Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities

Ulpia-Elena BOTEZATU
Romanian Space Agency
ulpia.botezatu@rosa.ro

Abstract: Cyber infrastructure and the outer space technologies and systems are profoundly reliant one onto another. Thus, any malfunction in one of these complex interrelated infrastructures, be it intentional or not, would induce errors in the other. Furthermore, space infrastructure only has ground-based, space-based, downlinks and uplinks components, thus complexifying even more the issue of security. Threats to space-based infrastructure can come in many forms, including denial-of-service attacks, malware infections, and unauthorized access to systems. When discussing cyber-attacks targeting satellite networks and space-based systems, it may emerge disruptions and severe consequences on communication, navigation, and other essential services.

Cyber security in outer space is a complex and evolving field that requires careful attention and planning. Vulnerabilities can create weaknesses that attackers can exploit, and effects such as disruption or destruction of critical services can have serious consequences. To mitigate the risk of cyber-attacks, organizations can take a variety of measures, such as implementing security best practices, conducting regular security assessments and testing, and developing response plans for cyber incidents. Consequently, the article looks at cyber threats to space-based infrastructures, reviews some incidents and proposes some recommendations for approaching the cyber security of space technologies and services. Ensuring the security and resilience of space-based infrastructure is critical for maintaining the integrity and reliability of modern cyber infrastructure.

Keywords: Critical Outer Space Infrastructure, Governance of Security, Complex Systems, Cyber Security, Space-Based Infrastructure.

INTRODUCTION

The final frontier of technology, i.e. the outer space, is just as vulnerable to cyber threats as any other area. The importance of overlapping cyber domain with the outer space is rising, as the number of space-based systems and applications grow. Moreover, as integrator of vital systems (Botezatu & Piso, 2020) and services, the outer space domain is strongly influenced by any weakness in this complex system of systems.

The modern cyber infrastructure, which includes communication networks, data centres,

https://doi.org/10.54851/v5i1y202306

cloud computing systems and the internet, heavily depends on outer space technologies and systems, as previously mentioned in the literature (Piso, 2019 ; Wilson Center, 2021). Firstly, satellites play a crucial role in providing global communication infrastructure, allowing data to be transmitted across vast distances. Satellites are used for a range of communication services, including television and radio broadcasting, internet connectivity and telecommunication. Second aspect refers to the Global Navigation Satellite System (GNSS), a space-based navigation system that provides precise location and timing information, which is essential for many applications, including transportation, logistics and emergency response. Thirdly, Earth Observation satellites equipped with sensors provide high-resolution images and data on weather, natural disasters and climate change. Such data is used in various applications, including agriculture, disaster management and urban planning. Finally, cloud computing services are increasingly using space-based infrastructure for storage and processing of large amounts of data. Space-based computing offers high-performance computing capabilities and storage for mission-critical applications.

However, the increasing reliance on space-based infrastructure also poses significant cyber security risks. Cyber-attacks targeting satellite networks and space-based systems can have severe consequences on communication, navigation and other essential services that rely on these systems. Therefore, ensuring the security and resilience of space-based infrastructure is critical to maintaining the integrity and reliability of the modern cyber infrastructure.

SPACE AS CRITICAL INFRASTRUCTURE

Space has become a critical infrastructure for modern society, with its services playing an increasingly vital role in daily lives. Given the criticality of these outer space services, many of which are enabled or enmeshed with the cyber sphere, the disruption or failure of space-based infrastructure could have severe consequences for many aspects of human activities, including transportation, energy, finance and emergency response (Livingstone & Lewis, 2016; Piso, 2019).

The space infrastructure is a complex system of systems, with many interconnected components that rely on each other to function effectively. These systems include satellites, ground-based control stations, communication networks and data centres, among others. To ensure the safe and secure operation of this complex system of systems, it is essential to consider both the outer space and cyber infrastructure together (Botezatu & Piso, 2020). This is because the operation of space-based infrastructure relies heavily on cyber systems, and any disruption or failure of either system can have severe consequences.

For example, a cyber-attack on a ground-based control station could compromise the security of a spacecraft or satellites under its control, leading to the disruption of critical services or even the loss of the spacecraft. Similarly, a solar storm or space debris collision could damage or disable a satellite, leading to a loss of service and potential cascading effects on other systems.

