3 Main Points

There is an immediate need for a thorough, multifaceted strategy to security that incorporates international collaboration, regulatory restrictions, technical standards, and moral principles for AI space cybersecurity. There is an immediate need for a thorough, multifaceted strategy to security that incorporates international collaboration, regulatory restrictions, technical standards, and moral principles for AI space cybersecurity.

About the Authors

Petra graduated in IRO at Leiden University and is focusing on Aerospace Law, EU Law, and Telecommunications Law before starting her Master's in September 2025. She developed a strong interest in space affairs, viewing space as a unique arena to advance diplomacy amid rising political polarization and growing influence of private entrepreneurs.

Lenaïg Deslandes holds a B.Sc. in International Relations and Organizations from Leiden University (NL). Her research focuses on US-China relations, international security, and space strategy.

Cybersecurity of Space Assets

Introduction

Space infrastructure is essential for global cyber networks in today's interconnected world, enabling critical services like navigation, satellite communications, weather forecasting, and Earth observation. The increasing dependence on space-based technology has made cybersecurity more important than ever. There is an immediate need for a thorough, multifaceted strategy to security that incorporates international collaboration, regulatory restrictions, technical standards, and moral principles for AI space cybersecurity, from impaired communications to jeopardised national security.

Satellites, ground stations, uplink/downlink channels, and control centres are examples of interconnected systems that make up space infrastructure. Cyberthreats like malware injection, spoofing, jamming, denial-of-service (DoS) attacks, and unauthorised access can affect these systems. For example, Global Navigation Satellite System (GNSS) signal spoofing can affect military operations, transportation, and emergency response, while satellite hacking can result in unlawful control. Data interception can reveal private information, and jamming can interfere with communications. Furthermore, before a system is deployed, supply chain vulnerabilities may subtly jeopardise its integrity.

A notable example is the cyberattack on the Viasat KA-SAT satellite network during the early stages of the 2022 Russia-Ukraine conflict. This attack disrupted satellite internet services across Europe, affecting both military and civilian infrastructure. Such incidents highlight how cyberattacks on space assets can have far-reaching consequences beyond their immediate targets.

Existing cybersecurity and space policy frameworks are inadequate to handle the difficulties created by the merging of cyberspace and space, despite the increasing hazards. Incorporating machine learning (ML) and artificial intelligence (AI) into space operations presents opportunities for threat identification and decision-making. However, it also adds additional challenges, especially in the space environment.

The militarisation of outer space and the quick growth of space operations by both public and private actors bring about moral, legal, and technological issues. Due to the interdependence between space and cyber infrastructures, a failure in one area might have a cascading effect on the other, increasing potential dangers. There is an immediate need for a thorough, multifaceted strategy to security that incorporates international collaboration, regulatory restrictions, technical standards, and moral principles for AI space cybersecurity.

Impact and Consequences

The consequences of cyber threats have gotten more severe due to our increasing reliance on space infrastructure. Critical services like emergency communications, telecommunications, GPS navigation, and weather forecasting depend on satellites. Cyberattacks on these systems have the potential to compromise public safety and interfere with emergency response activities. For instance, satellite communication networks are crucial for organising rescue efforts during natural disasters. Any interference with these systems may slow responses down, potentially harming more people and damaging more goods.

Such vulnerabilities can impact both military and civilian infrastructure, as the 2022 Viasat cyberattack showed. With repercussions that extended well beyond Ukraine, the attack interfered with broadband services throughout Europe. GPS spoofing attacks have also been used to interfere with the navigation of commercial aircraft and military unmanned aerial vehicles. This underscores the increasing complexity of space-based cyberwarfare strategies.

From a national security perspective, space-based assets are increasingly militarised, creating significant strategic risks. Cyberattacks on satellites can weaken military monitoring, block communication routes, or enable espionage. New risks are introduced by the growing use of Unmanned Aerial Vehicles (UAVs) in disaster relief and defence. Because UAVs rely on GNSS signals to navigate, they are vulnerable to jamming and spoofing. This may lead to civilian casualties, lost assets, or mission failure in conflict scenarios. In addition to international legal frameworks like the Geneva Conventions, integrating multi-GNSS platforms with cryptography and AI-based anti-spoofing measures will be necessary to secure these systems.

Cyberattacks can cause immediate interruptions as well as spillover effects on vital infrastructure. Terrestrial systems that depend upon satellite data for communication and timing, like energy grids, transportation, and banking, are closely linked with space systems. The impact of a successful cyberattack on one system can be increased by spreading failures to other systems. For instance, GPS jamming or spoofing can distract emergency services,

interfere with autonomous vehicles, and skew financial transactions. Because of deteriorating infrastructure and growing digitisation, urban areas are especially at risk.

It is essential to increase the robustness of space-based systems as the cyber-physical boundary grows. It is crucial to have a thorough awareness of the technologies, threat environments, and links across the legal, military, civil, and cyber realms. Cyber threats in space are not hypothetical, as real-world events have shown; they are occurring right now and have serious repercussions. Governments, businesses, and international organisations must work together to address these challenges and create safe, interoperable systems that can endure changing threats.

