CYBERSECURITY GOVERNANCE FOR CRITICAL SPACE INFRASTRUCTURES – THE EUROPEAN FRAMEWORK

Alexandru GEORGESCU, Andreea DINU
National Institute for Research and Development in Informatics ICI Bucharest
alexandru.georgescu@ici.ro, andreea.dinu@ici.ro

Abstract: The cybersecurity of space systems has emerged as a critical concern due to their growing role in delivering essential services across sectors such as energy, finance, and transport. This article provides a structured policy analysis and conceptual framework on the cybersecurity of Critical Space Infrastructures (CSI) within the European Union (EU). Drawing on a wide range of recent legislative and strategic documents, the article profiles CSI cyber risks using a multi-dimensional approach, maps the evolving governance and institutional landscape in the EU, and offers targeted recommendations to enhance cyber resilience. The work contributes to current literature by contextualizing CSI within broader EU strategic autonomy and resilience policies, addressing existing gaps in coordination, threat awareness, and regulatory implementation.

Keywords: space systems, critical infrastructures, resilience, cybersecurity, governance.

INTRODUCTION

Space systems have emerged as critical enablers for a wide variety of applications in our societies, from weather forecasting to geolocation, the timestamping of financial transactions and the coordination of complex electricity grids spread over large distance and with many intermittent producers (such as in the EU's Energy Union). The variety of applications is very large but they come down to a series of key capabilities in communications, data gathering, remote sensing, positioning, and timing. Some of these capabilities can only be provided without space systems at the expense of significant investment in infrastructure on the ground (such as complex sensor networks or widespread physical communications infrastructure) and the space systems provide the most accessible, affordable, and sustainable source of such capabilities especially in societies where they did not already exist and were amortized.

The Critical Infrastructure Protection (CIP) framework states that the functioning of society is reliant on the normal functioning of critical infrastructures (CI) which provide critical goods and services and that their disruption or destruction can cause significant loss of human life, economic damage, loss of functionality or loss of confidence. CIP theory is at the basis of the European Programme for Critical Infrastructure Protection which has recently been upgraded with the addition of the Critical Entities Resilience (CER) Directive and the Network and Information Security (NIS 2) Directive, in addition to sectoral efforts such as risk preparedness in the electricity and natural gas sectors.

Space systems, through their provisioning of critical services, have become components in various critical infrastructure sectors, such as in energy, transport, but also finance and ICT. The latest framework developments in CIP governance, not just at the level of the EU, but

https://doi.org/10.54852/ijcd.v6y202505

also in individual Member States or in NATO, recognize space as a CI sector, necessitating the identification and designation of Critical Space Infrastructures (CSI) (as seen in both the CER and NIS 2 Directives).

The present article is focused on the cybersecurity aspect of the protection of CSI. The cybersecurity resilience and governance of CSI has become very important to states and, at the same time, the crossborder nature of CSI operation and utilization requires a collective approach towards CSI cyber resilience, especially in the context of the interdependencies within the EU (Botezatu, 2024a). This article adopts a policy analysis and conceptual synthesis approach. It does not include empirical research or quantitative evaluation but rather integrates and interprets a wide corpus of official EU documentation, strategic policy initiatives, legislative acts, expert reports, and academic literature relevant to cybersecurity governance for Critical Space Infrastructures (CSI). The sources were selected based on their institutional authority (e.g., European Commission, ENISA, ESA, NATO), recency (published after 2019), and direct relevance to cybersecurity and resilience in space systems. The objective is to frame the CSI cybersecurity challenge within the European Union's emerging governance landscape and to extract actionable insights for policy, governance, and strategic development. The article also incorporates a conceptual risk profiling framework adapted to the distinct characteristics of space-based infrastructures.