To address these challenges, it is essential to take a holistic approach to the security and resilience of space-based infrastructure (Pellegrino & Stang, 2016). This includes implementing robust cyber security measures, such as encryption and authentication, regularly updating software and firmware, and ensuring the physical security of both space-based and ground-based systems.

Space situational awareness is also critical for identifying and mitigating threats to space-based infrastructure. This involves monitoring the space environment for hazards such as space debris and solar storms and developing contingency plans to minimize their impact (Cernat et al., 2020). For issues related to the Space Surveillance and Tracking (SST), i.e. cataloguing and tracing pieces of space debris so that it won't collide with functional assets, international cooperation and collaboration are essential for ensuring the safe and secure operation of space-based infrastructure. This includes sharing information about threats and best practices, establishing standards and regulations, and working together to respond to emergencies.

The complex system of systems that is space-based infrastructure requires a holistic approach to security and resilience that considers both the outer space and cyber infrastructure together. By doing so, we can ensure the continued safe and secure operation of this critical infrastructure. Moreover, space-based infrastructure is also vulnerable to a range of threats, including natural hazards such as space debris and solar storms, as well as human-made threats such as cyber-attacks and intentional interference (King & Goguichvili , 2020).

Recognizing the importance of space as critical infrastructure, governments and space agencies around the world are taking steps to enhance the resilience and security of space-based infrastructure. This includes investing in space situational awareness and debris mitigation, developing contingency plans for space emergencies and strengthening cyber security measures to protect against cyber threats. In conclusion, space infrastructure is a critical infrastructure that plays a crucial role in modern society, and its security and resilience must be a top priority.

DISRUPTIVE CYBER-ATTACKS ON SPACE SYSTEMS

Disruptive cyber-attacks on space systems are a significant threat that can cause severe damage to critical infrastructure, including satellites, ground stations and communication networks. Such attacks can result in the loss of valuable data, interruption of critical services and potentially even the destruction of assets in space (Botezatu et al., 2020). Some examples of disruptive cyber-attacks on space systems include:

- *Jamming* is a technique used to disrupt satellite signals by transmitting a high-power signal on the same frequency as the satellite's signal. Jamming can cause significant disruptions in communication networks and can even render a satellite useless. In 2013, for example, a GNSS jamming incident disrupted signals over a large area of the UK, causing widespread disruption to aviation, maritime navigation and other critical services.
- *Denial-of-service* (DoS) attacks are designed to overwhelm networks or systems with large amounts of traffic or requests, making them unavailable to legitimate users. DoS attacks can be particularly damaging to space systems, where reliability and availability are critical. In 2018, a DoS attack (exemplified in the next section of the article) was reported to have disrupted the Galileo navigation system, causing outages that lasted for several days.
- *Malware* is a type of software designed to disrupt or damage computer systems. Malware can be particularly damaging to space systems, where the consequences of a successful attack can be severe. In 2018, for example, a malware attack disrupted the operations of a satellite ground station in Australia, causing significant delays in the delivery of critical data.

The potential for disruptive cyber-attacks on space systems is likely to increase as our reliance on space-based technologies continues to grow, especially within the era of New Space economy. To mitigate these threats, space agencies and companies must develop robust cyber security strategies and deploy effective countermeasures, such as advanced encryption, intrusion detection and network segmentation, to protect their assets in space.

CYBER SECURITY INCIDENTS AND OUTER SPACE

As our dependence on technology increases and we become more reliant on satellites and other space-based infrastructure for communication, navigation and surveillance, the need for cyber security in outer space has become increasingly important. The lack of gravity, extreme temperatures and harsh radiation environment in space can pose unique challenges to cyber security. Spacecraft and satellites are vulnerable to cyber-attacks, which can disrupt or damage critical systems, compromise sensitive data, or even render them inoperable.

To address these challenges, cyber security measures must be integrated into the design, construction and operation of space-based infrastructure. This includes implementing strong encryption and authentication protocols, regularly updating software and firmware and ensuring physical security of spacecraft and ground-based systems. Space agencies and private companies operating in space must also collaborate and share information about cyber security threats and best practices. International cooperation and agreements may be necessary to establish standards and regulations for cyber security in outer space.

