Centre for International
Governance Innovation

Policy Brief No. 173 — May 2022

The First Space-Cyber War and the Need for New Regimes and Policies

Eytan Tepper

Key Points

- A combined space-cyber warfare theatre is emerging to become the primary battlefield in the twenty-first century and the main mode of space warfare.
- Cyberattacks on critical space-based infrastructure may be — and already have been — launched by states, as well as by non-state actors, notably criminal organizations and terrorist groups, and such attacks could even trigger a war.
- The space-cyber nexus is a looming risk for security, economic infrastructure, and many commercial companies and their clients.
- Current multilateral regimes and most national policies do not address the emerging space-cyber nexus in security. There is an urgent need to develop robust national policies and an integrated, flexible, multilateral regime.

Introduction: The Emerging Space-Cyber Nexus

Space-based infrastructure is a critical infrastructure for security and the economy — in fact, it is critical to most aspects of modern life — and therefore is a prime target for malicious attacks (Falco 2019). The most significant current security threat to space-based infrastructure and applications is from cyberattacks. Only a handful of countries have the capabilities to physically destroy satellites (Weeden and Samson 2022) — and they are likely to be exposed as the perpetrators. In contrast, executing a cyberattack requires much less in terms of funds and technological and engineering capabilities. Moreover, the attacker can attempt to cover its tracks, leaving the attacked country uncertain about attribution and its own response. Therefore, cyberattacks are likely to become the leading method of targeting space-based infrastructure for state actors, as well as non-state actors, notably criminal organizations and terrorist groups. There is evidence that such attacks have already occurred: Russia allegedly disrupted Global Positioning System (GPS) signals during North Atlantic Treaty Organization exercises in Finland, Sweden and Norway in 2018 (Harrison et al. 2020), affecting, *inter alia*, the ability of commercial aircrafts to navigate; Turla, a Russian criminal

About the Author

Eytan Tepper is research coordinator and lecturer, space governance, at the Graduate School of International Studies, Laval University. He coordinates the university's research project on space debris, funded by Social Sciences and Humanities Research Council of Canada. He is also leading the Space-Cyber Governance project (www.chaire-epi.ulaval.ca/en/space-cyber), which 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 and aims to identify principles for responsible space-cyber behaviour that will represent a broad international consensus.

Eytan earned his doctorate from the McGill University Faculty of Law, where he was associated with the Institute of Air and Space Law, and subsequently pursued a postdoctoral fellowship at the New York University School of Law. As a lawyer, he provided legal counsel to the Bank of Israel and the Israeli Foreign Trade Administration, including co-authoring the feasibility study on a China-Israel free trade agreement. His work in the private sector included serving as counsel for the largest infrastructure project in Israel, representing Fortune 500 companies, and working on Albert Einstein's estate.

gang, allegedly hijacked satellite IP (Internet Protocol) addresses (Zetter 2015), which it later used to steal data; and Hamas of Gaza, a terrorist organization, hacked the satellite broadcast of a major Israeli television channel (Leyden 2014).

A cyberattack targeting space assets, or *space-cyberattack*, can jam GPS signals, disabling navigation, or spoof GPS signals, providing misleading locations, in both cases disrupting travel and guided weapons systems. A space-cyberattack can "blind" remote sensing satellites that provide satellite imagery and other data collected by various sensors. It can interrupt communication satellites services, including television, radio and internet. Moreover, it can disrupt banking and payment systems, including the use of credit cards and automated banking machines, which rely on satellite-based precise timing. Indeed, important segments of the global financial system depend on GPS (Fernholz 2017). Further, a space-cyberattack can do more than render a satellite defunct: it can turn it into a weapon, for example, by taking control of it and altering its course so that it crashes into another satellite. Indeed, the combined space-cyber warfare theatre will be the primary battlefield for global powers in the twenty-first century (Boucher 2013). Accordingly, a report published by Harvard's Belfer Center for Science and International Affairs suggested that the first mission of the new US Space Force should be to ensure cybersecurity of space assets (Falco 2018). In a signal on the future of warfare, the head of the US Indo-Pacific Command, Admiral John Aquilino, recently noted, "We've come a long way in a short time to be able to integrate the space and cyber domains" (quoted in Sevastopulo 2022).