WHY THE SPACE ECONOMY IS IMPORTANT

Space activities have become extremely important to the global economy, measured both in their financial impact and also in their systemic impact. The Organisation for Economic Co-operation and Development defined the space economy as "the full range of activities and the use of resources that create and provide value and benefits to human beings in the course of exploring, understanding, managing and utilizing space. Hence, it includes all public and private actors involved in developing, providing and using space-related products and services, ranging from research and development, the manufacture and use of space infrastructure (ground stations, launch vehicles and satellites) to space enabled applications (navigation equipment, satellite phones, meteorological services, etc.) and the scientific knowledge generated by such activities. It follows that the space economy goes well beyond the space sector itself, since it also comprises the increasingly pervasive and continually changing impacts (both quantitative and qualitative) of space-derived products, services and knowledge on economy and society" (OECD, 2019).

Bryce Aerospace and Technology, an American consultancy, calculated that the global space economy was worth 384 billion dollars in 2022, including research, basic science, manufacturing, launch services and the commercialization of services produced through space system operations (Bryce Space and Technology, 2023). The rate of development of the global space economy exceeds the rate of growth for the world itself, attesting to the growing demand for space services. This is also illustrated by a London School of Economics study regarding the multiplier effect of investment into space, which is between 5 and 12 depending on sub-domain, meaning that every euro invested produces 5-12 euro in additional economic activity (Sadlier et al., 2015).

OECD (2019) also cites various estimates by investment firms: "A 2018 report by the investment firm Goldman Sachs predicted that the space economy would reach USD 1 trillion in the 2040s, while a different study by Morgan Stanley projected a USD 1.1 trillion space economy in the 2040s. A third study by Bank of America Merrill Lynch has the most optimistic outlook, seeing the market growing to USD 2.7 trillion within the same timeframe" (OECD, 2019). A more recent estimate by McKinsey places the space economy at 1.8 trillion dollars per year adjusted for inflation by 2035 (Acket-Goemaere et al., 2024).

CRITICAL SPACE INFRASTRUCTURES

Space Infrastructures 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 and at some point in the future goods for markets composed of numerous users and beneficiaries. In accordance with the definitions at the level of the EU and member states, these infrastructures are critical if their destruction or disruption would cause significant loss of human life, economic damage, loss of capabilities and, we would add, the loss of confidence on the part of citizens, investors, partners and allies (Georgescu et al, 2019).

The inclusion by the EU of CSI into taxonomies of critical entities as part of the CER Directive and the NIS 2 Directive (while they were already included in numerous member states among the previous taxonomies of critical infrastructure domains) reflects growing awareness of transborder effects of space infrastructure disruption. We are critically dependent on transport, energy, finance, food supply and numerous other domains. In their turn, these are critically dependent on the reliable functioning of a small (but rapidly growing) number of vulnerable systems which are difficult to replace, easy to identify and must operate in the most challenging environment known to man, with radiation profiles and kinetic hazards that can lead to spontaneous malfunctions. There is also an increasing awareness that space sustainability requires either efforts for disposal at the end of their useful life, the prevention of impact with debris and other space systems and, at some point, active clean-up efforts in ever crowded orbital bands (which are also the most economically useful and where most development is concentrated (OECD, 2024).

We can describe a global navigation satellite system CSI as being composed of the following components: a constellation of GNSS satellites with similar architecture and functionality and maybe with back-up satellites in place to maintain accuracy in case of the loss of one or more systems; one or more ground control stations; ground auxiliary units to boost the signal, sometimes also additional satellites belonging to a separate user to enhance regional functionality such as ZENITH in Japan; communication uplinks and downlinks; the network of devices that can utilize the signal, from normal everyday products such as smartphones to military-grade devices utilizing certain spectrum bands and having additional functionality; a supply chain on the ground for satellite replacement over time.