There have been several cyber incidents that have affected outer space infrastructure, including satellites and spacecraft. Here are some notable examples:

Stuxnet Worm (2010)

There have been several cyber incidents that have affected outer space infrastructure, including satellites and spacecraft. Here are some notable examples:

Although not specifically targeted at space infrastructure, the Stuxnet worm (Gregersen, 2021) was a highly sophisticated cyber weapon that targeted industrial control systems, including those used in nuclear facilities. The worm was designed to cause physical damage to centrifuges used in uranium enrichment. Stuxnet demonstrated the potential of cyber-attacks to cause physical damage to critical infrastructure. The worm was able to spread through networks and infect ICS software, allowing it to gain control of the centrifuges and cause them to spin at dangerously high speeds or stop completely.

Stuxnet used a range of advanced techniques to evade detection and spread through networks, including the use of stolen digital certificates, zero-day vulnerabilities and a rootkit to hide its presence. The worm was also able to modify the code on programmable logic controllers used to control the centrifuges, making it difficult to detect and remove.

While Stuxnet was not specifically targeted at space systems, it highlights the potential for cyber-attacks to cause physical damage to critical infrastructure, including those used in space exploration and satellite communication. As the reliance on space-based technologies continues to grow, the risk of cyber-attacks on these systems is likely to increase, making cyber security a critical issue for the space industry.

Dragonfly (2011)

Dragonfly is a hacking group that has been active since at least 2011 and is believed to be based in Russia. The group has been linked to attacks on energy companies and has also been found to have targeted the industrial control systems of EU and US companies (Schaffer, 2017).

There is limited information available on Dragonfly's specific attacks on space systems. However, it is known that the hacking group has been linked to attacks on energy companies, including those involved in the production and distribution of natural gas, electricity and petroleum.

In 2014, the US Department of Homeland Security (DHS) issued an alert warning that Dragonfly had targeted the industrial control systems of US aerospace companies. The alert stated that Dragonfly had been „able to compromise a number of organizations, including defence contractors and subcontractors, aerospace companies and energy companies" (Cybersecurity and Infrastructure Security Agency, 2022; Paganini, 2016). While the DHS alert did not provide specific details on the impact of Dragonfly's attacks, it highlighted the potential for the group to cause significant damage to critical infrastructure (Cybersecurity and Infrastructure Security Agency, 2022).

The alert also noted that Dragonfly had used a variety of tactics to gain access to its targets, including spear-phishing emails and watering hole attacks. Once inside a target's network, the group would use a range of techniques to move laterally and escalate privileges, including the use of stolen credentials and malware designed to bypass security controls (Krause et al., 2021).

It is worth noting that the threat landscape for cyber-attacks on space systems is constantly evolving, and the techniques used by Dragonfly may have changed since the DHS alert was issued. However, the alert serves as a reminder of the importance of robust cyber security measures to protect against the growing threat of cyber-attacks on space systems.

International Space Station Malware (various incidents)

Initially in 2008, but then in several other moments in time, it was reported that malware had infected computers on board the International Space Station (ISS) (Wells, 2020). The malware was believed to have been introduced through a USB drive used to transfer files between Earth and the ISS. While the malware did not appear to have caused any significant harm, it highlighted the vulnerability of space-based infrastructure to cyber-attacks.

GNSS signal Jamming (various incidents)

GNSS is a critical component of many space-based systems, including navigation, communication and timing. There have been several incidents of GNSS jamming, where signals from satellites have been intentionally blocked or disrupted. While not technically a cyber-attack, GNSS jamming can have similar effects, causing disruption or even loss of service.

To exemplify, in 2020, there have been thousands of interruption instances reported from China to California, from the Arctic Circle to New Zealand (Buesnel, 2020). For instance, on December 2019, a jammer set up at a nearby pig farm is to blame for the intermittent GNSS signal loss experienced by planes landing at Harbin Airport in northeastern China. According to The South China Morning Post (Zuo, 2019), the jammer was intended to stop criminal gangs from using drones to drop swine fever-infested packets on the herd, forcing farmers to sell them the sick meat at a lesser price. A remarkable tale that once again shows how the deployment of illicit jammers can have unforeseen, potentially harmful effects on public aviation.