The First Space-Cyber War

Many dubbed the Gulf War of 1991 the "first space war" due to the US Armed Forces' extensive use of satellites (Anson Bt and Cummings 2008). The current war in Ukraine might be remembered as the first space-cyber war. It is demonstrating the potential and temptation of targeting space assets during an armed conflict. The cyberwar in Ukraine is mostly secret, playing out in the shadows, as inconspicuous as it is insidious.

However, we already know that on the day of the Russian invasion of Ukraine, Viasat, a US-based provider of high-speed satellite broadband services, suffered an outage, which disrupted the internet services it provides to the Ukrainian armed forces, intelligence service and police (Rid 2022). In addition, Russia allegedly jammed GPS signals locally in Ukraine, disabling the ability of Ukrainians to determine their location or navigate and guide weapons to their targets (Hitchens 2022). Moreover, Dmitry Rogozin, the head of the Russian space agency Roscosmos, said that Russia will treat any hacking of its satellites as a *casus beli* (Reuters 2022) — justification for war. This provides a stark demonstration of the explosive potential of the space-cyber nexus: launching a cyberattack on space assets can trigger a response in the form of conventional warfare. This Russian statement may become a new customary norm, as it builds on previous statements and actions regarding cyberattacks in general. In 2011, the United States released its "International Strategy for Cyberspace," which declared it would "respond to hostile acts in cyberspace as it would to any other threat to our country" (The White House 2011, 14). Israel was the first country to take this type of action: in 2019, it attacked a building in Gaza from which Hamas hackers allegedly launched or tried to launch cyberattacks against Israeli targets (Israel Defense Forces 2019).

Commercial space companies have also become embroiled in the war in Ukraine. After Google Maps marked the traffic jam that was the invading Russian army, it turned off live traffic updates in Ukraine that might be used to target troops or refugees (Meaker 2022). Satellite imagery from commercial companies is used to shed light on the unfolding events and situation on the ground, including destruction of targets, as exemplified by Maxar Technologies' satellite images of the 40-mile Russian military convoy en route to Kyiv (Sky News 2022). Moreover, commercial companies' satellite imagery is also used by the Ukrainian army. MDA, a Canadian commercial space company, provides the Ukrainian government with satellite imagery, which the Ukrainian military uses to pinpoint Russian troops (Wark 2022). SpaceX's Starlink announced the provision of space-based internet service in Ukraine (Jin 2022), amid problems faced by traditional suppliers, and, after having its satellite signal jammed (Swinhoe 2022), declared a new focus on cyber defense (Malik 2022). What this war did not yet see, and is less likely to see, is the physical destruction of satellites, although Russia has such capabilities, as revealed again by its anti-satellite test in November 2021 (Gohd 2021), as do the United States, China and India. Indeed, the Ukraine war demonstrates that cyberattacks are the main contra-space mode of warfare.

Separated Multilateral Regimes and Inadequate National Responses

Whereas a combined space-cyber theatre has already emerged and manifested itself, the governance responses remain disjointed at the international level and inadequate at the national level.

At the international level, the United Nations has done work in two separate channels. There have been a series of five UN-mandated Groups of Governmental Experts (GGEs) on cybersecurity and a separate GGE on Transparency and Confidence-Building Measures in Outer Space.[1] The UN-mandated Open-ended Working Group on cybersecurity, or "developments on information and telecommunications in the context of international security," submitted its final report in March 2021, and it does not mention space even once (UN General Assembly 2021). Separately, UN organs are holding multi-year discussions under the agenda items of the prevention of an arms race in outer space[2] and reducing space threats through norms.[3]

In addition, three manuals have resulted from the work of international groups of experts on international law and either cybersecurity or space, but none are yet written on the combined space-cyber theatre. The *Tallinn Manual 2.0* addresses international law applicable to cyberwarfare (Schmitt 2017), and the *Manual on International Law Applicable to Military Uses of Outer Space* (MILAMOS)[4] and the *Woomera Manual on the*