CSI were already strongly digitalized by the necessity of communication with orbital assets transmitting complex data, but the cyber medium is now also the principal linkage between CSI and CIs which are critically dependent on space systems, such as in transport, finance, and energy. Because of the important growth of the space economy, as detailed in the previous section, we can clearly state that CSI are becoming more and more important in a quantitative and qualitative sense to the functioning of CIs on Earth, and their design, commissioning, operation, protection, and decommissioning represents a large part of the space economy. This means that, alongside other factors in the evolution of CSI, such as the use of commercial-off-the-shelf hardware and software to achieve economies of scale and lower costs, CSI have become attractive targets for hackers.

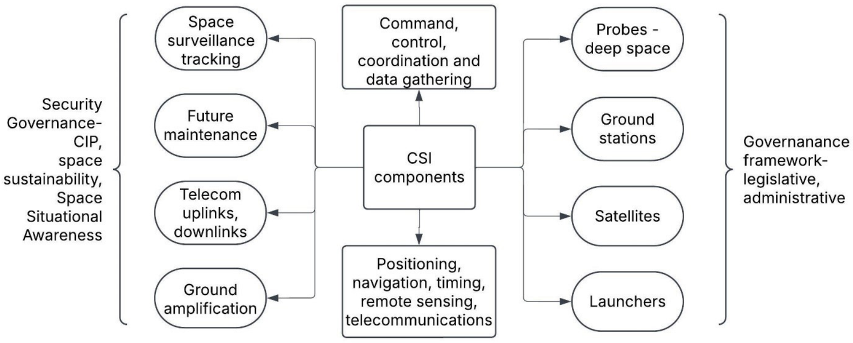

Security Governance-CIP, space sustainability, Space Situational Awareness
Space surveillance tracking
Future maintenance
Telecom uplinks, downlinks
Ground amplification
Command, control, coordination and data gathering
CSI components
Positioning, navigation, timing, remote sensing, telecommunications
Probes - deep space
Ground stations
Satellites
Launchers
Governanance framework-legislative, administrative

Figure 1. Components of CSI

CSI FROM A CYBER RISK PERSPECTIVE

The cyber risk profile of CSI is quite different from that of other CIs, because of the special characteristics of the construction, operation, and operating environments of CSI (Botezatu, 2024b). This extends to their complex cyber risk profile which we can describe as being made up of four components, as in Figure 2. They are as follows:

- The security environment – changes in cybersecurity stemming from exogenous transformations in the environment, encompassing threat actors, stakeholders, incentives, and general environmental elements. For instance, non-state disruptive groups such as terrorists, organized crime groups or hacktivists can gain the know-how and technology, as well as the motivation, to target space systems. Their incentive structure might change – for instance, profit can become a greater motivation, with the ability to use ransomware to extort significant sums for the operator to avoid loss of system functioning (given the cost and timeframes of replacement for most categories of CSI space components);
- The individual risk profiles of CSI components – stemming from Figure 2, we see that the variety of CSI component types leads to different risk profile for each of them. For instance, ground control and telemetry stations will be different compared to orbital assets. If we add the electronic warfare dimension, which has significant overlap with cybersecurity, the differences deepen. Their recovery profile will also be different, as is their ability to mitigate the physical impact of cyber-induced disruption;
- The systemic risk profile of CSI – complex system governance theory teaches us that the whole is greater than the sum of its parts, or the CSI as a system-of-systems exhibits novel behavior than what could have been anticipated from the analysis of individual components (Gheorghe et al., 2018). Component interaction is a source of new behaviors and of new risks, giving rise to the potential for cascading disruptions, but also to novel and emerging behaviors which could not be anticipated from the analysis of individual components. This perspective is most easily used in the wider interaction between CSI

and other CI systems, such as transport or energy, but any sufficiently complex CI is a system-of-system in itself, with individual sub-CI or components. Attackers may also leverage this knowledge in their planning, banking on identifying a systemic vulnerability which the CSI operators had not anticipated. One of these is the use of directional satellites to approach others in order to disrupt them physically or to jam them on-site, which CSIS reports has become a frequent topic of experimentation for systemic rivals such as China or even Russia. Most satellite systems, if not all, are not equipped for physical robustness or for preventing access to internal systems, because this had not been anticipated as an issue;

