The European Union and the Protection Of Critical Space Infrastructure from Cyber-Threats: A Strategic Approach?

Alexandru Georgescu[1], Clara Cotroneo[2] and Andreea Dinu[1]
[1]National Institute for Research and Development in Informatics, ICI Bucharest, Romania
[2]Global Governance Institute, Brussels, Belgium

alexandru.georgescu@ici.ro
c.cotroneo@globalgovernance.eu
andreea.dinu@ici.ro

Abstract: The functioning of terrestrial critical infrastructures, such as electricity, transportation, and finance depends on critical space infrastructures (CSI). CSI underlie the provision of vital goods and services, economic activities, national and global security. Consequently, securing CSI from cyber-attacks is important to avoid disruptions in the provision of critical goods and services and ensure high levels of security in our societies. Existing cases of cyber-attacks against ground and space components of CSI have proven the consequences of such attacks for domestic and international security, economic, systemic, environmental and social safety and stability. With strategic gains increasingly motivating state and state-sponsored attacks against CSI, the European Union (EU) expanded its resilience and response toolbox to address cyber-threats against CSI. Space has become a highly strategic domain with the EU *Strategic Compass*, since 2022. Furthermore, in 2023, the High Representative and the Commission put forward an *EU Space Strategy for Security and Defence*, presenting the EU's vision for space security. This programmatic document marks a shift in the EU's configuration of space, from a domain for scientific and civilian enterprises, to one central to security and defence. This paper examines the quick evolution of the EU's approach to protecting CSI between 2020 and 2024 against the background of the development of the EU's approach to CI protection more broadly and the development of its space governance aspirations and capabilities. It examines the EU institutional and legislative frameworks for CSI resilience to assesses how relevant and strategic these are considering new technological developments, in the current global security context.

Keywords: Critical space infrastructures, Resilience, Cyber-attacks, Governance

1. Introduction

Critical space infrastructure (henceforth "CSI") are complex systems composed of distributed components on Earth, in orbit and in deep space, made up of technical assets and operating entities, connected through communication links, and producing space services for numerous users and beneficiaries. Space systems have become a critical enabler for a wide range of applications in command, control and coordination of complex distributed infrastructures, in communication and data gathering, utilizing a widening range of capabilities such as remote sensing, for positioning, navigation and timing. For example, on CSI depend the use of mobile phones, web connectivity, and the availability of coordinates needed for private, public and commercial transportation. Their functions are therefore key to the provision of vital services and goods, economic stability and prosperity. CSI also underlie the functioning of a range of activities to manage environmental hazards, from earthquakes to forest fires, and man-made threats, such as border crossings. In the current global geopolitical environment, space assets and capabilities have an increasingly strategic value: while space was once configured primarily as a domain for research, exploration and for asserting states' scientific and technological capabilities, it has now become a critical domain for both civil and military operations. Moreover, this domain represents an instrument for exercising state power and influence in the international arena, by allowing to showcase technological sovereignty and competitiveness, economic power and defence capabilities.

Over the past ten years, the EU has increasingly been exploiting CSI across domains. The 2016 *European Space Strategy* set forth the EU strategic vision for the development and deployment of the space sector to enhance EU economy and society. The strategy came in response to shifts in technological development, private sector involvement and global competition. After the 2022 *Strategic Compass for Security and Defence* recognised space as a strategic domain, the new 2022 *EU Space Strategy for Security and Defence* promoted the protection of space assets from a range of threats, the advancement of EU's interests in space and EU autonomy. In the same direction, the 2023 *Critical Entities Resilience Directive* (CER) identified space as one of the sectors crucial for the EU growth and security, obliging Member States (MS) to take steps towards the identification, designation and protection of space assets. At the EU level, the inclusion of CSI into taxonomies of critical entities as part of the CER Directive reflects growing awareness of transborder effects of space infrastructure disruption. With the EU deepening its reliance on CSI to achieve promote economic growth,

technological innovation and advance its international stature, protecting such assets is emerging as a central European concern.

