to "achieve and maintain an effective and resilient cyber survivability posture throughout the space system lifecycle,"[11] so they remain mission capable even after a cyberattack.

[6] *Space Policy Directive-5 of September 4, 2020*, 85 Fed Reg 56155 (2020) [SPD-5], online: <www.govinfo.gov/content/pkg/FR-2020-09-10/pdf/2020-20150.pdf>.

[7] US, Bill S 1425, *Satellite Cybersecurity Act*, 118th Cong, 2023 [*Satellite Cybersecurity Act*], online: <www.congress.gov/bill/118th-congress/senate-bill/1425/text>.

[8] *SPD-5*, *supra* note 6.

[9] Ibid., s 3.

[10] See www.cisa.gov/securebydesign.

[11] *SPD-5*, *supra* note 6, s 4(a).

→ Space systems should be designed to allow operators to “retain or recover positive control of space vehicles” and to “verify the integrity, confidentiality, and availability of critical functions and the missions, services, and data they enable and provide.”[12]

→ Space systems should be designed to include:

- protection that can prevent unauthorized access to critical functions of space vehicles, including the safeguarding of command, control and telemetry links;
- measures to physically protect a space vehicle’s command, control and telemetry receiver systems;
- protection against communications jamming and spoofing;
- protection of ground systems, operational technology and information-processing systems, including from insider threats; and
- intrusion-detection capabilities and methodologies for control systems.

Guidelines for Space Systems Developers and Operators

→ Space systems developers, owners and operators — which SPD-5 refers to collectively as *space operators*[13] — should collaborate to develop best practices.

→ These operators should share information on threats, warnings and incidents.

→ Space operators should incorporate cybersecurity principles into all phases of space systems design, development, acquisition, licensing, deployment and operation across government and industry so as to ensure “full life-cycle cybersecurity.”[14]

→ They should use risk-based, cybersecurity-informed engineering to design and operate space systems.

→ Beyond these recommendations from SPD-5, space operators should manage two-way supply chain risks: both the risk of introducing compromised components to their systems, and the risk of sensitive technologies and information finding their way to unauthorized people and organizations.

Institutional Action

→ The government, in cooperation with industry, should establish a “Centre of Excellence for Aerospace Cybersecurity” to serve as a central coordinating body for cybersecurity for both government and industry aerospace operators, to coordinate the national effort in terms of research, standards, training and response.

Additional Recommendations

In addition to the takeaways from the above documents, regulation or best practices can require all aerospace operators to nominate a cybersecurity officer, known as a CISO or chief information security officer. In addition, introducing a system of space-cyber security rating can provide procurers of space services and insurance companies with a simple tool to ensure they work with safe space operators, and also promote industry-wide adoption of space-cyber security measures.

Furthermore, designers, owners and operators of space systems are of various sizes, from start-ups and small businesses to mega corporations and government departments and agencies, and a one-size-fits-all approach to security would not work. Instead, a risk-informed approach would allow the tailoring of measures to lower-risk projects and access points, thereby allowing meaningful participation by small and medium-size actors as well.

Building Our Own Model

The above recommendations provide a much-needed framework for addressing the space-cyber threats in several dimensions: an umbrella strategy; principles to be followed in the design and build of space systems; and guidelines for their operators. In addition to these substantive responses, the recommendations also provide institutional responses with the establishment of a central coordinating body and nomination of officers in each space actor. Together they ensure

[12] Ibid., s 4(b).

[13] Ibid., s 4(d).

[14] Ibid., s 3.

the creation and dissemination of knowledge on the threats and how to address them. They also designate authority and responsibility for the execution of the required responses.

Whether by pointing to instruments adopted by the United States or Germany or by adopting similar Canadian ones, introducing and implementing a standard of care would boost space-cyber security and provide legal protection to actors who adhere to the standard.