- The governance framework – since governance concerns itself with the underlying mechanisms, frameworks, and incentive structures which determine decision-making, the governance framework can also have a significant impact on the cyber risk profile. Is there legislation in place to compel investment into cybersecurity and in keeping up with the environment? Are there liability frameworks or insurance issues in place to incentivize investing in resilient CSI? Do the authorities recognize the critical infrastructure status of space systems and regulate it? Do the users of CSI, especially those who are themselves operators of CI, perform due diligence on supplier risk from critical space service providers and have plans to deal with disruption? Many interventions on the part of the competent authorities are designed to raise awareness of issues among CI operators, to establish a reasonable burden of investment in protection and disclosure of incidents, and to affect the incentive structures of operators so that security and resilience are not seen as costs to be minimized (Pulfer, Bucovetchi, and Gheorghe, 2015).

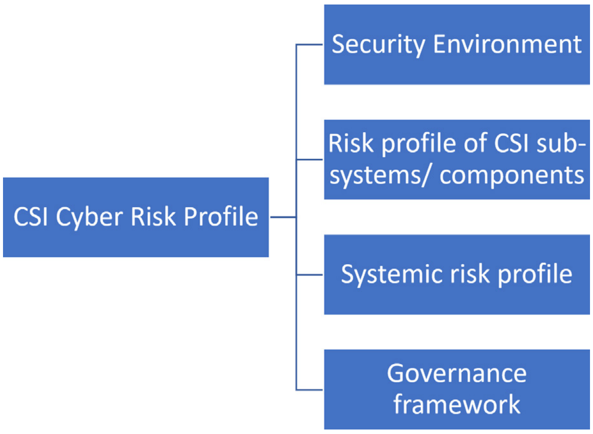


Figure 2. Components of the cyber risk profile for CSI

CYBERSECURITY FOR CSI AT EU LEVEL – FRAMEWORK DEVELOPMENT

The European Union currently lacks a complete and integrated framework on space issues, let alone on space and cybersecurity. There are four main reasons for this:

- The piecemeal construction of EU governance efforts, which takes time and must harmonize with the views of all member states;
- Lack of awareness of the importance of space for national and EU security from a CIP perspective until recently;

- The absence of a fully developed EU space actor with the full roster of strategic space capabilities (unlike the US, Russia and China which feature the entire spectrum of CSI capabilities developed nationally, including global navigation satellite systems);
- This drives the collective project building at the level of the EU which, prior to recent development, resulted in a leading role for the European Space Agency in developing strategic EU capabilities.

This has led to certain issues since the ESA is an intergovernmental organization, not an EU body, which has gained greater salience in the context of more EU decision-making powers. The EU has had to adapt to the reality of ESA's non-military mandate, which places concrete limits on EU-ESA cooperation on security and defense and mainly limits the EU to safety issues such as orbital debris, space weather and, only more recently, cyber issues (Georgescu et al., 2019).

Consequently, the EU has advanced further in its capabilities than in its governance efforts, especially as it has strategically chosen to advocate for peace and the non-militarization of space, while maintaining non-discriminatory access to key systems between legitimate civilian and military users (unlike every other space power which prioritizes military needs) (Georgescu et al., 2019). It has prioritized the development of critical space capabilities through projects such as the Copernicus Earth Observation constellation, the Galileo global navigation satellite system, EGNOS, the European Geostationary Navigation Overlay Service, or the future GOVSATCOM secure government communications network, recently renamed as IRIS (Infrastructure for Resilience, Interconnectivity and Security by Satellite). Nevertheless, the bulk of Europe's consumption of space services for its advanced economy comes from the global market, since its production cannot keep pace with its demand, thereby generating significant dependencies on non-European entities, including with regards to their exposure to cyber risk.