Space systems are registering attacks which are more numerous, frequent, sophisticated, and destructive, because space is a "contested, congested and competitive space environment" (Department of Defense and Office of the Director of National Intelligence, 2011) in which space systems are becoming legitimate targets for conflict. CSI are increasingly the target of malicious actors looking to disrupt their functioning, steal data, manipulate outputs, disrupt or sabotage the functioning of critically dependent CI, weaken the capabilities of military actors that rely on these systems (Botezatu, 2024a). Existing cases of cyber-attacks against ground and space components of such CIs have proven the consequences of such attacks for domestic and international security, economic, systemic, environmental and social safety and stability. Against this background, this chapter examines the development of the EU approach to CSI protection from cyber-attacks, considering current technological trends and developments, in the current geopolitical and international security contexts. It provides an overview of the CSI cyber-risk profile and an analysis of relevant technological trends impacting CSI security from cyber-attacks, before examining the EU's approach to CSI protection. This is assessed for comprehensiveness and relevance to identify strengths and weaknesses. The methodology has involved documental research and review of public documents, combined with the quality analysis of a small number of surveys (seven responses) and three interviews with researchers, project implementers and CI operators.

2. The Cyber Risk Profile of CSI

Space systems represent a hybrid threats target that enable attackers to maintain their efforts below the threshold of armed response, defeat attribution efforts that can trigger diplomatic repercussions, and limit the damage in such an interdependent environment. CSI have a risk profile with certain specificities resulting from their construction, operation and operating environment (Botezatu, 2024b). Their complex cyber risk profile has four components. The first component is the security environment, encompassing threat actors, stakeholders involved in the construction and operation of CSI, stakeholders benefitting from them, and transformations to any of the above. The second component is the risk profile of the individual components of CSI, the combination of which leads to a different overall cyber risk profile. The third component is the systemic risk profile of CSI components acting in concert in a system-of-systems and complex system approach, where the behavior of the system is affected by the interaction between components. The fourth component is the governance framework, that is the underlying mechanisms, measures, incentive structures which govern the decision-making capability of CI operators and the competent regulatory authorities.

Based on the analysis of the CSI cyber-risk profile, a comprehensive and adequate framework for their resilience must incorporate the following elements. First, an approach tailored to the CSI sector for threat identification, analysis and assessment, incident response and management, which addresses cascading effects; second, an awareness of actor-specific motivations and *modus operandi*, accounting for a range of antagonistic actors; third, an understanding of threats of different nature, including intentional and accidental, man-made or natural (e.g., natural disasters, extreme weather events, etc.) and the inter-relations between them; fourth, an integrated and coherent approach to CIS resilience between actors, public and private, at different governance levels.

3. Analysis of Trends and Technological Development Affecting Cybersecurity in CSI

This section presents a non-exhaustive list of the major technological trends which alter either the CSI security environment or the characteristics of their components in such a way as that the deployment of such technologies can increase or decrease CSI vulnerability to cyber-attacks.

The adoption of Artificial Intelligence

AI use in CSI can become prevalent because of the intrinsic digitalization of CSI processes as they deliver critical services (and, in the future, critical goods). AI can aboost CSI functioning as they will more and more be applied in resilient design of CSI systems, as industrial control system for distributed CSI, as coordinator of complex auxiliary processes (such as cybersecurity threat identification and response) and as contact point in the information and decision-making flow with interconnected CI that adopt AI as well. AI capabilities can also be used to defend against cyberattacks, for example to identify and fix vulnerabilities in software libraries and databases. However, there are cybersecurity risks stemming from these evolutions in AI use, ranging from disruption of normal AI functioning to defects in the functioning of the AI systems. Furthermore, AI can also be

used by attackers as a tool to enable new cybersecurity threats (Sambucci & Paraschiv, 2024), to increase the sophistication and complexity of attacks.

The adoption of Distributed Ledger Technology

The decentralized nature of Distributed Ledger Technology (DLT) or Blockchain makes it a useful tool also for space systems (Wainscott-Sargent, 2019). Blockchain technology can improve cybersecurity outcomes on many current systems within CSI SoS, especially by preventing single points of failure through decentralized architectures and by enabling data integrity and secure software updates (especially given the increased number of supply chain attacks (CybersecAdmin, 2024). However, an emerging risk is the possibility of new cybersecurity vulnerabilities appearing, since DLT has been shown to be vulnerable depending on architecture, specific infrastructure, transaction validation algorithms and the resources of the attackers. The fact that many industry-specific applications run on private, more centralized blockchain networks running proof-of-authority algorithms with a much smaller number of validation nodes makes it more likely that a force attempt compromise their functioning and introduces numerous possibilities of sabotage into the system (Vacusta & Nica, 2023).