GNSS Spoofing (various incidents)

For many years, GNSS spoofing (the broadcasting of a phony or delayed GNSS signal) has been a problem in the defence sector, but it is now beginning to affect commercial and civilian users as well. More unsecured systems will be subject to spoofing assaults as more gadgets and autonomous systems depend on GNSS and as spoofing knowledge and tools are now very simple to obtain.

Autonomous systems, such as drones and driverless autos, require reliable Positioning, Navigation and Timing (PNT) services to function dependably. Multi-sensor systems' real-world performance, dependability and resilience must be evaluated by manufacturers to ensure that they are functioning properly for operations that are both safety- and liability-critical. Because of this, platform performance and integrity testing is likely to be moved in the future outside of the lab and into actual environments.

Traditionally, standalone systems have been used to build and test GNSS receivers. Yet, as time goes on, they become more and more integrated into a sophisticated device that has a number of ports, sensors and connections. Since the radio-frequency (RF) interface is just another attack vector from a hacker's perspective, it is more likely that the specific GNSS vulnerabilities in the RF domain will be addressed as part of a comprehensive cyber security framework rather than being handled separately.

There have been a few reported cases of GNSS spoofing affecting space systems, including:

- spoofing of a drone: In 2013, a team of researchers from the University of Texas demonstrated that they could spoof the GNSS signals of a drone, causing it to deviate from its intended course. The researchers used a spoofer to transmit false signals to the drone's receiver, which caused it to believe it was in a different location. This technique could be used to hijack or disrupt drones used in space exploration or satellite communication.

- spoofing of a satellite: In 2018, researchers from ETH Zurich demonstrated that they could spoof the GNSS signals of a satellite in low Earth orbit. The researchers used a software-defined radio to transmit fake signals to the satellite's receiver, causing it to report false position data. This type of attack could be used to disrupt satellite-based navigation systems, including those used in space exploration.
- spoofing of a ship: In 2019, the US Maritime Administration issued an alert warning that several vessels in the Black Sea had reported GNSS disruptions. The alert noted that the disruptions appeared to be the result of spoofing, which was causing the vessels to report false positions. While this event did not directly affect space systems, it highlights the potential for GNSS spoofing to cause disruptions in critical infrastructure. Another example highlights Iran's presumed activities in the Strait of Hormuz, which used spoofing technology to cause the British tanker Stena Impero to deviate its course and enter the sovereign waters of Iran (Wiese Bockmann, 2019a). The Islamic Revolutionary Guard Corps seized Stena Impero and its 23 crew members on July 19 2019 in a move widely regarded as retaliation for the impounding of the Iranian-controlled very large crude carrier Grace 1 in waters off Gibraltar on July 4 (Wiese Bockmann, 2019b).

As the reliance on space-based technologies continues to grow, the risk of GNSS spoofing attacks on space systems is likely to increase, making it critical to develop robust countermeasures to detect and prevent spoofing (Botezatu et al., 2020).

Galileo Satellite System Outage (2019)

The European Union's Galileo satellite system suffered a major outage in 2019, affecting the accuracy and availability of its positioning services. The outage was caused by a „technical incident related to its ground infrastructure" (European Commission, 2019), which was later attributed to a cyber-attack. The incident highlighted the importance of securing both space-based infrastructure and its ground-based support systems (Samson, 2023).

These incidents demonstrate the potential of cyber-attacks to disrupt or damage space-based infrastructure and the need for robust cyber security measures to protect them. Overall, as space becomes an increasingly important domain for human activity, ensuring the cyber security of space-based infrastructure will be critical for maintaining the safety and security of our planet.

CYBER SECURITY IN OUTER SPACE

When discussing cyber security related to the outer space realm, the following key considerations should be highlighted:

- Threats - Like any other system connected to the internet, space-based infrastructure is vulnerable to cyber-attacks. Threats to space-based infrastructure can come in many forms, including denial-of-service attacks, malware infections and unauthorized access to systems.
- Vulnerabilities - Space-based infrastructure is complex and relies on many interconnected systems and applications. This complexity can create vulnerabilities that attackers can exploit. For example, a single vulnerability in a satellite's software could potentially compromise the entire system.
- Consequences - Cyber-attacks on space-based infrastructure can have serious consequences. Disruption or destruction of space-based infrastructure can impact critical services such as telecommunications, navigation and weather forecasting. These services are important for many sectors, including transportation, finance and emergency response.
- Regulation - While there are no specific international laws or regulations governing cyber security in outer space, there

are several international organizations working to develop guidelines and best practices for space-based cyber security. In addition, individual countries are developing their own regulations to ensure the security and resilience of space-based infrastructure.