Development of Domestic Capabilities

Encouraging the Training of a Skilled and Diverse Workforce

Addressing space-cyber threats requires a skilled Canadian workforce. While there are many cybersecurity training programs and experts, there are no such training programs specifically for space-cyber security, and very few experts, most of whom are in the United States. The existing cybersecurity training programs in Canada do not address space systems or provide the knowledge and tools required to protect them. Space systems present unique challenges. While established terrestrial cybersecurity standards and methods can be applied to ground stations and operator segments, the space segment presents new challenges, including, first, that satellites operate in extreme conditions and often have basic hardware and software, due to the need for backwards compatibility and limits on energy use. They therefore require highly specialized security architecture. Second, once a satellite is placed in orbit, it is nearly impossible to conduct hardware adjustments, and software adjustments are very limited. It is therefore necessary to introduce training programs that focus on space-cyber security. Third, while the approach to satellites and constellations of satellites in low Earth orbit is shifting toward shorter lifespans and faster replenishment, there are still many satellites with a long lifespan and old systems. Legacy systems are a significant challenge for defence.

In addition, the current cybersecurity workforce, as well as the space workforce, is insufficiently diverse. For example, a study done in the United States by the (ISC)^2 (in full, the International Information System Security Certification Consortium) reports that women represent only 24 percent of the cybersecurity workforce, although the researchers also note that "buoyed by higher levels of education and more certifications than their male counterparts, women cybersecurity workers are asserting themselves in the profession...[and] forging a path to management" ((ISC)^2 2019, 3). Another (ISC)^2 study done in the United States and focused on ethnic and racial minorities found that these minorities represent only 26 percent of the cybersecurity workforce, although their representation is "slightly higher than [in] the overall U.S. minority workforce (21%)" (Reed and Acosta-Rubio 2018, 3). In Canada, women represent 28 percent of the space workforce (Canadian Space Agency [CSA] 2020). Being at the starting point of training the future Canadian space-cyber security workforce provides an opportunity to achieve a diverse workforce by weaving this objective into student recruitment efforts to encourage diverse groups to apply.

At Indiana University Bloomington, the Space Governance Program,[15] together with the Center for Applied Cybersecurity Research, recently launched a new Certificate Program in Space-Cyber Security,[16] in collaboration with US agencies and the private sector, including the Department of Homeland Security, the Aerospace Corporation, the Space Information Sharing and Analysis Center (Space ISAC),[17] Blue Origin and Amazon.[18] The US National Science Foundation recently approved a nearly US$300,000 grant in support of this program. Canada could and should encourage and support the participation of Canadians in this program. Better yet, there is room to explore the introduction of such a program in Canada, possibly in collaboration with US counterparts.

Recruitment efforts for Canadians to participate in such a program could be designed so as to encourage a diverse workforce, including through partnership with local community

[15] See https://ostromworkshop.indiana.edu/research/space-governance/index.html.

[16] See https://kelley.iu.edu/programs/executive-education/programs-for-individuals/digital-badges/cybersecurity-foundations.html.

[17] See https://s-isac.org/.

[18] The author is involved in this effort.

colleges or CÉGEPs (Collèges d'enseignement général et professionnel) and through promotion targeting groups who remain under-represented in the space or cybersecurity fields.

Moreover, the emerging space-cyber security sector will create high-salary jobs. Cybersecurity jobs are among the highest-paying jobs in Canada (Herron and Quan 2022), and average salaries in the space sector are higher than the Canadian average and even those in the information communications technology sectors (CSA 2020). Space-cyber security personnel are expected to be among the top-paying professional positions in Canada.

Even before the pandemic, in 2019, "34% of Canadian space companies faced difficulties hiring personnel to the extent that positions went unfilled" (CSA 2020, 14). When it comes to space-cyber security specialists, the situation is dire. Encouraging the training of a skilled and diverse space-cyber workforce will satisfy the needs of the industry as well as create high-paying jobs and help strengthen, grow and diversify the middle class.

Developing and Acquiring Defensive Capabilities

Defence is not a one-time project but a perpetual race to identify vulnerabilities and defend against their exploitation. The space-cyber nexus represents a new major vulnerability that requires attention and investment.

A variety of defensive technologies and tools should be made available to Canadian actors. The Department of National Defence can acquire such capabilities, and also learn from the experience of the US Space Force, which hired Xage, a Silicon Valley–based company, to develop new cybersecurity architecture for satellites (Barnett 2020). Innovation, Science and Economic Development Canada (ISED), for its part, can encourage Canadian companies to develop defensive space-cyber capabilities, and by that, the creation of a Canadian space-cyber security sector, which, beyond boosting Canada's defence, may provide a growth engine for the economy, as the next section elaborates.

