Cyber security and space security

What are the challenges at the junction of cybersecurity and space security?

by Nayef Al-Rodhan
Tuesday, May 26, 2020
Comments (1)

In 2014, the network of the National Oceanic and Atmospheric Administration (NOAA) was hacked by China. This event disrupted weather information and impacted stakeholders worldwide. Satellites are often highly vulnerable to cybersecurity breaches as some telemetry links are not even encrypted.

Space is a critical asset for the modern state and the challenges it faces. This dependency relies on the critical interaction of cybersecurity and space security.

Cybersecurity is defined by the International Telecommunication Unionas "the collection of tools, policies, security concepts... risk management approaches... and technologies that can be used to protect the cyber environment and organization." Space security can be understood similarly, but instead towards the protection of outer space and assets there. This article aims at understanding the links between these two notions and the challenges at their junction.

Two intertwined domains

My theory of meta-geopolitics outlines seven interrelated dimensions of state power (social and health issues, domestic politics, economics, environment, science and human potential, military and security issues, international diplomacy) that constitute the new paradigm of statecraft. The book *Meta-Geopolitics of Outer Space explains* how these seven dimensions are present in outer space. In the social and health sector for instance, satellites are crucial to monitor diseases or even guide remote medication delivery systems. In the case of the COVID-19 outbreak in China, it appeared that disease monitoring and large scale disinfection by unmanned aerial vehicles, guided by 28 BeiDou Phase III navigation satellites, were crucial to mitigate the spread.

Space is thus a critical asset for the modern state and the challenges it faces. This dependency relies on the critical interaction of cybersecurity and space security. Indeed, several data flows can be identified between the Earth and space-based assets. First, information is sent from Earth to satellites and other

space-based assets (Earth-space interactions.) Second, information is sent back to Earth from satellites and other space-based assets (space-Earth interactions.) These flows are critical and vulnerable to threats. The security of space-based infrastructure depends on the safety of Earth-space interactions, and the security of systems relying on data from space depends on the safety of space-Earth interactions. For example, false information could be given by Earth-based attackers to a satellite to force it to collide with another.

New dynamics in outer space have increased the level of vulnerability of cyberspace and space-based infrastructures. Indeed, space used to be reserved to major powers as the expertise and technologies required were scarce. However, innovations such as cubesats and the privatization of outer space made access to space easier and cheaper. New states and individuals have access to this domain and multiply the presence in the LEO, and thus the risk of malicious interactions. Moreover, growing space militarization may increase the risks of confrontation and thus the numbers of attacks.

On Earth, the increased number of self-trained or state-supported hackers, as well as the cheap access to computer technologies, also increases the risk of disruption to Earth-space and space-Earth interactions. These attacks are particularly hard to trace and thus complicate the attributions of responsibilities.

New dynamics in outer space have increased the level of vulnerability of cyberspace and space-based infrastructures.

Threats at the junction of space and cyber security can be placed in five categories: kinetic physical, non-kinetic physical, electronic, cyber, and Earth-based. Kinetic physical threats include direct strikes against space infrastructure, either through another satellite or a weapon such as anti-satellite systems (ASATs.) Non-kinetic physical threats damage space assets through effects from a distance, such as electromagnetic pulses (EMP). Hackers could take control of such systems to launch attacks. With the rise in innovative processes, electronic and cyber threats are however more widely used. Electronic threats include actions undertaken to damage the transmission and reception of data (jamming) or even the transmission of false data (spoofing.) Cyberattacks in this domain mostly deal with the direct injection of false data or the unauthorized monitoring of traffic or activities in outer space. Finally, Earth-based threats include the malicious acts within the supply chains of these systems or against the physical infrastructures used for transmission or storage of data. To be mitigated, all these potential threats

require international cooperation, a process that for the time being seems quite stuck.

National capabilities

The United States' space operations are advanced but vulnerable. Additionally, the United States itself has the capabilities to conduct kinetic physical, kinetic non-physical, electronic, and cyber attacks. It is, however, hard to precisely measure the capability of the United States as most information in this domain is classified. The activities of the Space Force, for example, are not actively shared. In terms of cyberattacks capacity we can however note that the National Security Agency has recently declared its willingness to use cubesats for better intelligence collection and vulnerabilities assessments. It thus appears that the United States has significant resources but keeps communication on this matter low key.