1 See www.un.org/disarmament/topics/outerspace/.

2 Ibid.

3 See www.un.org/disarmament/topics/outerspace-sg-report-outer-space-2021/.

4 See www.mcgill.ca/milamos/.

International Law of Military Space Operations (Woomera)[5] provide guidance on the international law applicable to space warfare. These three manuals follow the tradition of the International Committee of the Red Cross's 1994 *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* and Harvard University's 2009 *Manual on International Law Applicable to Air and Missile Warfare*. They identify the different existing rules of international law that may apply to the respective warfare theatre, found across various international treaties and regimes, and suggest *how* they may apply and what they prescribe in each case. While the manuals do not create new rules and serve mainly as suggested interpretation, the rationale behind them is that, in the absence of a dedicated treaty, legal advisers to defence establishments will use them as first reference and as guides of legitimate practice. The *Tallinn Manual 2.0* includes a section on space law, and the MILAMOS includes a rule on the applicability of cyber law, each from a different perspective.

These separate efforts and manuals on space and cyber warfare, respectively, are, however, only a starting point. There is a need for an integrated approach and focus to develop and then adopt policy through the prism of the space-cyber security nexus that responds to the complexities of the nexus.

Indeed, a series of Chatham House studies found that there is an "escalatory cycle" of militarization of the space-cyber realm that meets inadequate national policies and global governance, and the development of a flexible, multilateral regime is urgently required (Baylon 2014; Livingstone and Lewis 2016; Unal 2019).

To be sure, at the national level, the space-cyber threat has not evaded the attention of some defence establishments and policy makers, but national responses are either incipient or non-existent.

In the United States, for example, in September 2020, then president Donald Trump signed an executive order: "Space Policy Directive–5: Cybersecurity Principles for Space Systems" (SPD–5).[6] This is the first comprehensive government policy related to cybersecurity for space-based assets and operations, and it provides a set of best practices that agencies and companies should follow to protect space systems from hacking and other cyberthreats. However, these practices are not mandatory, and there is no current plan to codify them into binding regulation. The US National Institute of Standards and Technology published a draft document on cybersecurity for commercial space operations, including satellites.[7] The Space Information Sharing and Analysis Center (Space ISAC), specifically endorsed by SPD–5, facilitates collaboration across the global space industry in the exchange of information on space-related cybersecurity threats. The US Space Force, on its part, is working to secure space assets from cyberattacks; it hired Silicon Valley-based company Xage to develop new cybersecurity architecture for satellites (Barnett 2020) and is also working on new satellite cybersecurity standards that will apply to the private sector satellite communication providers working with the military (Waterman 2021).

In January 2022, US senators Gary Peters (Democrat, Michigan), Chairman of the Homeland Security and Governmental Affairs Committee, and John Cornyn (Republican, Texas) introduced bipartisan legislation, a bill titled Satellite Cybersecurity Act[8]; in March 2022, the Cybersecurity & Infrastructure Security Agency, together with the Federal Bureau of Investigation, released an alert on securing communication satellites from cyberattacks.[9] Still, if the United States has only just begun addressing the space-cyber security nexus, many other countries, including key US allies, lag behind.

The Case for an Integrated Approach to the Space-Cyber Domain

Properly addressing the space-cyber security nexus at both the multilateral and the national levels requires an integrated approach and the introduction of international norms and national policies. It further requires supporting

5 See https://law.adelaide.edu.au/woomera/.

6 See www.govinfo.gov/content/pkg/FR-2020-09-10/pdf/2020-20150.pdf.

7 See https://csrc.nist.gov/publications/detail/nistir/8270/draft.

8 See www.congress.gov/bill/117th-congress/senate-bill/3511.

9 See www.cisa.gov/uscert/ncas/alerts/aa22-076a.

commercial companies' defence against space-cyber threats, and the encouragement of a space-cyber security industry that would develop adequate tools and expertise.