Quantum computing

Growing quantum computing capabilities present a significant risk to CSI, given their strong reliance on telecommunications to link components together and provide the critical services. Cyber criminals have already adopted a “Harvest Now, Decrypt Later” approach to data, where they steal encrypted data waiting that the necessary quantum cryptography capabilities are accessible to them (European Parliamentary Research Service, 2024). CSI, as part of the critical IT and telecom infrastructure, is maximally exposed to this issue, which will require CSI operating entities and those suffering from a critical dependence on them to engage in a quantum transition strategy that minimizes current risks, based on current technology levels and sets the stage for quantum-safe techniques and products once they become available (Deloitte, 2023).

Morphological changes in CSI architecture

he impact of new technologies and new requirements leads to new architectures for individual CSI components and morphological changes at the level of the entire CSI. This reorganization will naturally change the cyber risk profile of the system. The architecture of individual space systems is also undergoing a shift. As demand for space services rises and new launch technologies come online, there has been a profusion of standardized satellite architectures that can be adapted for multiple uses and produced in large quantities for mega-constellations (Cookson, 2016), in contrast to the previous paradigm, in which sophisticated research and development centers or contractors created bespoke hardware and software systems in low numbers, designed with in mind resilience to the space environment, to hackers and other deliberate threats. Older systems benefited from “security through obscurity”, as potential attackers were not familiar with the hardware, software and communication links that were specially developed for a particular system, which limited their ability to infiltrate and do harm. This challenge is further exacerbated by the use of COTS, the lynchpin of growing cybersecurity vulnerability for CSI and is an increasingly important issue across all CI sectors (Falco, 2018). Hackers can become intimately familiar with these types of systems and their skills and competencies are transferrable from one CI to another, including to CSI. One example was the hacking of a European Space Agency nanosatellite (Interesting Engineering, 2023).

Worsening cyber threat environment

The cyber threat environment for CSI has deteriorated significantly in recent years. The significant growth of the space economic sector and the visible importance of space-based capabilities in high-profile situations such as in conflict situations, as it has been for the conflict in Ukraine, have fostered a greater awareness of space systems as a critical dependency and as a target (Georgescu, 2025). In addition to the possibility that organized crime groups and lone actors would disrupt space systems for profit or ideology, inter-state competition in space is also growing. This manifests in the development of anti-satellite capabilities (Defence Intelligence Agency, 2022), growing rhetoric that describes space systems, including civilian and commercial space systems, as legitimate military targets and an overall greater willingness to use hybrid warfare against civilian critical infrastructures in energy, transport and also space. Moreover, in space “grey zone threats” and measures under the threshold of war are growing in use, with the objective of degrading critical space capabilities for military, economic or strategic-circumstantial use (Robinson et al, 2019).

Overall, the examination of new and emerging trends highlights that a comprehensive and solid framework for CSI protection and resilience needs to address the following levels: first, the technological level, which entails a deep, continuous and up-to-date understanding of how each technology can be leveraged both for building efficiency or damaging CSI; second, an understanding of the capacities and capabilities of different actors, including state and non-state actors, with regards the malicious use of such technologies; third, a legislative and diplomatic toolbox that clearly defines what is admissible and how to hold accountable malicious actors attacking space systems; fourth, a framework for engaging and cooperating with the private sector, which plays a crucial role in providing components for, designing, developing, commercialising and operating CSI.