- Mitigation - To mitigate the risk of cyber-attacks on space-based infrastructure, organizations can take a variety of measures, including implementing security best practices, conducting regular security assessments and testing and developing response plans for cyber incidents.

In conclusion, cyber security in outer space is a complex and evolving field that requires careful attention and planning. As space-based infrastructure becomes increasingly critical to modern society, it is essential for organizations to prioritize cyber security and take proactive steps to mitigate the risk of cyber-attacks.

ADDRESSING THE NEXUS BETWEEN THE CYBER SPHERE AND THE OUTER SPACE

The European Union (EU) has made several attempts to regulate cyber security in outer space. Here are some notable examples:

- The EU Space Surveillance and Tracking (SST) program - The SST program is a collaborative effort between the European Commission and EU Member States to improve the tracking and monitoring of objects in space. The program includes a focus on space debris mitigation and the development of cyber security measures for space-based infrastructure.
- The European Union Agency for Cyber Security (ENISA) - ENISA is an EU agency responsible for promoting cyber security in Europe. As part of its mandate, ENISA works to develop guidelines and best practices for cyber security in outer space, as well as coordinating with other EU institutions and international organizations to promote the security and resilience of space-based infrastructure.
- The EU Space Policy - The EU Space Policy is a framework for the development of EU space activities, including space-based infrastructure. As part of the policy, the EU has identified cyber security as a key area for action, with a focus on developing standards and best practices for space-based cyber security and promoting international cooperation on the issue.
- The EU's General Data Protection Regulation (GDPR) - While not specific to outer space, the GDPR is a regulation that applies to all EU Member States and aims to protect the privacy and personal data of EU citizens. The GDPR has implications for space-based infrastructure that collects and processes personal data, such as Earth observation satellites.

In addition to these regional endeavours, on the international arena, several international organizations play a role in promoting cyber security in outer space:

- United Nations Office for Outer Space Affairs (UNOOSA) - UNOOSA is responsible for promoting international cooperation and understanding in the peaceful uses of outer space. As part of this mandate, UNOOSA promotes the development of norms, guidelines and best practices for space activities, including cyber security.
- International Telecommunication Union (ITU) - The ITU is a specialized agency of the United Nations responsible for promoting the development and coordination of international telecommunications. As part of its mandate, the ITU develops international standards and guidelines for space-based telecommunications and works to ensure the security and reliability of space-based communication networks.
- European Space Agency (ESA) - The ESA is an intergovernmental organization responsible for the coordination and funding of European space activities. As part of its mandate, the ESA promotes the development of secure and resilient space-based infrastructure and works with

international partners to address cyber security threats to space-based systems.

- International Committee on Global Navigation Satellite Systems (ICG) - The ICG is an intergovernmental forum for promoting the use of global navigation satellite systems (GNSS), such as GPS and Galileo. As part of its mandate, the ICG promotes the security and resilience of GNSS systems and coordinates international efforts to address threats to their security.
- International Association for the Advancement of Space Safety (IAASS) - The IAASS is an international non-profit organization dedicated to promoting the safety and sustainability of space activities. As part of its mandate, the IAASS promotes the development of cyber security standards and guidelines for space-based infrastructure to ensure its safe and secure operation.

These international organizations work to promote cyber security in outer space by developing standards, guidelines and best practices, sharing information and best practices and coordinating international efforts to address cyber security threats (Bailey, 2022). By working together, these organizations can help to ensure the safe and secure operation of space-based infrastructure for the benefit of all. As space-based infrastructure becomes increasingly critical for modern society, it is essential for policymakers to continue to prioritize cyber security and resilience in outer space.