Russia possesses different space assets, notably the GLONASS navigation system. These systems give it great capability but also vulnerabilities. In terms of kinetic physical threats, Russia developed ASAT missiles and conducted a test in 2018. With regards to kinetic non-physical threats, Russia developed many laser-based systems and reportedly used one in 2011 against a Japanese satellite. It also appears that Russia has the capacity to interfere with GPS signals, most recently in the Arctic.

China is also an important space power with demonstrated anti-satellite capabilities. It can use several laser-systems and has the capacity to detonate a nuclear-powered weapon which could damage satellites from distance. It also has electronic warfare capacity; one example is an ionospheric radar developed in the island of Hainan and able to influence particles up to 2,000 kilometers. Finally, the cyberattacks capabilities of the Chinese government appear high. They seemed to have been used in several instances and with additional hackers' participation such as during the 2014 National Oceanographic and Atmospheric Administration hack.

Iran and North Korea also have increasing space capabilities, but a low space presence compared to big powers. Indeed, Iran put its first nationally produced satellite (Safir-1) in 2009, while North Korea appeared to have launched one satellite in 2016. As it will be mentioned in the next section, though, Iran and North Korea are developing increasingly strong electronic and cyber capabilities.

Recent space cybersecurity incidents

There has not been any recent kinetic physical attack in outer space. It is, however, important to note that several nations already developed the ability to attack satellites through ASATs, and similarly plan for the possible hijacking of space systems. For example, the United States Air Force has developed a partnership with researchers at the Defcon hacking conference in order to test satellites' vulnerabilities. Non-kinetic physical attacks can cause severe damage with limited debris. In 2018, the Center for International and Strategic Studies reported that the Russian government developed a laser-based system (1LK222 Sokol Eshleon) that can "dazzle and blind sensors on satellites." This tool can damage a satellite severely and potentially prevent.

Electronic warfare is more widely used than physical attacks in outer space, with numerous examples in recent years. Finland's civilian air navigation systems were interrupted by an electronic attack during a NATO exercise in 2018. It was claimed that Russia was behind this jamming operation. In 2009, Iran was accused of jamming BBC's signal in its territory in order to disrupt broadcasting during popular movements. Similarly, in 2010, North Korea was blamed for GPS signal jamming in South Korea.

Cyberattacks in outer space are also more common that physical attacks. An example is the NOAA satellite hacking incident mentioned at the opening of this article. While it was claimed that Chinese hackers were behind the hack, identifying a government is complex in the context of cyberattacks.

These attacks increase tensions and create a lack of trust between international players. They compromise the need for a global concorde on these challenges.

Perspectives on cooperation

Human nature is emotional, amoral, and egoistic. The human being is a predisposed *tabula rasa* with no initial notions of right and wrongs but only minimally equipped with a survival instinct. This theory is applicable to states as they often function through the prism of survival with some pre-existing but limited influences of moral thoughts in their endeavors., mostly because their socialization process does not push for the adoption of moral principles as most socialization processes at the community level entail. The result of these dynamics, with regards to cyber security and space security, is a very low level of cooperation.

Indeed, as space assets are bound to the most sensitive and precious activities of the state, the logic of survival is paramount. It implies a reluctance to share information, limited transparency and a lack of binding mechanisms. At the international level, the current framework is weak. Indeed, the Outer Space Treaty of 1967 prohibits "harmful interference" but does not explicitly ban lethal systems other than weapons of mass destruction (WMD.) ASATs, and hacking of space systems, is thus not explicitly forbidden. Similarly, the word "peaceful" brings a doubt on the nature of permissible activities: if aggressive activities are prohibited, what about defensive ones?

The junction of cybersecurity and space security should be taken seriously and certainly requires specific international assessments.

The United Nations Charter is also part of the current framework. It urges states to use restraint in the use of force and acknowledge a right to self-defense. However, cyberattacks may be hard to trace and thus claiming a right of self-defense based on an initial act of aggression can be tricky. ITU regulations and export controls mechanisms can help in managing the launch of satellites and management of space traffic, yet military satellites are often not registered. The overall result of this conglomerate of instruments is a loose environment where cooperation is limited.

Policy recommendations

I previously advanced a theory of international relations called symbiotic realism, which holds that despite the inherent anarchy of the state system, states are bound to cooperate as they share cultures and challenges. In space, it takes on a whole new dimension as states also rely on each other for information, launch, missions, and experiments. Despite the current tensions, space qualifies as a global common in which appropriation is forbidden. Moreover, security, including space security, cannot be understood as a zero-sum game but rather as a multi-sum game where good governance ensures justice for all individuals, states and cultures, without gains at the expense of the other. Indeed, if space is unsafe for one, it will be unsafe for all.