4. The Current EU Framework on CSI and Cyber

This section examines the development of the EU approach to CSI protection between 2020 and 2024, when the most far-reaching developments have taken place (Pursiainen & Kytömaa, 2023). Its objective is to draw conclusions on the extent to which the EU approach to the protection of CSI is strategic. The most significant development in the systemic understanding of space infrastructure as critical assets and systems to be protected took place with the simultaneous launch of the CER Directive (European Union, 2022a) and the NIS 2 Directive (European Union, 2022b). The former identifies space assets as part of European essential entities, placing them in a wider taxonomy of essential entity domains that includes energy, transport, banking, financial markets, health and food. Following the designation of space infrastructure as critical, EU CSIs also benefit from the existing general cybersecurity and critical infrastructure protection governance framework, provided for by the NIS2 Directive. These two documents together affirm the criticality of CSI protection and promote a EU-wide approach to CSI cyber-resilience, with clear objectives and obligations.

The CER and NIS2 Directive work in tandem with other core instruments, including the 2022 *Council Recommendation to strengthen the resilience of critical infrastructure* (European Union, 2023a) and the 2024 *EU Critical Infrastructure Blueprint* to build capacity to react to cross-border incidents (European Union, 2023b). Both these instruments identify cyber-attacks as a priority hybrid threat and put forward an all-hazard, risk-based approach which takes into account risks of different nature, including man-made and natural, intentional and accidental. This approach is crucial to CSI protection because of the inter-relatedness between risks, vulnerabilities and incidents: that is, the impacts arising from an incident not of cyber-nature can cause vulnerabilities to cyber-attacks. For example, an incident caused by an extreme space weather event can cause vulnerabilities to cyber-attacks, and vice versa. Third, on the actor level, these instruments intend to account for a range of actors, including state and state sponsored actors, criminal actors, and terrorist groups.

In addition to the previously mentioned legislation on CI space governance and cybersecurity issues, horizontal and sectorial instruments contain elements relevant to the protection of CSI from cyber-attacks. These include the *Cyber Resilience Act* (European Union, 2024a), *Regulation (EU, Euratom) 2023/2841 for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union* (European Union, 2023c), the *Cyber Solidarity Act* (European Comision, 2023d), the *Council Conclusions on the EU Policy on Cyber Defence* (Council of the European Union, 2023), the *EU Cyber Diplomacy Toolbox*, which provides the framework for the EU to attribute a cyber-attack on a space system to a malicious actor, designate him as the perpetrator, enact proportional sanctions and the *EU Strategic Compass*, where space has emerged as an important domain. Alongside horizontal instruments, sectoral initiatives also contain relevant protection elements. Examples are the *AI Act* (European Union, 2024b) and the 2021 *Coordinated Plan on Artificial Intelligence* (European Commission, 2018), on the basis of which CSI applications of AI would fall into the high-risk category, creating obligation for robust transparency, data and process integrity, accountability, reliability and traceability (Georgescu, 2022).

Table 1: Core elements of an emerging EU framework on CSI and Cybersecurity

The EU Framework in CSI and cybersecurity				
Critical Assets and Infrastructures	**Space-relevant agencies**	**Cyber-relevant Agencies and instruments**	**Key space legislation**	**Key cybersecurity legislation**
COPERNICUS **GALILEO** **IRIS² (GOVSATCOM)** **EGNOS**	EUSPA ESA DG DEFIS	ENISA CERT-EU EC3 ISACs	EU Space Strategy for Security and Defence Regulation (EU) 2021/696	CRA Directive CER Directive NIS 2 Directive Regulation 2023/2841

The EU Framework in CSI and cybersecurity				
EUMESAT (meteorological) **SSA Space Situational Awareness (EU and national)** **Space Situational Surveillance and Tracking** **Launch sites (example: CSG Guiana)**	National agencies EU Satellite Center SatCen European GNSS Service Center	ECCC CSIRT EU Cyber Defence Coordination Centre EEAS (through Cyber Diplomacy Toolbox) MICNET Hybrid Toolbox Hybrid Rapid Response Teams (Council of the European Union, 2022)	EU-ESA framework agreement Secure Connectivity Programme EU Space Law Space Data Economy Strategy	Cyber Solidarity Act AI Act DORA EU Policy on Cyber Defence