A dedicated multilateral regime would provide policy makers and those who execute national policies with a guidebook on what they can — and cannot — do in defensive *and offensive* space-cyber operations. If such a multilateral regime could be established, it would provide a common baseline standard of behaviour. It would allow those state and non-state actors that play within the rules to direct their operations accordingly, and flag and demand accountability from actors that breach the rules.

Admittedly, with the diffusion of power in global politics and multilateralism increasingly being contested, introducing a new regime is not an easy task. UN organs struggle to achieve wide consensus, but once they do, a new, long-term baseline emerges. Given these challenges, other tracks may serve to complement the UN-centred process, notably track two diplomacy,[10] the unofficial, informal interactions by non-state actors. The *Tallinn 2.0*, MILAMOS and Woomera manuals are examples of such tracks, and they complement, rather than replace, the UN work. The eventual introduction of a multilateral regime on space-cyber governance will require work in multiple tracks.

National policies must also address the security threats in the space-cyber realm. The defence establishment should introduce policies and measures to protect its space assets and prepare responses to possible cyberattacks directed at them. Economic ministries and central banks should introduce policies and measures for the protection of critical space-based applications and also guide and support private actors, notably the financial system, in defence against such threats. This work may include introducing industry standards and best practices, as well as providing a forum for exchange of information or creating a national chapter of the Space ISAC. Finally, national policies would benefit from encouraging a domestic space-cyber security industry, as detailed below.

Canada's Role

The role of middle powers in the establishment of multilateral regimes is well known and demonstrated, from examples such as Canada's leadership in the creation of the 1997 Mine Ban Treaty, also known as the "Ottawa Treaty,"[11] to the more recent UK-initiated process for reducing space threats through norms.[12] Canada is probably most associated with the middle-power doctrine. While middle powers wield less influence on the world stage than a superpower does, they make significant contributions to the global order and are believed to better protect the values of that order than the self-interested great powers (Neack 2017). They may be more widely trusted, a factor that facilitates "middle-power diplomacy." According to the "functional principle," a country's contributions to global affairs should match its capabilities (Chapnick 2016, 68). Canada is already an established leader in international aerospace governance and in the study and development of international space law. It hosts international institutions on aviation: the ICAO (International Civil Aviation Organization) and the IATA (International Air Transport Association), the former an international, UN-affiliated organization and the latter an industry association. It also hosts McGill University's Institute of Air and Space Law, the world leader in its field, which led international initiatives including the McGill Declaration on Active Space Debris Removal and On-Orbit Satellite Servicing, the comprehensive Global Space Governance Study[13] and the above-mentioned MILAMOS. Canada has the capacity — and therefore the responsibility — to lead the way on space-cyber governance.

10 See https://peacemaker.un.org/sites/peacemaker.un.org/files/TrackOneandaHalfDiplomacy_Mapendere.pdf.

11 See www.thecanadianencyclopedia.ca/en/article/ottawa-treaty.

12 See www.un.org/disarmament/topics/outerspace-sg-report-outer-space-2021/.

13 See www.mcgill.ca/iasl/gsg.

The Economic Aspect and the Space-Cyber Security Sector

While the emphasis herein leans toward security, the space-cyber nexus is as much about economics. Building a strong space-cyber security infrastructure would promote technological and economic growth across the board. On the one hand, space assets are essential infrastructure for any modern, advanced economy and even a short "outage" may lead to huge damages; on the other, a space-cyber security market has just emerged, and it is likely to reach hundreds of billions of dollars annually.

For comparison, according to *Forbes*, the global cybersecurity market was worth US$173 billion in 2020 and is estimated to grow to US$270 billion by 2026 (Columbus 2020). Based on venture capital dollars invested in cybersecurity, the top four countries are (in this order) the United States, Israel, the United Kingdom and Canada (Morgan 2019), a position that provides these countries with an initial advantage in the new space-cyber security market. Government encouragement of a space-cyber security sector would thus provide support to a highly profitable economic sector, benefiting the economy at large with an important growth engine.