The EU has taken steps to address the fragmentation of its space framework and to ensure better cooperation among member states. This could be seen not only in the light of European development, but also as part of a process of raising awareness of space issues at a global level, since many of the developments were coterminous, taking place in a few short years (Georgescu, 2020):

- The development of the EU Space Programme Agency (EUSPA) with a mandate for cooperation with other member state agencies and partners abroad like the US;
- The development of an EU Space Strategy for Security and Defence in 2023;
- The upgrading of space to the level of operational domain within NATO in 2019 followed by an overarching space policy in 2022. Unlike the EU, NATO is focused on interoperability among members and will not develop and operate its own space assets;
- The development of DG DEFIS, the Directorate General for Defence Industry and Space;
- The 2024 decision of having an EU Commissioner for Defence and Space, whose mission also includes "the design and implementation of a European Air Shield and cyber defence common project", the implementation of the EU Space Strategy for Security and Defence,

the EU-NATO partnership covering "all threats, including those linked to cyber, hybrid or space", further European Defence Fund investment in space capabilities and cyber, while overseeing the future Space Law and the Space Data Economy Strategy (European Commission, 2024);

- The rising number of national Space Forces, following the establishment of the US Space Force and then that of France.

The main high-level framework for space that establishes also the importance of asset security, including through cybersecurity, is made up of the:

- EU Space Strategy for Security and Defence (for a stronger and more resilient European Union) (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2023);
- Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme (European Union, 2021);
- The 2004 EU-ESA framework agreement (European Community and European Space Agency, 2004) and subsequent roadmaps and visions, which have been updated over the years, though the process of making ESA the official EU Space Agency failed;
- The EU Space Programme 2021-2027 (Council of the European Union, 2021);
- The Union Secure Connectivity Programme 2023-2027 (European Union, 2023).

The EU Space Law will have its first draft in 2025 and will focus on "common EU rules addressing the safety, resilience and sustainability of space activities and operations". It will combine information sharing with the protection of assets and the common framework for incident management. It will also "incentivise the exchange of information on threats targeting space assets or their supply chain, focusing on actionable information to relevant security operation centers (SOCs)" (European Space Law, 2024). The cybersecurity oversight of all EU space programs will be managed by EUSPA, in cooperation with ENISA (the European Union Agency for Cybersecurity) and EU-CERT (the Computer Emergency Response Team for EU institutions), which play key roles in ensuring security. At the same time, a Strategy for the Space Data Economy will be introduced to regulate data sharing across EU sectors. Given its scope, this strategy will inherently require cybersecurity measures and other safeguards to ensure the integrity, confidentiality, and reliability of both data and systems (European Parliament, 2024). This linking of trade, innovation, security and defense is seen also in the space section of the Draghi Report on European Competitiveness (European Commission, 2024).

The EU framework is also focused on space domain awareness through space surveillance and tracking and the integrity of systems involved and of the data sharing channels (European Union, 2014). Part of this effort also involves Space Traffic Management, which is a governance issue of global importance with impact on cybersecurity through the required allocation of the electronic spectrum for communications in order to serve requirements for specific transmission types, while avoiding frequency fratricide (unintentional jamming of satellites in close proximity by orbital standards) (European Commission, 2022). Adversaries can also exploit governance deficits to intentionally jam or otherwise disrupt space system operations while maintaining plausible deniability regarding intent (Botezatu, 2023).