Encouraging a Canadian Space-Cyber Security Sector

The critical nature of space-based infrastructure mandates that Canada will have indigenous defensive capabilities and not be reliant on other countries, just as it maintains defensive capabilities in general. In addition to playing a role in national security, such capabilities will also become an economic growth engine. The recent demonstration of space-cyber threats during the war in Ukraine has ushered in a space-cyber security market, likely to reach hundreds of billions of dollars annually. Globally, spending on cybersecurity for the five-year period from 2021 to 2025 is expected to exceed $1.75 trillion, with 15 percent year-over-year growth (Braue 2021). Indeed, in their recent *Satellite and Space Cybersecurity Markets* report, the space market research and consulting company Northern Sky Research (NSR) predicts exponential growth in the market for cybersecurity of space systems over the next decade (NSR 2022). As the market moves to develop and implement a new wave of security practices and technologies preventing attacks and securing the space and ground segments, new market opportunities arise for providers of products and services to government, military and commercial end-users. According to Cybersecurity Ventures' 2019 cybersecurity market report, Canada is already one of the top four countries in cybersecurity (behind the United States, Israel and the United Kingdom), based on venture capital dollars invested in cybersecurity (Morgan 2019). As such, Canada is poised to become a space-cyber power, with the right support from the government. Such a highly profitable sector would support economic growth and create high-salary jobs.

The National Research Council of Canada and ISED are "working to position Canada as an innovation leader on the global stage" (Champagne 2021, 1) by providing financial support for research and development and various projects. Extending such support to space-cyber security projects could potentially yield higher returns on investment than those from other sectors receiving such government support. For example, the *2020 State of the Canadian Space Sector Report* prepared by the Economic Analysis and Research Team, Policy Branch, at the CSA found that the return on investment from CSA space development programs is 2.5 to 1, meaning that for every dollar invested, 2.5 dollars are returned through follow-on revenues (CSA 2020, 4), and states that its analysis may be conservative in nature (ibid., 27). If one considers the opportunities for additional follow-on revenues after the completion of projects, the actual return on investment may be even higher, and continue growing over time. Canada's various programs, including its Innovation and Skills Plan, can and should be harnessed to encourage training of space-cyber security personnel and investment in research and development in this emerging sector.

Supporting Commercial Companies' Defence from Space-Cyber Threats

Commercial companies are also exposed to space-cyber threats (Heilweil 2021) and have already sustained such attacks, with Viasat being a known, but not the only, example. It is commercial companies that develop, launch and operate satellites and build and operate the ground control infrastructure. Moreover, commercial companies are exposed to space-cyber threats even if they do not themselves operate satellites, as many commercial companies rely on space-based applications. In defending against such threats, the commercial companies need the backup of their states. Such support may include several elements: support for training of personnel; support in acquiring defensive capabilities or otherwise making them available to commercial space operators; and sharing of information on risks, how to defend from them, and how to address incidents of space-cyber attacks.

In order to share such information, Canada needs to establish a Canada chapter of the Space ISAC. A US non-profit specifically endorsed by SPD-5, the Space ISAC facilitates collaboration across the space industry in the exchange of information among its members (businesses and universities working and researching in the space sector) and related government agencies on space-related cybersecurity threats. Establishing a Canada chapter of the Space ISAC, in collaboration with the US Space ISAC, will allow dissemination of information from the US and Canadian sources to all Canadian space actors. A Canada chapter should be a collaboration between the Canadian government and the industry association.

Moreover, and reminiscent of the proposed bill currently in discussion in the US Congress,[19] Canada should establish and maintain a publicly available clearinghouse of resources concerning the cybersecurity of commercial satellite systems, including on vulnerabilities, how to protect against attacks, and responses in the event of an attack. The future Canada chapter of the Space ISAC could be entrusted with this task.

Promoting International Norms

As argued in an earlier policy brief, there is an urgent need to develop an integrated, flexible, multilateral regime on cyber-space governance, and Canada has the capacity — and therefore the responsibility — to lead the way (Tepper 2022, 1).

