SHUTTERSTOCK/ZMITER

The critical interplay between cybersecurity and outer-space security

BY NAYEF AL-RODHAN

Outer space has become a critical asset for the modern state. Satellites in outer space are crucial for life on earth: We are dependent on satellites to support everything from vital supply chains, emergency communications and military operations to weather forecasting, financial markets, navigation and electrical power grids. But as technology advances, space activities are increasingly exposed to potential vulnerabilities and security risks on earth and in space, especially when drawn into geopolitical disputes. The war in Ukraine is a timely reminder that attacks targeting space systems can rattle the foundations of political and economic life as well as the sustainability of a peaceful global order. This begs the question: How safe are our satellites and space assets? And how do we protect critical infrastructure and society at large from vulnerabilities on the cusp of cyber and space security?

Space and terrestrial systems, traditionally isolated from one another, are becoming ever more interdependent. This is perhaps most evident in the military sector, where armed forces rely on the smooth interplay between both environments. More broadly, global communication is dependent on the infrastructure at the junction of cyber and space technologies for international transmission and connection. In our pandemic-era reality, satellites are also crucial to monitoring diseases and maneuvering remote medical supply delivery systems. During the Covid-19 outbreak in China, unmanned aerial vehicles guided by BeiDou navigation satellites played a crucial role in monitoring the spread of the virus and providing large-scale disinfection.

The pivotal importance of space services for modern-day life make them particularly vulnerable – especially in times of geopolitical unrest – to cyberattacks and other hostile acts. Threats at the intersection of space and cybersecurity 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 a satellite or anti-satellite weapons (ASAT), which several space-faring nations have developed. Non-kinetic physical attacks, such as electromagnetic pulses, can cause severe damage to space assets. In 2018, the Centre for International and Strategic Studies reported that the Russian government had developed a laser-based system that blinds the sensors of enemy satellites rather than destroying them. Electronic threats include activities designed to damage the transmission and reception of data (jamming) or the transmission of false data (spoofing). Cyberattacks in this domain largely deal with the direct insertion of false data or the unauthorized monitoring of traffic in outer space. Direct links to ground stations make the new generation of satellites vulnerable to cybersecurity breaches. For example, hackers could take control of systems to launch attacks. Finally, earth-based threats include interference with space-system supply chains or attacks on physical infrastructure used for the transmission or storage of data.

Recent events have shown that cyber and electromagnetic attacks are no longer the remit of science fiction. Increased levels of space militarization may increase the risks of confrontation as well as the number of attacks. The exploration of outer space used to be reserved to major space-faring nations. However, this is now changing as technological innovations such as CubeSats, used for remote sensing and communications, and the burgeoning role of the private sector in the space industry make access to space easier and cheaper. This is a mixed blessing and is likely to amplify the vulnerabilities mentioned above. The proliferation of self-trained or state-supported hackers combined with cheaper access to computer technologies increases the risk of disruption to earth-space and space-earth interactions. These attacks are often hard to trace, making it difficult to identify the aggressor.

> AS GEOPOLITICAL TENSIONS HEAT UP ON EARTH, IT IS CRUCIAL THAT ALL SPACE-FARING PARTIES UNDERSTAND THAT IF OUTER SPACE BECOMES CRITICALLY UNSAFE, IT WILL NOT BE SELECTIVELY UNSAFE, BUT UNSAFE FOR EVERYONE

As geopolitical tensions heat up on earth, it is crucial that all space-faring parties understand that if outer space becomes critically unsafe, it will not be selectively unsafe, but unsafe for everyone. In a global commons such as outer space, humanity will either triumph or fail together. And yet, despite the weighty challenges, co-operation in outer space continues to be impeded by the lack of trust, narrow geopolitical interests, a reluctance to share information and the absence of binding and non-binding mechanisms. Our global order remains an anarchic system with no over-arching global authority able to arbitrate and enforce mandates in a just and equitable way. No wonder that states are preoccupied with safeguarding what they consider to be their national interest.

So how do we go about achieving sustainable peace and security in outer space and shield ourselves from the perils of malicious cyber activities? On a fundamental level, we need to rewire our geopolitical paradigms and move from zero-sum to multi-sum security, where good governance ensures justice for all individuals, states and cultures, without gains at the expense of the other. In a connected and deeply interdependent world, we should adopt a Symbiotic-Realist paradigm, which holds that despite the inherent anarchy of the state system, states are bound to cooperate as they share cultures and challenges. It also allows absolute gains and non-conflictual competition. In space, this takes on a whole new dimension as states rely on each other for information, launches, missions and much more. Security in outer space and on earth go hand-in-hand. They cannot be achieved without reconciling the national interests of states with transnational, global and planetary interests.

In practical terms, this means increasing co-operation around space-based services and deepening collaboration of all stakeholders, including public and private entities. With this in mind, I recommend prioritizing the following five policy actions:

1. Create stronger regulatory frameworks

We need to address the glaring gaps in space law. Current international regulatory frameworks are weak and have not been able to keep pace with technological advances. The Outer Space Treaty of 1967, the international mainframe for space law signed by over 130 countries, is dated and lacks bite. The treaty prohibits "harmful interference" but does not explicitly ban lethal systems other than weapons of mass destruction. This provides wiggle room for the use of ASATs and the hacking of space systems, which are not explicitly forbidden.

2. Build coalitions of support

We need to improve the cyber resilience of space-based services that depend on satellite networks. This will require strengthening the response capacity of governments and creating collaborative and informed exchanges between policy-makers, satellite manufacturers and software developers.

3. Increase satellite security

We need to rethink how we design and operate our satellite systems, with a focus on enhancing cybersecurity. This will require creating new methods of data encryption tailored to the space environment. We should apply the hardware and network security know-how that satellite operators have gleaned from working in other sectors with strict security requirements.

4. Regulate the rise of commercial actors in outer space

Space is becoming more crowded and more commercialized, with space exploration slated to create $1.2 trillion in retail revenue by 2030. The influx of private actors has increased the risk of competition, collisions and geopolitical tensions, with some governments encouraging activity by private actors to stake national territorial claims. With space exploration no longer exclusively a government-dominated environment, we need clear-cut codes of conduct for commercial actors.

5. Improve cooperation around space-traffic management

According to the United Nations Office for Outer Space Affairs, there are currently almost 11,000 satellites orbiting the Earth, of which over 2,000 were launched last year. With a record number of satellites shot into orbit, space debris is becoming a serious concern as an object as small as a paperclip can sabotage a spacecraft or satellite. As the risk of collisions in outer space grows, we must rethink how we use – and govern – outer space. Collaborative efforts to mitigate space debris and improve space management frameworks could increase trust and improve co-operation among spacefaring nations in other fields.

Humans are more dependent on space assets than ever before. But opportunities for global societal benefits come hand-in-hand with greater risks, and we are now increasingly vulnerable to disruptions of those assets. These vulnerabilities have become more pronounced in the face of cyber-threats and geopolitical fissures on Earth. Looking to the future, governments will need to pay closer attention to the security challenges at the space-cyber nexus. By devoting resources to space security, governments are investing in more robust health systems, reliable food chains, a cleaner environment and a safer planet. It is crucial that we improve co-operation and co-ordination in this domain.

NAYEF AL-RODHAN
is Head of the Geopolitics & Global Futures Programme at the Geneva Centre for Security Policy (GCSP) and an Honorary Fellow at St Antony's College, Oxford University.