2018

Cybersecurity and the New Era of Space Activities

David P. Fidler
Indiana University Maurer School of Law, dfidler@indiana.edu

from Digital and Cyberspace Policy Program

Cybersecurity and the New Era of Space Activities

A Tesla Roadster automobile floats through space after it was carried there by SpaceX's Falcon Heavy. SpaceX handout/Reuters

Governments, critical infrastructure, and economies rely on space-dependent services—for example, the Global Positioning System (GPS)—that are vulnerable to hostile cyber operations. However, few space-faring states and companies have paid any attention to the cybersecurity of satellites in outer space, creating a number of risks.

Report *by* David P. Fidler

April 02, 2018

Facebook Twitter LinkedIn Email Print PDF

Up

Introduction

The tasks of securing outer space and cyberspace are converging. The internet increasingly depends on space-enabled communication and information services. Likewise, the operation of satellites and other space assets relies on internet-based networks, which makes these assets, like cars and medical equipment, devices on the internet of things. New government actors, companies, goals, and technologies are expanding and transforming space activities. However, neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, which could increase national security risks.

To meet these challenges, government, industry, and international action is needed. The Donald J. Trump administration's National Space Council should develop cybersecurity recommendations for space activities, and federal agencies should prioritize these within the government and in cooperation with the private sector. In crafting needed legislation for commercial space activities, Congress should bolster industry efforts to strengthen cybersecurity. Private-sector actors should strengthen their adoption of cybersecurity best practices and collaborate with one another on improving implementation of cybersecurity strategies. Internationally, the United States should pursue collaboration on space cybersecurity through the North Atlantic Treaty Organization (NATO), plurilateral space cooperation mechanisms, and bilateral forums.

Cybersecurity Comes to the Final Frontier

Outer space has been a national security priority for spacefaring nations since the 1950s. Governments started space programs for intelligence, military, political, and scientific purposes and developed countermeasures against space-based threats from rivals, such as anti-satellite capabilities. Countries managed security competition by banning weapons of mass destruction in space and cooperating on peaceful uses of space. Government programs catalyzed private-sector adaptation of dual-use technologies to provide satellite communication services.

Despite the importance of satellites, the U.S. General Accounting Office concluded [PDF] in 2002 that efforts on critical infrastructure protection did not include the satellite industry, but should do so. Similarly, cybersecurity has not been a priority in government and private-sector space endeavors. One leading analysis [PDF] asserted that cybersecurity discussions often overlook space activities' vulnerability to cyberattack. For example, neither the UN governmental group of experts (GGE) on outer space nor the UN GGE on cyberspace addressed the convergence of their respective agendas.

Governments, critical infrastructure, and economies rely on space-dependent services—for example, the Global Positioning System (GPS)—that are vulnerable to hostile cyber operations. Geopolitical competition fuels the militarization of space, which heightens state incentives to devise cyber espionage, interference, and attack strategies against rivals' space operations. The United States suspects that China has engaged in cyber operations against U.S. satellites. Chinese military writings emphasize [PDF] the need to target satellites to "blind and deafen the enemy." The then commander of Air Force Space Command, General John E. Hyten, told Congress in 2016 that "adversaries are developing . . . cyber tools to deny, degrade, and destroy" [PDF] U.S. space capabilities that support war fighting, critical infrastructure, and economic activity. Other countries likely believe the United States is preparing to conduct cyber espionage, disruption, and attack operations against the space assets of rival states.

> "Cybersecurity has not been a priority in government and private-sector space endeavors."

The commercialization of space heightens cybersecurity concerns for many reasons, including market incentives to lower costs and innovate quickly, often at the expense of software and hardware security. Entrepreneurial activities—dubbed the New Space sector—are underway in

space transport, space tourism, asteroid mining, lunar operations, and missions to Mars. A small-satellite ("smallsat") revolution involving spacecraft far smaller than traditional satellites is unfolding. Networks of linked smallsats can provide internet access, communications, data storage and transmission, imaging, and remote sensing. This next generation of satellites harnesses innovations in computing, electronics, miniaturization, imaging, sensors, big data, and artificial intelligence. Satellite services for Earth observations from space are growing. They support many policy and commercial purposes and contribute to agricultural productivity, transportation efficiency, and environmental monitoring. Commercial space activities use cutting-edge technologies and produce valuable data and are, thus, targets for cyber espionage, including economic cyber espionage, and cybercrime.