With regards to EU agencies, the EU institutional structure for CSI protection involves a range of agencies with different, complementary but not always clearly integrated tasks concerning the protection of CSI. EDA is tasked with developing a Capability Development Plan (CDP), which facilitates the set-up and coordination of defence planning amongst Member States. The 2023 CDP identifies the protection of space systems as one of the key priorities and cyber-attacks against them as a key threat for which MS need to prepare. ENISA advances the cyber-security of the Union's CSI by disseminating tailored threat analysis and assessments, such as the assessment of cyber threats against the Low Earth orbit (LEO) telecommunication service (European Union Agency for Cybersecurity, 2023). On the operational level ESA has the responsibility of keeping the space systems it operates secure from cyber-attacks, via specialized teams responsible for incorporating the principle of 'cybersecurity by design' in all projects and activities and for the forensic analysis and investigation of incidents. ESA is particularly well placed for identifying and deterring cyber-threats, thanks to its network of sites that allow for the identification of earth and space threats. Crucially, the agency uses quantum technologies to support its assessment of security risks.

In addition to the agencies mentioned above, working groups have been established to minimise fragmentation and facilitate the coordination, cooperation, exchange of information and good practices among MS. The CER Directive established the *Critical Entities Resilience Group* (CERG) which facilitates cooperation, exchange of information and good practices between Member States and the Commission. The Directive mandates the CERG to cooperate with the *NIS2 Cooperation Group*, which focuses on facilitating cooperation and information exchange among MS, the European Commission, and ENISA. On the operational level, the *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe) is also foreseen to support with managing and information exchange in case of large-scale incidents and crisis.

Finally, on the external policy level, the EU *Strategic Compass* and the EU S*pace Strategy for Security and Defence* outline clear actions for the protection of space systems and services. The latter envisages the creation of tailored capabilities, including the *Information Sharing and Analysis Centre* (ISAC) to facilitate exchanges between commercial and public entities, addresses the security of space systems supply chains and the EU long-term objectives for autonomy. Finally, EU foreign policy also address the topic of responsible and secure space, both at the level of EU-NATO cooperation and within international trade and foreign relations, such as within the EU-US cooperation on space issues and on cyber issues.

Overall, the EU framework for the protection of CSI from cyber-attacks present some key protection elements including the adoption of an all-hazard, risk-based approach which accounts for a range of antagonistic actors. The approach also brings focus to the cooperation between public entities and commercial actors, necessary to ensure the security of CSI supply chains, their safe operation, and the deployment of civilian space systems for public use and security interests. The approach leverages on new and emerging technologies, though only at the agency-level, and attempts at addressing some of the risks related to such technologies, such as in the case of AI and quantum. However, the approach presents several weaknesses. First, it is still rather fragmented at the institutional level, potentially due to the lack of awareness of critical dependencies on space until recently, the overall lack of comprehensive capabilities on the part of any single EU space actor, and the existence of the European Space Agency as an intergovernmental, rather than EU organization, tasked with developing the common space capabilities of the EU. The latter factor also limits the EU approach to security and defence in space, as ESA is non-military in orientation and is concerned mainly with threats such as orbital debris, space weather and, recently, cyber issues. Second, from a threat analysis perspective, a systematic approach to the interconnectedness between impacts of different types of threats (cyber, military/kinetic,

natural) is missing, such as one considering the impacts of extreme weather events on the cyber-security of CSI.

With regards to future development, the first draft of the EU Space Law, published in 2025 aims at introducing "common EU rules addressing the safety, resilience and sustainability of space activities and operations". Its main objectives are: combine information sharing with the protection of assets and the common framework for incident management; enshrine security (and cybersecurity) by design into space systems and operations; and, "incentivise the exchange of information on threats targeting space assets or their supply chain" (European Space Law, 2025). Therefore, the EU Space Law aims at addressing some of the fragmentation and advance a more integrated distribution of tasks across EU bodies. The cybersecurity monitoring of all EU space programs will be done under EUSPA, with the assistance of ENISA (European Union Agency for Cybersecurity) and EU-CERT (the Computer Emergency Response Team for EU institutions) taking a lead role in ensuring cybersecurity. In parallel, there will also be a *Strategy for Space Data Economy* governing the sharing of data across all EU sectors which, by necessity, will require cybersecurity and other forms of assurance of data and system integrity, confidentiality and so on (European Parliament, 2025).