Canada is a member of the UN-mandated open-ended working group (OEWG) on reducing space threats through norms, rules and principles of responsible behaviours.[20] The issue was raised in the February 2023 session of the OEWG as states expressed concern about harmful effects of non-kinetic interference with space systems, including cyber, that could result in the loss of functionality or permanent damage. Some states suggested a norm proscribing harmful interference to critical space systems or essential services, including by cyber means. However, China objects to discussions of cyber at the space OEWG (there is a separate OEWG dedicated to cyber[21]) (West 2023). Canada can promote such a norm within the working group, but a general norm is essential but not sufficient, and there is a need for further elaboration. Another way to promote the introduction of an international norm, and, significantly, its elaboration, would be to support an initiative by a Canadian university or non-governmental organization to launch an international effort similar to the one initiated and led by the McGill Institute of Air and Space Law that brought together scholars and experts from around the globe to produce the *Manual on International Law Applicable to Military Uses of*

[19] *Satellite Cybersecurity Act, supra* note 7.

[20] See https://meetings.unoda.org/open-ended-working-group-on-reducing-space-threats-2022.

[21] Namely, the OEWG on security of and in the use of information and communications technologies. See https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

Outer Space (MILAMOS).[22] MILAMOS, the product of a diverse group of experts, represents a wide international consensus. Similarly, the Space-Cyber Governance project initiated by Université Laval and supported by CIGI aims to identify the international law applicable to space-cyber warfare and principles representing a broad international consensus. For that purpose, the project "brings together a cohort of scholars, experts, and practitioners from around the world to discuss governance responses to the emerging nexus of space-cyber security."[23] Support for this project, stalled *inter allia* by the geopolitical turmoil, can come in addition to, not instead of, promoting the above norm with the UN-mandated working group.

In advancing international norms of behaviour for the space-cyber nexus, Canada can demonstrate international leadership as well as serve its own interest as an advanced country reliant on space systems.

Conclusions

Canada's space-based infrastructure is vulnerable to cyberattacks of the kind already executed by states and non-state actors. Yet currently there is no policy in place to address this exposure, and commercial space operators have expressed to the author their own concern about the sector's need for more knowledge, skilled personnel and means to protect themselves and their clients, including government/military end-users. Canada is already a cybersecurity power. Building on that positioning, as well as the nation's close relationship with the United States, which has been leading in space-cyber security efforts, provides Canada with the opportunity to adequately defend its space-based infrastructure from space-cyber threats. Moreover, there exists an opportunity to build a profitable sector that would serve as an economic growth engine and provide many thousands of high-paying jobs to a diverse workforce. There are several steps that Canada can — and should — take today. These include launching a national effort on the space-cyber nexus, in terms of capabilities and governance, in cooperation with the industry; introducing national policy and regulations; adopting standards and best practices, modelled on those of the United States and Germany; developing and acquiring defensive capabilities; training a skilled and diverse space-cyber security workforce; encouraging a Canadian space-cyber security sector; and supporting commercial space companies in defence against space-cyber threats. Taken together, these steps may turn a risk into an opportunity, and safeguard Canada's place among the leading space and cyber nations. In addition, Canada should consider promoting or even leading an international effort to introduce norms of behaviour for the space-cyber nexus.

[22] See www.mcgill.ca/milamos/.

[23] See www.chaire-epi.ulaval.ca/en/space-cyber. The author is principal investigator for this project.

Acronyms and Abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik
CÉGEPs	Collèges d'enseignement général et professionnel
CISA	Cybersecurity & Infrastructure Security Agency
CSA	Canadian Space Agency
(ISC)^2	International Information System Security Certification Consortium
ISED	Innovation, Science and Economic Development Canada
NIST	National Institute of Standards and Technology
NSR	Northern Sky Research
OEWG	open-ended working group
Space ISAC	Space Information Sharing and Analysis Center
SPD-5	Space Policy Directive-5: Cybersecurity Principles for Space Systems

Works Cited

Barnett, Jackson. 2020. "Space Force continues work securing space from cyberattacks." FedScoop, September 21. www.fedscoop.com/space-force-cybersecurity-contract-silicon-valley-xage-security/.

Bennet, Jamie. 2023. "House Bipartisan Legislation Proposes to Categorize Space as Critical Infrastructure." ExecutiveGov, August 1. https://executivegov.com/2023/08/house-bill-proposes-to-categorize-space-as-critical-infrastructure/.

Braue, David. 2021. "Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021–2025." *Cybercrime Magazine*, September 10. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/.