Challenges

Space agencies, the satellite industry, cybersecurity researchers, nongovernmental bodies, and intergovernmental satellite organizations show increasing awareness of the space cybersecurity challenge. Nevertheless, experts are worried. NASA's then chief information security officer, Jeanette Hanna-Ruiz, warned that "it's a matter of time before someone hacks into something in space." Chatham House's David Livingstone asserted that "people are just shuffling . . . paper around" and suggested that only "a disaster" might catalyze serious action. Josh Hartman, a former senior Pentagon official and Air Force officer, argued before the satellite industry's first cybersecurity summit held in 2017 that, on cybersecurity, "most of the space community . . . has their heads in the sand." The "attack surface" of space activities is expanding, but governments and industry are not taking adequate action.

More on:

Space **Cybersecurity** **Digital Policy** **Technology and Innovation**

Protecting space activities requires understanding the particular cyber vulnerabilities that arise in various space operations. For example, satellite cybersecurity encompasses the satellite itself,

transmissions to and from Earth, and ground stations. U.S. military and intelligence satellite systems are vulnerable to kinetic and cyberattacks. Civilian smallsat systems might also prove insecure, given the lack of cybersecurity in their design, their use of commercial off-the-shelf components, and the vulnerabilities potentially created by connecting satellites to operate as complex, orbiting networks.

Neither international law nor diplomacy has grappled effectively with space cybersecurity. Multiple bodies of international law are relevant, but controversies about whether and how international law applies to cyberspace have adversely affected cyber diplomacy. Such travails have elevated the prominence of nongovernmental efforts to clarify international law's application in cyberspace, such as the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. However, states continue to conduct cyber operations that violate international law. For example, the UN International Telecommunication Union prohibits interference with satellite transmissions, yet such interference frequently occurs.

> "The United States has declared that space is now a 'war-fighting domain.'"

The militarization of space potentially threatens the requirement in the Outer Space Treaty (OST) that space activities comply with international law to maintain international peace and security and promote international cooperation. The United States has declared that space is now a "war-fighting domain," and China's and Russia's military ambitions in space are growing. The UN Committee on Disarmament's work on a treaty to prevent an arms race in space failed. As happened with cyberspace, these difficulties in space diplomacy have increased nongovernmental interest in clarifying how international law applies to military operations in space.

The commercialization of space fuels concerns that the private sector will unduly influence how states interpret the OST's duty to authorize and supervise nongovernmental space activities. The debate over whether U.S. support for commercial space activities violates this OST requirement might also create diplomatic problems.

New diplomatic initiatives on space cybersecurity would encounter headwinds. Putting "space" before "cybersecurity" does not alleviate the geopolitical tensions that already limit cooperation on cyberspace and space. The United States, China, and Russia have not agreed on how to approach cybersecurity or address military activities in space. Recent diplomatic activities on space and cybersecurity concluded without addressing space cybersecurity, including the UN GGEs on cyberspace and outer space and the European Union's code of conduct for space activities [PDF]. Negotiations in the UN Committee on Peaceful Uses of Outer Space on guidelines for the long-term sustainability of space activities considered but did not adopt proposed guidelines [PDF] on information-security policies for the terrestrial and orbital parts of space systems. Controversies and disagreements during these efforts suggest that reopening them for space cybersecurity would not be effective. Further, the increased number of spacefaring nations, which now includes such countries as South Korea and the United Arab Emirates, complicates diplomacy by requiring more countries to reach consensus.

States might also believe more diplomatic activity is not necessary because they already have sufficient incentives to refrain from dangerous cyber operations in space. Disabling a satellite through cyber means could turn it into space debris—already a major problem—that threatens space activities for all countries. The importance of intelligence satellites in maintaining nuclear deterrence also encourages restraint in interfering with the satellites of rival nuclear powers. Following trends on Earth, countries might want to avoid diplomatic activity in order to engage in cyber operations in space that "subvert the integrity of political, social, and economic systems, rather than destroy physical infrastructure" by, for example, manipulating or hijacking an adversary's space infrastructure to spread propaganda and misinformation.