5. Conclusions and Recommendations for Increased CSI Cybersecurity and Resilience in the EU

The European Union is critically dependent on the secure supply of space services in the field navigation, positioning and timing, remote sensing and telecommunications, which enable long distance trade, the digital economy, complex financial markets and more. The analysis of the EU policy and institutional structures for the protection of CSI from cyber-attacks has shown that the approach presents key strategic elements, including the identification of space systems as critical assets and the identification of cyber-attacks as a key threat. Tailored instruments also set-out obligations for MS to address and cooperate on the protection of CSI from cyber-attacks. At the institutional level, however, the approach would benefit from an integrated coordination mechanism, in the form of an entity responsible for coordinating the overall protection of EU CSI from cyber-attacks. Further integration is particularly important given the fragmentation of CSI governance and their operationalisation, which fall on MS authorities and commercial entities. With regards to the latter, the EU approach misses a set of standards for the protection of CSI from cyber-attacks, applicable to all commercial entities providing for CSI, managing or operating them.

Based on the analysis of the EU approach to CSI protection against CSI vulnerabilities to cyber-attacks and new technological trends some key recommendations for the EU to achieve greater resilience in the new technological, geopolitical and security context are included below:

- The creation of a CSI-oriented Information Sharing and Analysis Center (ISAC) with automated indicator and data sharing, as put forward in the CER and NIS2 Directives;
- The organization of regular cross-sector cybersecurity exercises between the space sector and other critically dependent CI sectors (Yamin & Nowostawski, 2021);
- The creation, in partnership with industry bodies from the EU or likeminded partners such as the US, of a "trusted vendor program" that builds a cyber resilient ecosystem of space systems and components vendors (especially in the context of growing COTS solution use);
- The drafting and promotion of unified cybersecurity standards for EU space systems, applicable to commercial entities and drafted with their inputs;
- The creation of a specialized pool of satellite capabilities accessible to any EU MS or partner country suffering from disruption of ordinary space-based systems during crises;
- The acceleration in scope and ambition of EU strategic autonomy programs in space, to lower dependence on non-EU systems, and ensure greater trust in cybersecurity and the resilience of these systems (Bucovetchi, 2020);

References

Botezatu, U.-E. (2024a) 'Cybersecurity in the Era of Space Domain Awareness', *Romanian Cyber Security Journal*, 6(1), pp. 29-38. Available at: https://rocys.ici.ro/documents/116/Art._3_ROCYS_1_2024.pdf (Accessed: 30 January 2025).

Botezatu, U.-E. (2024b) 'Space Cybersecurity: A Survey of Vulnerabilities and Threats', *Romanian Cyber Security Journal*, 6(2), pp. 53-60. Available at: https://rocys.ici.ro/current-articles/space-cybersecurity-a-survey-of-vulnerabilities-and-threats/ (Accessed: 30 January 2025).

Bucovetchi, O., 2020. *Resilience of Critical Infrastructure Index Design Between Diversification and Uniformization*. Space Infrastructures: From Risk to Resilience Governance, 57, p.181. IOP Press.

Caba-Maria, F., Georgescu, A., Mureșan, L. and Mușetescu, R. C. (eds.) (2020) *Promoting the Belt and Road Initiative and 17 + 1 Cooperation in Central and Eastern Europe, from the Perspective of Central and Eastern European Countries*. Eikon. ISBN: 978-606-49-0389-1. Available at: https://mepei.com/report-policy-analysis-promoting-the-belt-and-road-initiative-and-17-1-cooperation-in-central-and-eastern-europe-from-the-perspective-of-central-and-eastern-european-countries/ (Accessed: 30 January 2025).

Cookson, C., 2016. *Nano-satellites dominate space and spread spies in the skies*. FT Research, 11 July. Available at: https://www.ft.com/content/33ca3cba-3c50-11e6-8716-a4a71e8140b0 [Accessed 30 January 2025].

Council of the European Union, 2022. *Council conclusions on a framework for a coordinated EU response to hybrid campaigns*. Council of the European Union, [online] Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/ [Accessed 30 January 2025].

Council of the European Union, 2023. *Council conclusions on Security and Defence (23 May 2023)*. Council of the European Union, [online] Available at: https://www.consilium.europa.eu/media/64526/st09618-en23.pdf [Accessed 30 January 2025].