As an example, potential debris created by kinetic physical attacks could endanger assets belonging to many states and companies. The cybersecurity of space assets is thus a collective problem. Space should thus be understood as a collective domain where no conventional actor has an interest in militarization and lack of trust. Additionally, overall Earth security is dependent on space security. As mentioned earlier, dynamics in space are impacted by, and influence, the seven dimensions of statecraft discussed earlier. Earth-space

and space-Earth interactions are crucial for the functioning of numerous terrestrial assets. By devoting efforts to space security, governments invest in safer and more performing health systems, domestic and international politics, economy, environment, and innovation.

It is thus crucial for states to consider increased efforts and coordination. The following recommendations notably concern cooperation, space-assets security, privatization and dependency.

1. Multiply efforts for cooperation

Despite current limited results most recently illustrated by the inability of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space (GGE PAROS) to produce a final report, cooperation should remain a priority. The junction of cybersecurity and space security should be taken seriously and certainly requires specific international assessments. Possible steps include the creation of a new group of governmental experts to provide guidance on this topic as well as the production of more working papers to build upon during international fora such as the Conference on Disarmament. Transparency and confidence-building measures (TCBMs) or Codes of Conduct could be an alternative to a binding treaty but should not become the practical illustration of a lack of will or a weakening of institutions' power in regulating outer space practices.

2. Increase the level of space cybersecurity

In the meantime, actions should be taken to reduce the vulnerability of Earth-space and space-Earth interactions. One possible, if long-term, solution is the use of quantum encryption that is currently being studied by several nations. The expertise and techniques required might be an obstacle to a largeOscale diffusion of quantum encryption but could at least help mitigate the risk for those with access to such systems. States with less capacities could start by an assessment of vulnerabilities and first-level corrections. National actors could also ensure that private companies launching space assets obey tough security rules in supply chains and network safety.

3. Reduce the influence of private actors

Another critical action to take is to reduce or at least reflect on the influence of private actors in the space domain. At the junction of cyber and space security, they are critical in providing innovation, tools, and support. However, their influence should never go beyond the authority of the state as to ensure a lack

of profit-based policy decisions. This goes notably through the implementation of parliamentary auditing in space activities and cyber space activities. International institutions such as the United Nations Office for Outer Space Activities (UNOOSA) could also have an impartial mediating role in these dynamics.

4. Reflect on the overreliance on space assets and possible alternatives

Finally, states should conduct a reflection on their overreliance on space-based assets and Earth-space/space-Earth interactions. They should think about the ways in which their needs could be met with the same quality but within a diverse portfolio of techniques. At the more technical level, it is also relevant to diversify data intakes. As an example, NATO overreliance on the GPS system for navigation was pointed out and the use of the European Galileo was proposed to ensure better resilience in case of failure. For the time being this policy has not been implemented.

5. Think through scenarios

An important aspect of space assets security concern our common ability to think in advance and plan in advance with a risk-focus mindset. The best way to deliver on this aspect is to conduct scenario-making exercises. Based on the different types of threats outlined, policymakers should outline the relevant actors to mobilize, the different stages of response and tasks to achieve. Below, I provide examples of scenarios for mitigating kinetic physical threats and jamming threats.

Cybersecurity and space security are two interlinked domains. Space assets are crucial for modern statecraft but face serious vulnerabilities. The range of threats at the junction of these two domains as well as the current lack of cooperation requires immediate actions. It remains in the hand of states to unlock the potential of international fora at their disposal and avoid serious incidents.

■

Prof. Nayef Al-Rodhan (@SustainHistory) is a neuroscientist, philosopher, and geostrategist. He is an Honorary Fellow at St Antony's College, University of Oxford, and Senior Fellow and Head of the Geopolitics and Global Futures Programme at the Geneva Centre for Security Policy, Geneva, Switzerland. Through many innovative books and articles, he has made significant conceptual contributions to contemporary geopolitics, outer space

security, international relations, future studies, and war and peace, as well as the application of the field of neurophilosophy to policy and global security. He is the author of Meta-Geopolitics of Outer Space. An Analysis of Space Power, Security and Governance (Basingstoke: Palgrave Macmillan, 2012).