INSTEAD OF CONCLUSIONS: HIGHLIGHTING TRENDS IN CYBER SECURITY AFFECTING SPACE INFRASTRUCTURE

The article so far has presented just a few examples of cyber-attacks on space systems. As our reliance on space-based technologies continues to grow, the risk of cyber-attacks on these systems is likely to increase, making cyber security a critical issue for the space industry.

As the world becomes increasingly reliant on technology, the risks of cyber-attacks in outer space are becoming more apparent. Cyber security measures are essential in addressing these threats and protecting critical infrastructure in space (Holmes, 2020). Here are some trends in cyber security measures addressing cyber-attacks in outer space:

- Securing satellite communication: Satellites are an essential component of our space infrastructure, and securing their communication channels is critical. Encryption and authentication protocols are being developed and deployed to secure the data transmissions between satellites and ground stations.
- Artificial intelligence and machine learning: AI and ML technologies are being developed to detect anomalies and unusual behaviour in satellite systems. These technologies can help identify potential cyber-attacks before they cause significant damage.
- Collaborative efforts: International cooperation and collaboration between space-faring nations are essential to address cyber-attacks in space. Efforts are being made to establish international cyber security standards and protocols for space systems.
- Supply chain security: The supply chain for space systems is complex, and vulnerabilities can be introduced at any stage. Ensuring the security of the supply chain is crucial to preventing cyber-attacks in space.
- Advanced threat intelligence: Advanced threat intelligence can help space agencies and companies stay ahead of emerging threats and identify potential vulnerabilities in their systems. This involves collecting and analysing data from a variety of sources to provide actionable intelligence.

In summary, cyber security measures for outer space are rapidly evolving and include a combination of technical solutions, collaborative efforts and advanced threat intelligence. As space becomes more accessible and integral in daily lives, securing the space infrastructure will become even more critical.

In order to mitigate the extent of cyber-attacks in outer space, comprehensive measures should be taken into consideration.

Firstly, legal measures are essential to mitigating cyber-attacks in outer space. The development of international laws and norms, the establishment of liability and responsibility and the promotion of transparency and information-sharing are all important steps in this process. Additionally, the development of cyber security standards, increased monitoring and enforcement, and strengthened international cooperation can help prevent cyber-attacks from occurring in the first place.

Secondly, organizational measures are critical to mitigating cyber-attacks in outer space. Conducting regular risk assessments, implementing security measures, establishing incident response plans, training personnel, conducting regular audits, engaging in information-sharing and collaborating with cyber security experts can help organizations protect their space systems from cyber-attacks.

Finally, technical measures are essential to mitigating cyber-attacks in outer space. Implementing strong encryption, multi-factor authentication, access controls, conducting regular vulnerability assessments, monitoring network traffic, using intrusion detection systems and implementing data backup and recovery systems can all help organizations protect their space systems from cyber-attacks.

In summary, addressing cyber security in outer space is of critical importance because cyber-attacks can have severe consequences for both space systems and the safety of personnel on Earth. Space systems are vulnerable to cyber-attacks due to their complex and interconnected nature, and the potential consequences of such attacks can be devastating.

As this paper discussed, cyber-attacks on space systems can cause disruption to critical services such as communication, navigation and remote sensing. These disruptions can affect a range of industries, from transportation and finance to national security and emergency response. Moreover, cyber-attacks can cause damage to the space systems themselves, leading to significant financial losses and delays in space exploration and research.

In addition to the economic and operational consequences, cyber-attacks on space systems can also pose a threat to the safety of personnel on Earth. For instance, cyber-attacks on communication or navigation systems could impact the ability of rescue teams to respond to emergencies, or interfere with critical satellite data used to monitor natural disasters.

Addressing cyber security in outer space is crucial to ensure the safety and security of space systems, the continuity of critical services on Earth and the success of space exploration and research. As space activities become more widespread and complex, the need to address cyber security will only become more important.

REFERENCE LIST

Bailey, B. (15 July 2022) Cybersecurity Protections for Spacecraft: a Threat Based Approach. *The Aerospace Corporation.* https://aerospace.org/paper/cybersecurity-protections-spacecraft-threat-based-approach [Accessed 23 March 2023].

Botezatu, U. E., Nistor, C., Radutu, A. & Olteanu, V. (2020) GNSS and Earth Observation Services Disruption, Between Collapse and Myth. *Space Infrastructures: From Risk to Resilience Governance.* IOS Press, pp. 294 - 309.