CybersecAdmin (2024) 'Blockchain in the Stratosphere: Pioneering the Future of Software-Defined Satellites', *Decent Cybersecurity*. Available at: https://decentcybersecurity.eu/blockchain-in-the-stratosphere-pioneering-the-future-of-software-defined-satellites/ (Accessed: 30 January 2025).

Defense Intelligence Agency (2019) *Challenges to Security in Space*. Available at: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf (Accessed: 30 January 2025).

Defense Intelligence Agency (2022) *2022 Challenges to Security in Space*. Washington, DC, USA. Available at:https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf (Accessed: 30 January 2025).

Deloitte, 2023. *Future forward readiness: Preparing for quantum risk*. Deloitte Insights, [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-future-forward-readiness-quantum-risk.pdf [Accessed 30 January 2025].

Department of Defense and Office of the Director of National Intelligence, 2011. *National Security Space Strategy: Unclassified Summary*. Washington, DC, [online] Available at: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy [Accessed 30 January 2025].

European Commission, 2018. *Coordinated plan on artificial intelligence*. European Union, [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0795 [Accessed 30 January 2025].

European Commission (2019) *Ethics guidelines for trustworthy AI*, High-Level Expert Group on AI. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed: 30 January 2025).

European Commission, 2023b. *Communication from the Commission to the European Parliament and the Council on the European Defence Industrial Strategy*. European Union, [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023DC0526 [Accessed 30 January 2025].

European Commission, 2024c. *Draghi Report on EU Competitiveness*. European Commission, [online] Available at: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en [Accessed 30 January 2025].

European Commission, 2023d. *Proposal for a Regulation of the European Parliament and of the Council on the Cyber Solidarity Act*. European Union, [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209 [Accessed 30 January 2025].

European Space Law, 2025. *European Space Law platform*. European Space Law, [online] Available at: https://www.european-space-law.com/ [Accessed 30 January 2025].

European External Action Service (EEAS), 2024. *Space: EU carries out Space Threat Response Architecture 2024 exercise (STRA-X 24)*. EEAS, [online] Available at: https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-2024-exercise-stra-x-24_en [Accessed 30 January 2025].

European Union, 2022a. *Directive (EU) 2022/2557 on the resilience of critical entities*. Official Journal of the European Union, [online] Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng [Accessed 30 January 2025].

European Union, 2022b. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, [online] Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng [Accessed 30 January 2025].

European Union, 2022c. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA Regulation)*. Official Journal of the European Union, [online] Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng [Accessed 30 January 2025].

European Union, 2023a. *Council Recommendation (EU) 2023/020 on a coordinated approach by the Union to strengthen the resilience of critical infrastructure*. Official Journal of the European Union, [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_020_R_0001 [Accessed 30 January 2025].

European Union, 2023c. *Regulation (EU) 2023/2841 of the European Parliament and of the Council of 13 December 2023 establishing the European Defence Industry Reinforcement through common Procurement Act (EDIRPA)*. Official Journal of the European Union, [online] Available at: https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng [Accessed 30 January 2025].

European Union, 2024a. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013*

and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union, L 2847, pp. 1–81. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng [Accessed 30 January 2025].

European Union, 2024b. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act)*. Official Journal of the European Union, L 1689, pp. 1–144. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 30 January 2025].

European Union Agency for Cybersecurity (ENISA), 2023. *Low Earth Orbit (LEO) SatCom cybersecurity assessment*. ENISA, [online] Available at: https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment [Accessed 30 January 2025].

European Parliament, 2025. *Strategy on Space Data Economy*. Legislative Train Schedule – A Europe Fit for the Digital Age, [online] Available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-strategy-on-space-data-economy [Accessed 30 January 2025].

European Parliamentary Research Service (EPRS), 2024. *Artificial intelligence and cybersecurity: Opportunities and risks*. European Parliament, [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf [Accessed 30 January 2025].

Falco, G. (2018) 'Job One for Space Force: Space Asset Cybersecurity', *Cyber Security Project*, Belfer Center, Harvard University, 12 July. Available at: https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity (Accessed: 30 January 2025).