According to Statistics Canada, the Canadian cybersecurity industry contributed more than CDN$2.3 billion in GDP and 22,500 jobs to the Canadian economy in 2018 (Innovation, Science and Economic Development Canada 2022), and the current number should be much higher. Recently, in February 2022, the Canadian government announced that the National Cybersecurity Consortium will be receiving up to CDN$80 million to lead the Cyber Security Innovation Network. The objective of this funding is to foster a strong national cybersecurity ecosystem in Canada and position the country as a global leader in cybersecurity. However, Canada's National Cyber Security Strategy (Public Safety Canada 2019) and its international cyber policy[14] do not address the space-cyber nexus. The promised revamping of the strategy should address issues related to threats to space-based infrastructure and applications. Canada should build on its strong cybersecurity sector to develop a robust space-cyber security industry.

Conclusions

Space-based infrastructure epitomizes both the potential of transformative technologies and their vulnerability to cyberattacks. To harness this potential, and avoid the risks, there is a need for work at the national policy level and in terms of global governance.

It is time to explore and identify principles for responsible space-cyber behaviour that would represent a broad multilateral consensus. Identifying these principles may not prevent space-cyber hostilities, but it could provide "rules of the game," which states could choose to respect or else risk facing consequences — from reputation damage to retaliation by use of force, and everything in between.

States should adopt national policies to defend against threats to space-based assets and applications that are increasingly vital to both national security and economic security. States would also benefit from encouraging a space-cyber security industry that, beyond protecting against space-cyber threats, has the potential to be a significant growth engine.

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

Works Cited

Anson Bt, Sir Peter and Dennis Cummings. 2008. "The First Space War: The Contribution of Satellites to the Gulf War." *The RUSI Journal* 136 (4): 45–53. www.tandfonline.com/doi/abs/10.1080/03071849108445553.

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/.

Baylon, Caroline. 2014. "Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives." Research paper, December. London, UK: The Royal Institute of International Affairs, Chatham House. www.chathamhouse.org/sites/default/files/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf.

Boucher, Marc. 2013. "The Emerging Space Cyberwarfare Theatre." SpaceRef.com, March 19. http://spaceref.com/military-space/the-emerging-space-cyberwarfare-theatre.html.

Chapnick, Adam. 2016. "Principle for Profit: The Functional Principle and the Development of Canadian Foreign Policy, 1943–1947." *Journal of Canadian Studies* 37 (2): 68–85. doi:10.3138/jcs.37.2.68.

Columbus, Louis. 2020. "2020 Roundup of Cybersecurity Forecasts and Market Estimates." *Forbes*, April 5. www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=f09422c381d7.

Falco, Gregory. 2018. "Job One for Space Force: Space Asset Cybersecurity." Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs. www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf.

———. 2019. "Opinion: Our satellites are prime targets for a cyberattack. And things could get worse." *The Washington Post*, May 7. www.washingtonpost.com/opinions/our-satellites-are-prime-targets-for-a-cyberattack-and-things-could-get-worse/2019/05/07/31c85438-7041-11e9-8be0-ca575670e91c_story.html.

Fernholz, Tim. 2017. "The entire global financial system depends on GPS, and it's shockingly vulnerable to attack." *Quartz*, October 22. https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/.

Gohd, Chelsea. 2021. "Russian anti-satellite missile test was the first of its kind." Space.com, November 17. www.space.com/russia-anti-satellite-missile-test-first-of-its-kind.

Harrison, Todd, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way and Makena Young. 2020. *Space Threat Assessment 2020: A Report of the CSIS Aerospace Security Project*. Washington, DC: Center for Strategic and International Studies. www.csis.org/analysis/space-threat-assessment-2020.

Hitchens, Theresa. 2022. "'Local' Russian GPS jamming in Ukraine hasn't affected US support ops, so far." Breaking Defense, March 1. https://breakingdefense.com/2022/03/local-russian-gps-jamming-in-ukraine-hasnt-affected-us-support-ops-so-far/.

