Responding to the Cybersecurity Challenges of the New Space Environment

Robert Mazzolin, January 2023

This piece was first published by the Centre for International Governance Innovation, copyright 2023.

This essay is part of Cybersecurity and Outer Space, an essay series that explores space governance through three themes: space security and risk, international governance challenges, and global perspectives and the pursuit of inclusivity.

Space-based assets and associated ground-based infrastructure are both increasingly subject to internet-based threats from a variety of sources. These threats need to be dealt with in a comprehensive manner by Western nations using collective technical system design, operational and security policy perspectives. Without such a comprehensive approach, the current vulnerabilities in the space environment could result in serious impacts to critical infrastructure supporting global economic development and international security.

The unprecedented fielding of commercial satellite constellations through various orbits and frequency bands supporting a vast array of commercial and military services in the disciplines of Earth observation, communications, positioning, navigation and timing will increasingly link a new generation of artificial intelligence-driven Internet of Things (IoT) networks residing on cloud-based infrastructure. The emphasis on small, inexpensive and rapidly deployable satellites mirrors the fast-moving, entrepreneurial environment associated with the information technology sector but lacks sufficient focus on security.

The nature of these new satellite networks will clearly accentuate the increasing risks arising from exposure to sophisticated cyberthreats. It is anticipated that the significant shift in dependency from terrestrial networks to the space segment over the next 10 years will generate close to 25,000 satellites launched into space, US$1.2 trillion in commercial retail and more than 500,000 petabytes of data (Northern Sky Research 2022, 3). This development highlights the economic and data security risks associated with the greatly expanded aperture of vulnerability created by the dramatically increased dependency on cyber-based space infrastructure.

China and Russia place heavy emphasis on the exploitation of cyber and space domains to support their economic, geopolitical and military objectives. Other nations such as Iran and North Korea, among 100 other nations active in space but with less capability, could consider the same focus to gain an asymmetric strategic advantage through degradation and destruction of systems. Consequently, the North Atlantic Treaty Organization, in 2019, recognized space as a new operational domain. A number of advanced military nations have established space and cyber commands, reflecting the unique interdependence between the two environments. The intent of such new commands is to enable militaries to respond more effectively to crises and enhance defence and deterrence capabilities in a globally competitive geopolitical environment.
Cyber and space are poised to become the “high ground” of information-age conflict and have witnessed more sophisticated computational attacks against increasingly complex, interconnected systems. The traditional legacy (“old space”) systems that have been historically fielded by governments and large commercial entities to provide long-term, bespoke missions lack sufficient security mechanisms to protect them from these increasingly sophisticated threats. Their growing interconnection to a rapidly expanding IoT infrastructure of billions of devices creates the potential for asymmetric attacks that are globally catastrophic without reaching the threshold of an armed attack. The low cost of such attacks means that many more players such as nation-states, their proxies, terrorists, criminals and hacktivists may take advantage of the many tools and techniques that readily exist and are shared on the open market to impart dangerous effects.

This threat environment dictates a more comprehensive technology and governance policy approach to the application of defensive measures as the increasing sophistication of traditional distributed denial of service attacks, botnet attacks, man-in-the-middle attacks, ransomware attacks and encryption-enhanced advanced persistent threat cyberattacks have outpaced traditional perimeter-based protections. These protections rely upon high-grade link encryptors, intrusion detection and antivirus protection capabilities that protect operational space-based system components in space, ground, user and related links.

The Threat Environment and Its Potential Impact

The increasing use of military space assets, along with dual-use commercial capabilities, largely in low-Earth orbits (LEOs) to support national security interests, increases the prospect of space-based cyberattacks against such assets and raises the potential for traditional conflict to extend to outer space (Harrison, Johnson and Roberts 2018). The disruption of communications, command and control, and satellite imagery for intelligence gathering, communications and geopositioning of strategic assets can serve to counter a nation’s force projection efforts.

“New space” technology developments are taking place in a multidisciplinary, heterogenous environment and leverage the proliferation of inexpensive commercially based LEO satellites. As security is not inherently built in, the proliferated software-defined LEO networks that connect with millions of terrestrially based IoT devices further expand the aperture for attack. The many distinct, mutually interdependent and interconnected applications facilitate access for hostile actors as they enable “backdoor” avenues of egress and the ability to move laterally within the network to manipulate data.

Space shares many commonalities with traditional terrestrial, wireless-based wide-area network, local area network and edge network environments, but they have elements that render them more vulnerable to attack. The wide geographical coverage areas provided by satellites via radio frequency networks that are more difficult to detect and defend against, and the limited ability to repair assets in space, potentially render any damage a catastrophic operational and financial loss. Further, cascading risk is created when an attacker achieves control over a satellite, thus enabling lateral movement not only over the directly connected network but also over the entire interconnected space sector via the various constellations and satellite crosslinks (Fox Business 2021). Finally, the increasingly heterogeneous services offered by commercial providers and the added complexity that requires gateway systems to be deployed at third-party facilities that include teleport and telecom operators, service providers and data centres, further widens the aperture for egress.
Risks could already result from having potentially antagonistic political actors in a common orbital space.

If a satellite could be disabled, the effects might be as widespread as a major internet outage and be particularly devastating for many small countries that have recently launched their own satellites but lack backups. The international nature of the satellite business poses unique risks. Every country, even the smallest, is assigned orbital space for satellites in geostationary orbit, where many traditional communications satellites are located so that they can be permanently positioned to provide coverage to a large and consistent swath of the Earth. As many countries lack satellites, some simply sell or rent their space to others. Given the low level of transparency regarding on-orbit capabilities and the challenges of space situational awareness in geostationary orbit, this means that risks could already result from having potentially antagonistic political actors in a common orbital space. This potential for conflict becomes particularly concerning in parts of the globe that have been underserviced by terrestrial networks and where emerging superpowers are seeking to gain strategic geopolitical advantage.