Interesting Engineering, 2023. *Cybersecurity researchers gain control of ESA nanosatellite in an ethical hacking exercise*. Interesting Engineering, 28 April. Available at: https://interestingengineering.com/culture/hackers-gain-control-esa-nanosatellite [Accessed 30 January 2025].

Georgescu, A., 2022. *Cyber diplomacy in the governance of emerging AI technologies – A transatlantic example*. International Journal of Cyber Diplomacy, 3, pp.13-22. Available at: https://doi.org/10.54852/ijcd.v3y202202 [Accessed 30 January 2025].

Georgescu, A., 2025. *A Critical Infrastructure Protection Perspective on the Conflict in Ukraine: Recommendations for a Resilient Post-war Ukraine*. In: S. Nate, ed. *Ukraine's Journey to Recovery, Reform and Post-War Reconstruction*. Contributions to Security and Defence Studies. Cham: Springer. Available at: https://doi.org/10.1007/978-3-031-66434-2_19 [Accessed 30 January 2025].

Georgescu, A. and Cirnu, C.E. (2019) 'Blockchain and critical infrastructures – challenges and opportunities', *Romanian Cyber Security Journal*, 1(1), pp. 93-100. Available at: https://interactive.satellitetoday.com/blockchain-the-next-big-disruptor-in-space/ (Accessed: 30 January 2025).

Georgescu, A., Gheorghe, A., Piso, M.-I. and Katina, P.F. (2019) *Critical Space Infrastructures: Risk, Resilience and Complexity*. Topics in Safety, Risk, Reliability and Quality, 36. Springer International Publishing. ISBN 978-3-030-12604-9. DOI: 10.1007/978-3-030-12604-9.

HP Threat Research, 2023. *Anticipating the quantum threat to cryptography*. HP Threat Research Blog, 9 October. Available at: https://threatresearch.ext.hp.com/anticipating-the-quantum-threat-to-cryptography/ [Accessed 30 January 2025].

Jones, H., 2023. *Revolutionizing satellite security: NASA's groundbreaking project to integrate AI, blockchain & nanosatellites*. Forbes, 16 November. Available at: https://www.forbes.com/sites/hessiejones/2023/11/16/revolutionizing-satellite-security-nasas-groundbreaking-project-to-integrate-ai-blockchain--nanosatellites/ [Accessed 30 January 2025].

Pursiainen, C. and Kytömaa, E., 2023. *From European critical infrastructure protection to the resilience of European critical entities: What does it mean?* Sustainable and Resilient Infrastructure, 8(sup1), pp.85-101.

Robinson, J., Robinson, R., Davenport, A., Kupkova, T., Martinek, P., Emmerling, S. and Marzorati, A. (2019) *State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints*. Prague Security Studies Institute, Prague. Available at: http://www.pssi.cz/download/docs/686_executive-summary.pdf (Accessed: 30 January 2025).

Sambucci, L. & Paraschiv, E.-A., 2024. The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure. Romanian Journal of Information Technology and Automatic Control, 34(3), pp.131-148. Available at: https://doi.org/10.33436/v34i3y202410.

Security, H.W. (2024) 'Anticipating the Quantum Threat to Cryptography', *HP Wolf Security*. Available at: https://threatresearch.ext.hp.com/anticipating-the-quantum-threat-to-cryptography/ (Accessed: 30 January 2025).

Vacusta, B. and Nica, C. (2023) 'Blockchain and Cyber-Security: the Opportunity to Develop a National Data Analysis Platform to Ensure National Security and Financial Stability', *Romanian Cyber Security Journal*, 5(2), pp. 65-74. Available at: https://rocys.ici.ro/documents/109/Art._7_ROCYS_2_2023.pdf (Accessed: 30 January 2025).

Wainscott-Sargent, A. (2019). *Blockchain: The Next Big Disruptor in Space*. [online] Satellitetoday.com. Available at: https://interactive.satellitetoday.com/blockchain-the-next-big-disruptor-in-space/ [Accessed 30 Jan. 2025].

Yamin, M.M., Katt, B. and Nowostawski, M., 2021. *Serious games as a tool to model attack and defense scenarios for cyber-security exercises*. Computers & Security, 110, p.102450. Available at: https://doi.org/10.1016/j.cose.2021.102450 [Accessed 30 January 2025].