Botezatu, U. E. & Piso, M. I. (2020) Vital Outer Space Infrastructures: Romania's Pursuits and Achievements. *Space Infrastructures: From Risk to Resilience Governance*. Springer, pp. 329 - 336.

Buesnel, G. (2 December 2020) Thousands of GNSS jamming and spoofing incidents reported in 2020. *Linkedin.* https://www.linkedin.com/pulse/thousands-gnss-jamming-spoofing-incidents-reported-2020-guy-buesnel/ [Accessed 23 March 2023].

Cernat, M., Botezatu, U. E, Poenaru, V. D., Nedelcu, D. A. & Turcu, V. (2020) SST and NEO Related Activities in Romania – An Overview of Institutional and Legal Framework. *Space Infrastructures: From Risk to Resilience Governance.* Springer, pp. 359 - 372.

Cybersecurity and Infrastructure Security Agency. (2022) *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a [Accessed 30 March 2023].

European Commission. (2019) *European GNSS (Galileo) Initial Services, Quarterly Performance Report.* Report number: Q4. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-IS-SAR-Quarterly-Performance_Report-Q4-2019.pdf.

Gregersen, E. (2021) Stuxnet. In: *Encyclopedia Britannica.* https://www.britannica.com/technology/Stuxnet [Accessed 30 March 2023].

Holmes, M. (2020) The Growing Risk of a Major Satellite Cyber Attack. *Via Satellite.* https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/[Accessed 27 March 2023].

King, M. & Goguichvili, S. (2020) Cybersecurity Threats in Space: A Roadmap for Future Policy. *Wilson Center Blog.* https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy [Accessed 23 March 2023].

Krause, T., Ernst, R., Klaer, B., Hacker, I. & Henze, M. (2021) Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors.* 21(18), 6225. doi: 10.3390/s21186225.

Livingstone , D. & Lewis, P. (2016) *Space, the Final Frontier?* London, UK, Chatham House, The Royal Institute of International Affairs.

Paganini, P. (2016) FBI-DHS JAR report links Russian hackers to Presidential Election hacks. *Security Affairs.* Report number: APT28, APT29. https://securityaffairs.co/54900/hacking/fbi-dhs-jar-report.html [Accessed 30 March 2023].

Pellegrino, M. & Stang, G. (2016) *Space Security for Europe.* European Union Institute for Security Studies.

Piso, M. (2019) *Space as Critical Infrastructure.* International Academy of Astronautics.

Samson, V. (2023) The Cyber Counterspace Threat: Coming Out of the Shadows. *Centre for International Governance Innovation (CIGI).* https://www.cigionline.org/articles/the-cyber-counterspace-threat-coming-out-of-the-shadows/ [Accessed 23 March 2023].

Schaffer, M. (2017) Dragonfly 2.0: Hacking Group Infiltrated European and US Power Facilities!. *Linkedin.* https://www.linkedin.com/pulse/dragonfly-20-hacking-group-infiltrated-european-us-power-m-shaffer/[Accessed 30 March 2023].

Wells, S. (2020) Protecting ISS. *Aerospace America.* https://aerospaceamerica.aiaa.org/features/protecting-iss/ [Accessed 30 March 2023].

Wiese Bockmann, M. (2019a) Seized UK tanker likely 'spoofed' by Iran. *Lloys's List.* https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran [Accessed 23 March 2023].

Wiese Bockmann, M. (2019b) Gibraltar orders release of Iranian tanker. *Lloys's List.*

https://lloydslist.maritimeintelligence.informa.com/LL1128798/Gibraltar-orders-release-of-Iranian-tanker [Accessed 23 March 2023].

Wilson Center. (2021) *Cybersecurity on the Final Frontier: Protecting Our Critical Space Assets from Cyber Threats.* https://www.wilsoncenter.org/event/cybersecurity-final-frontier-protecting-our-critical-space-assets-cyber-threats [Accessed 27 March 2023].

Zuo, M. (2019) China flight systems jammed by pig farm's African swine fever defences. *South China Morning Post.* https://www.scmp.com/news/china/society/article/3042991/china-flight-systems-jammed-pig-farms-african-swine-fever [Accessed 23 March 2023].