While counterspace cyberattacks require a high degree of understanding of the space assets being targeted, they do not necessarily require significant resources to conduct. Numerous types of non-kinetic attacks can be conducted from Earth, including electronic warfare techniques such as jamming, spoofing and hacking networks to target control systems and mission packages; targeting ground infrastructure such as satellite control centres with cyberattacks; and maximizing system vulnerabilities through individual vendors within the operations and supply chains that provide egress to a larger corporation’s network. These actions can be contracted out to private groups or individuals, which enables state or non-state actors that lack internal cyber capabilities to pose a cyberthreat.

Cyber remains the principal means of attacking space capabilities, largely due to the broad aperture of exposure to internet-facing infrastructure, which makes it a much easier target for offensive techniques that have already been developed in the terrestrial environment. Historically, space-based networks have been “air gapped” from terrestrial networks and employed bespoke protocols, affording some protection. The increasing reliance on commercial IP technologies and wide variety of commercial service providers to support mission systems creates a far easier target. The culture of security associated with private sector ownership and control of physical assets must evolve.

Mitigation through Technology Enhancement

The way forward requires a dual-track cultural evolution in both technological and governance enhancements. From a technology perspective, a revised approach to security is required for the space sector that involves developing a new array of solutions and best practices to replace traditional static approaches. An emerging area of cybersecurity “best practice” development specifically directed at the unique nature of space networks is taking form. This process includes tailoring US National Institute of Standards and Technology risk frameworks, US Space Force Infrastructure Asset Pre-Assessment commercial satellite communication security evaluation, European Space Agency cybersecurity program enhancements and specific policies being developed by some space-faring nations. However, such initial policy development still aligns with the traditional “ownership implies control and security” paradigm.

A new approach is needed, which would combine advanced risk assessment and automated defensive tools along with traditional security information and event management techniques uniquely designed for space systems. The objectives would be to increase the complexity and cost for attackers and enhance system resiliency. Cybersecurity assessments are a useful exercise for any satellite communications provider as current federal and industry cybersecurity regulations will eventually extend into space, requiring providers to develop audit plans for compliance. Further, security support
throughout the life-cycle management of any space system should be enhanced. The potential of quantum satellites presents interesting possibilities given their theoretical resiliency.

Mitigation through Improved Governance

As the space environment is transitioning from the preserve of select wealthy states into one where market forces dominate, capabilities possessed a few years ago only by government security agencies are now in the commercial domain. The current international legal regime is ill-equipped to prevent the weaponization of these environments, and mutual distrust among nations and the unpredictability of non-state actors are thwarting efforts in this direction. As space assets are intrinsically tied to cyber capabilities that support the most sensitive and valuable activities of a nation, the interests of national security inherently limit information sharing, transparency and application of binding mechanisms. The current 1967 Outer Space Treaty, UN Charter, International Telecommunication Union regulations and export controls are weak as they do not adequately protect against potentially lethal effects. The overall effects of these separate and limited protocols amount to nominal cooperation and a loosely governed environment.

Addressing competition in the space economy and securing national security interests are best achieved using strategies that combine and leverage the roles of government, industry and academia to include a tailored space and cyber industrial policy.

Beyond national strategies, the development of a flexible, multilateral space and cybersecurity regime is urgently required. International collaboration among leading space-faring nations sharing congruent interests and common values should be initiated to enhance the development of cooperative frameworks in the key areas comprising capability and technology development, sustenance of operations and enhancement of collective security capabilities, and highlight the global implications of destabilizing incidents in the space and cyber domains. Given the current mutual mistrust between major space players such as China, Russia and the United States, a positive approach to “kick-start” the identification of initial areas of collaboration would be to select key areas of mutual security interests such as debris removal, climate protection and defending the Earth from potentially harmful objects such as asteroids.

International cooperation will be crucial. So, too, will be a moderately regulated approach involving governments and industry to guide the development of industry-led standards, particularly in the areas of collaboration, risk assessment, knowledge exchange and innovation. The creation of such a regime comprised of a limited number of able states and other critical stakeholders, such as those in the space supply chain and insurance industries, could foster relationships between key members of the space-cyber community, and provide a vehicle for practical leadership in delivering enhanced security within the entire global space sector. Although these collaborations are critical to the innovation and tools associated with the development of space capabilities, care should be afforded to preventing profit-driven considerations from usurping nation-state authorities. Further, overdependency on individual space assets such as GPS and Galileo should also be considered by nations and diverse services identified.

Conclusion

Cybersecurity and space security are intrinsically interlinked, and both are crucial to the advancement of contemporary statecraft. The rapidly evolving technology base that integrates these unique environments, along with the increasing dependence of critical infrastructure, societal resiliency and, ultimately, government legitimacy, require a cultural change in the way innovative technical and policy solutions are developed to ensure global security. Work at both the international and national governance levels is needed. There is an important role to be played by the commercial space industry in developing new security standards and protocols.

Works Cited


The opinions expressed in this article/multimedia are those of the author(s) and do not necessarily reflect the views of CIGI or its Board of Directors.

ABOUT THE AUTHOR

Robert Mazzolin

BGen (Retired) Robert Mazzolin is a CIGI senior fellow and serves as the chief Defence, Security and Technology strategist at RHEA Group.