Innovation, Science and Economic Development Canada. 2022. "Government of Canada announces next phase to strengthen Cyber Security Innovation Network." News release, February 17. Ottawa, ON: Government of Canada. www.canada.ca/en/innovation-science-economic-development/news/2022/02/government-of-canada-announces-next-phase-to-strengthen-cyber-security-innovation-network.html.

Israel Defense Forces. 2019. "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. Hamas CyberHQ.exe has been removed" (Twitter thread). Twitter, May 5, 11:55 a.m. https://twitter.com/IDF/status/1125066395010699264.

Jin, Hyunjoo. 2022. "Musk says Starlink active in Ukraine as Russian invasion disrupts internet." Reuters, February 26. www.reuters.com/technology/musk-says-starlink-active-ukraine-russian-invasion-disrupts-internet-2022-02-27/.

Leyden, John. 2014. "Hamas hacks Israeli TV sat channel to broadcast pics of Gaza wounded." *The Register*, July 15. www.theregister.com/2014/07/15/hamas_hack_israeli_sat_tv/.

Livingstone, David and Patricia Lewis. 2016. "Space, the Final Frontier for Cybersecurity?" Research paper, September. London, UK: The Royal Institute of International Affairs, Chatham House. www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

Malik, Tariq. 2022. "Elon Musk says SpaceX focusing on cyber defense after Starlink signals jammed near Ukraine conflict areas." Space.com, March 5. www.space.com/elon-musk-spacex-starlink-cyber-defense-ukraine-invasion.

Meaker, Morgan. 2022. "High Above Ukraine, Satellites Get Embroiled in the War." *Wired*, March 4. www.wired.com/story/ukraine-russia-satellites/.

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

Neack, Laura. 2017. "Searching for Middle Powers." *Oxford Research Encyclopedia of Politics*, July 27. https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-330.

Public Safety Canada. 2019. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Ottawa, ON: Public Safety Canada. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

Reuters. 2022. "Russia space agency head says satellite hacking would justify war." Reuters, March 2. www.reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/.

Rid, Thomas. 2022. "Why You Haven't Heard About the Secret Cyberwar in Ukraine." *The New York Times,* March 18. www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html?.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge, UK: Cambridge University Press.

Sevastopulo, Demetri. 2022. "US and Australia boost space and cyber co-operation to counter China." *Financial Times,* March 28. www.ft.com/content/a6efecd9-8f7f-4072-ba86-f405c03bc005.

Sky News. 2022. "Ukraine invasion: 40-mile Russian military convoy nearing Kyiv, satellite pictures show." News.sky.com, March 1. https://news.sky.com/story/ukraine-invasion-40-mile-russian-military-convoy-nearing-kyiv-satellite-pictures-show-12554623/.

Swinhoe, Dan. 2022. "SpaceX's Starlink service facing signal jamming in Ukraine, Musk claims." Data Center Dynamics, March 7. www.datacenterdynamics.com/en/news/spacexs-starlink-service-facing-signal-jamming-in-ukraine-claims-musk/.

The White House. 2011. "International Strategy for Cyberspace." May 16. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

UN General Assembly. 2021. "Final Substantive Report: Open-ended working group on developments in the field of information and telecommunications in the context of international security." A/AC.290/2021/CRP.2. Conference room paper, March 10. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Unal, Beyza. 2019. "Cybersecurity of NATO's Space-based Strategic Assets." Research paper, July. London, UK: The Royal Institute of International Affairs, Chatham House. www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf.

Wark, Wesley. 2022. "Space wars — how Canadian satellite company MDA joined the push against Putin." *Ottawa Citizen,* March 25. https://ottawacitizen.com/opinion/wark-space-wars-how-canadian-satellite-company-mda-joined-the-push-against-putin.

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

Weeden, Brian and Victoria Samson. 2022. *Global Counterspace Capabilities: An Open Source Assessment.* Secure World Foundation. https://swfound.org/media/207350/swf_global_counterspace_capabilities_2022_rev2.pdf.

Zetter, Kim. 2015. "Russian Spy Gang Hijacks Satellite Links to Steal Data." *Wired,* September 9. www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/.

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
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz

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