Recommendations

Government

The United States can provide leadership on cybersecurity in outer space through a comprehensive strategy. The Trump administration is positioned to advance space cybersecurity because its priorities include improving critical infrastructure cybersecurity, addressing security threats to space operations [PDF], and promoting commercial space activities. The administration resurrected the National Space Council and should task it with developing recommendations on strengthening the cybersecurity of space infrastructure. To do so, the council should convene government officials and leaders from the commercial space sector to share insights on managing cybersecurity as space and cyberspace merge. These leaders should include people who have led both information technology and space enterprises, such as Paul Allen (Stratolaunch Systems), Jeff Bezos (Blue Origin), and Elon Musk (SpaceX). The Trump administration should instruct the Department of Commerce, Department of Homeland Security, Federal Aviation Administration, Federal Communications Commission, and NASA to make cybersecurity a priority in their space collaborations with the private sector.

With private-sector space activities expanding, Congress should adopt a comprehensive regulatory framework for the commercial space sector. Current law does not regulate the full range of space activities the private sector is planning, a problem recognized [PDF] but not addressed during the Barack Obama administration. A comprehensive framework would provide commercial space enterprises with regulatory certainty and help the United States comply with its OST obligation to authorize and

“Congress should adopt a comprehensive regulatory framework for the commercial space sector.”

supervise nongovernmental space activities. The legislation should emphasize the importance of existing federal law on cybersecurity information sharing, provide government assistance to industry-led efforts to strengthen space cybersecurity (especially concerning threats from state actors), and—as happened in other sectors, such as energy—facilitate public-private collaborations on cybersecurity.

Industry

Improving space cybersecurity requires extending good cybersecurity practices into the commercial space sector and addressing problems specific to space activities. Advice for this sector repeats familiar mantras, such as the need for intra-sector collaboration, information sharing, enterprise risk management, encryption, insider threat prevention, and supply chain protection. The federal government has, for example, rightly stressed [PDF] the utility of the Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity [PDF] for satellite companies.

Industry associations in space sectors should move from identifying general principles and recommendations, such as those in the Joint Statement on the Satellite Industry's Commitment to Cybersecurity, to supporting implementation activities. The Satellite Industry Association could, for example, include in its annual State of the Satellite Industry Report [PDF] information on the industry's cybersecurity activities, as is done in other industries.

International

The difficulty of reaching multilateral agreement on cybersecurity and space issues means the United States should address space cybersecurity in plurilateral and bilateral contexts. The United States should raise space cybersecurity within NATO, given the alliance's plans to upgrade its satellite and cyber defense capabilities. U.S. bilateral cybersecurity cooperation with spacefaring countries, such as India and Japan, should include space cybersecurity. With their history of collaboration, NASA and the European Space Agency, which is increasingly aware of

cybersecurity threats to its programs, should sign a memorandum of understanding to cooperate on space cybersecurity.

More ambitiously, the United States should use effective mechanisms of space diplomacy to improve space cybersecurity. For example, the International Space Station (ISS) has involved the United States, Canada, Japan, Russia, and the European Space Agency managing the "the most politically complex space exploration program ever undertaken." The United States should discuss the need for more cooperation on space cybersecurity within the ISS framework. In addition, the United States could lead establishment of an intergovernmental coordination mechanism for developing guidance on space cybersecurity. The mechanism could be modeled on the Inter-Agency Space Debris Coordination Committee (IADC), composed of space agencies from leading spacefaring countries. The IADC's nonbinding guidelines are credited with reducing space debris produced by new launches.

Conclusion

Actions at the national, industry, and international levels can harness growing awareness about space cybersecurity and strengthen policy and industry practices as the convergence of space and cyberspace accelerates. Outer space might not be the "final frontier for cybersecurity," but achieving cybersecurity beyond Earth is one of the many responsibilities the new era of space activities creates for governments and societies.

This Cyber Brief is part of the Digital and Cyberspace Policy program. ***The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.***

Explore More on Space

New Cyber Brief: Cybersecurity and the New Era of Space Activities

by Adam Segal

April 2, 2018

Who Owns Space? Commercial Activity Beyond…

with Joanne I. Gabrynowicz , Lori Garver *and* Bob Richards

November 30, 2017

The Outer Space Treaty's Midlife Funk

by Guest Blogger for Stewart M. Patrick

October 10, 2017

Explore More on CFR

Cybersecurity and the New Era of

Space Activities

by David P. Fidler

April 2, 2018

Time to Tighten the Screws on Cuba?

by Elliott Abrams

April 2, 2018

The End of Antibiotics?

by Claire Felter

March 29, 2018