Emerging Solutions and Obstacles

Cyber weapons have often been subject to attempts at regulation, either through domestic legislation, legal regimes, or multilateral agreements. Yet the connection between cyber and space is so far overlooked. There are no international laws regulating cyberthreats directly to space assets, but current regulatory space mechanisms can provide an amount of protection against such threats.

The 1967 Outer Space Treaty (OST) constitutes the basis for space law. It indirectly imposes a limitation on cyber counterspace capacities by prohibiting the use of force in space. Since, efforts were made to develop norms, rules, and principles for cyberspace by several nations. The United Nations' Open-Ended Working Group (OEWG) contributed to the most recent development through its 2021 Developments in the Field of Information and Telecommunications in the Context of International Security. Based on past UN reports, the OEWG has established guidelines that indirectly impact the use of cyber technology in space. Today, discussions within the OEWG on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours constitute the first step in remedying this phenomenon. While these discussions are unlikely to result in formal recommendations against cyber threats, some states have proposed a recognition of cyber counterspace capabilities as irresponsible behaviour and suggested general guidelines for transparency and confidence-building measures, lessening the threat and rendering it harder to carry out.

Domestic and Regional Strategies

After recognising space as a future domain of operations in 2019, NATO has encouraged member countries to join space and cyber operations, enhancing defence and deterrence capabilities. However, NATO states are split in their conception of space (operational or warfighting). An alternative for the organisation is to coordinate and promote interoperability and information sharing among members, increasing trust and best practices in cyberspace. This has been the case for joint services encompassing space situational awareness (SSA), intelligence, surveillance and reconnaissance (ISR), and positioning, navigation and timing, satellite communications (SATCOM). The EU is also developing its cybersecurity space vision. By developing space legislation according to cybersecurity principles, it encourages member states to integrate cybersecurity considerations into their domestic space laws.

Meanwhile, contentious relations with the Global South are likely to challenge current debates in fora like the OEWG. The Global South traditionally favours legally binding agreements compared to the norms-based preference of developed countries. Yet where this diversity of interests and stakeholders could drag the development of cyberspace global governance, it would also ensure the longevity of the mechanisms and state compliance.

Alternatively, India is a progressive space-faring power. Its latest National Cyber Security Strategy, envisioned by the Data Security Council of India, has yet to recognise space infrastructures, but is gradually incorporating cyber diplomacy. As for China, it has catalysed the adoption of responsive governance practices. In the wake of rising great power military confrontations, Chinese authorities advocate for the development of a strategic stability architecture, bringing the largest spacefaring nations to consider cyberattack prevention for nuclear facilities, communications systems, and space structures.

Future Considerations

Mitigating cyber counterspace threats demands technological and policy solutions. The cyber environment is ever-changing, and so should technological solutions adapt. A unified

policy structure could guide technological efforts to safeguard space assets as well as encompass the growing actor space, incorporating non-state and commercial actors.

A dual-track process combining technological and governance elements is often mentioned. From a technological standpoint, this includes a revision of security and best practices in space. In the USA, cybersecurity best practices in space networks would manifest through the US National Institute of Standards and Technology risk frameworks, and the US Space Force Infrastructure Asset Pre-Assessment of commercial satellite communications. Similar policy developments can be expected for the European Space Agency (ESA) cybersecurity programs. These securitising programs would include risk assessment, automatic defensive tools, and event management techniques; in combination with traditional security paradigms, they would increase the difficulty and cost of cyberattacks.

In terms of governance planning, the current international legal regime is outdated and lacks the necessary resources to address the rise of commercial actors, market forces, and space weaponisation. The interdependence between space assets and cyber capacities impacts national security interests, thus limiting transparency, information sharing, and the implementation of binding mechanisms. For national space strategies to adequately address rising competition and security concerns in space, the government, industries, and academia need to be included in national discussions of space and cyber industrial policy. Globally, a multilateral cybersecurity regime is required. International collaboration between space-faring powers is equally important. Other relevant stakeholders should also be incorporated into the discussion, as space systems are both publicly and privately owned, including actors in the space supply chain, civil society, and the private sector.

Conclusion

Outer space is the next step for geopolitical cybersecurity considerations. Existing cybersecurity and space policy frameworks are ill-equipped for the gradual merging of both spheres. As the 2022 Viasat cyber attack demonstrated, civilian, military, and government life are vitally reliant on space systems.

Including cyberspace in space security and defence dialogue is increasingly relevant, not only for governmental institutions, but also for commercial actors and civil society. Preliminary academia has been quick to outline necessary policy, regulatory, and legal measures to foster the growing interconnectedness. Yet, further thorough work is required to progress beyond shared values and towards technological, governance, and policy structures that can involve the array of affected actors as well as encourage a secure, sustainable, and mutually beneficial outer space.