BSI. n.d. "Cyber Security for Air and Space Applications." Bonn, Germany: BSI. www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt.html.

———. 2022. "IT baseline protection profile for space infrastructures: minimum protection for the satellite over the entire life cycle." [In German.] Bonn, Germany: BSI, June 30. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html.

Burgess, Matt. 2022. "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine." *Wired*, March 23. www.wired.com/story/viasat-internet-hack-ukraine-russia.

Champagne, François-Philippe. 2021. "2021-22 Departmental Plan." Cat. No. NRI-9E-PDF. Ottawa, ON: National Research Council Canada.

CISA. 2022. "Strengthening Cybersecurity of SATCOM Network Providers and Customers." Cybersecurity advisory, May 10. www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a.

CSA. 2020. *2020 State of the Canadian Space Sector Report: Facts and Figures 2019*. Ottawa, ON: Ministry of Innovation, Science and Industry. www.asc-csa.gc.ca/eng/publications/2020-state-canadian-space-sector-facts-figures-2019.asp.

Heilweil, Rebecca. 2021. "For hackers, space is the final frontier." *Vox*, July 29. www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force.

Herron, Chris and Trevor Quan. 2022. *Cybersecurity Talent Development: Protecting Canada's Digital Economy*. Ottawa, ON: Information and Communications Technology Council. www.digitalthinktankictc.com/reports/cybersecurity-talent-development.

Hollingham, Richard. 2013. "What would happen if all satellites stopped working?" BBC, June 9. www.bbc.com/future/article/20130609-the-day-without-satellites.

(ISC)^2. 2019. *Women in Cybersecurity: Young, Educated and Ready to Take Charge. An Cybersecurity Workforce Report.* Alexandria, VA: (ISC)^2. www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx.

Lightman, Suzanne, Theresa Suloway and Joseph Brule. 2022. *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control.* NIST Interagency/Internal Report 8401. December. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.IR.8401.

Magnuson, Stew. 2014. "U.S. Forces Prepare for a 'Day Without Space.'" *National Defense*, February 1. www.nationaldefensemagazine.org/articles/2014/2/1/2014february-us-forces-prepare-for-a-day-without-space.

Mayorkas, Alejandro N. 2022. "DHS Space Policy." Policy Statement 063-01, Revision 01, April 14. Washington, DC: US Department of Homeland Security.

Morgan, Steve. 2019. "Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017–2021." *Cybercrime Magazine*, June 10. https://cybersecurityventures.com/cybersecurity-market-report/.

NSR. 2022. *Satellite and Space Cybersecurity Markets.* Cambridge, MA: NSR. www.nsr.com/?research=satellite-and-space-cybersecurity-markets.

Ogden, Ben. 2023. "Never a Day Without Space: Spacecom [with Gen. James Dickinson]," May 26, in *A Better Peace*, produced by US Army War College, podcast, 27:50. https://warroom.armywarcollege.edu/podcasts/spacecom/.

Public Safety Canada. 2018. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Cat. No. PS4-239/2018E. Ottawa, ON: Public Safety Canada. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

Reed, Jason and Jonathan Acosta-Rubio. 2018. *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce.* Alexandria, VA: (ISC)^2. www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx.

Tepper, Eytan. 2022. *The First Space-Cyber War and the Need for New Regimes and Policies.* CIGI Policy Brief No. 173. Waterloo, ON: CIGI. www.cigionline.org/publications/the-first-space-cyber-war-and-the-need-for-new-regimes-and-policies/.

Waterman, Shaun. 2021. "Space Force Readies Long-Delayed Cybersecurity Standards for Commercial Satcom Providers." *Air & Space Forces Magazine*, September 9. www.airforcemag.com/space-force-readies-cybersecurity-standards-commercial-satcom-providers/.

West, Jessica. 2023. *The Open-Ended Working Group on Reducing Space Threats. Recap of the Third Session, January 30 to February* 3, 2023. Waterloo, ON: Project Ploughshares. www.ploughshares.ca/reports/the-open-ended-working-group-on-reducing-space-threats-recap-of-the-third-session.

White House. 2020. "Memorandum on Space Policy Directive-5 — Cybersecurity Principles for Space Systems." September 4. https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz

This work was made possible thanks to the financial support of Mitacs.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org