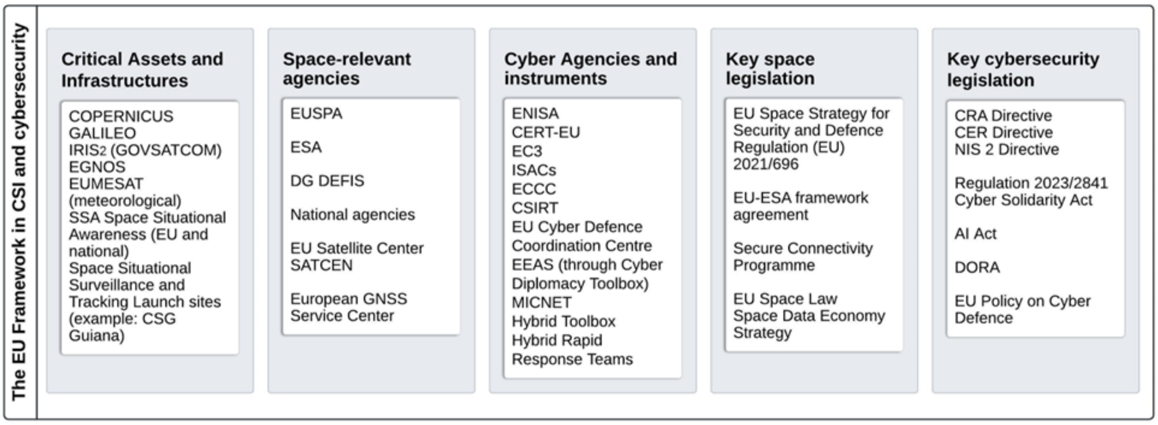
A significant development in the systemic understanding of CSI took place with the simultaneous launch of the Critical Entities Resilience Directive (European Parliament and Council of the European Union, 2022a) and the NIS 2 Directive (European Parliament and Council of the European Union, 2022b), which identify space as a domain for critical European entities and essential entities, respectively, as part of a wider taxonomy on critical/essential entity sectors. These sectors include energy, banking, ICT, public administration, transport, healthcare, financial markets, food production and banking. This implies the compatibility between the general cybersecurity and CIP governance frameworks and the CSIs of the EU.

At the highest levels, we find agencies such as ENISA, EU-CERT, EC3 (European Cyber Crime Center), the European CSIRT network (Computer Security Incident Response Team), the Information Sharing and Analysis Centers (ISACs), the national agencies responsible for cybersecurity in the member states, the national contact points network for cybersecurity and critical infrastructure issues, the recently established European Cybersecurity Competence Centre and network of national centers, EU Military Computer Emergency Response Teams Operational Network (MICNET) and more. Given the interconnectedness of all digitalized systems, CSI will fall under the heading of the EU cybersecurity governance apparatus by simply being a critical component of other critical infrastructures/entities, such as in energy or finance. Other potential tools include "EU Cyber Defence Coordination Centre, the Cyber Passport, the EU Cyber Academia and Innovation Hub and the EU's Defence Hub, the European Chips Act and the Hybrid Toolbox […] aimed at enhancing cyber- and cross-sectoral resilience" (Georgescu et al., 2024).

We also find other relevant elements within European governance frameworks such as: the Cyber Resilience Act (European Parliament and Council of the European Union, 2024), the NIS 2 Directive, Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (European Parliament and Council of the European Union, 2023), the Cyber Solidarity Act (European Commission, 2023), and sectoral initiatives with relevance for space like the AI Act (European Parliament and Council of the European Union, 2024) (given future AI use within CSI), Digital Operational Resilience Act (European Parliament and Council of the European Union, 2022) (DORA, covering financial institutions), the Council Conclusions on the EU Policy on Cyber Defence (Council of the European Union, 2023).

The EU Cyber Diplomacy Toolbox is also important, since it is the framework for the EU to manage the attribution to a malicious actor of a cyber-attack against a CSI, to designate him as the perpetrator and to enact proportional sanctions with the help of partners. A second special mention goes to the EU Strategic Compass, which mentions space as a component and enabler of its priorities (Fiott, 2021).

Lastly, we have the EU-US space cooperation framework as part of the ESA-NASA cooperation and also within the Trade and Technology Cooperation Council established after the 2021 EU-US Summit (whose working groups also include vendor security issues, cybersecurity issues, emerging digital technology issues, hybrid threat protection). Also relevant is the EU-NATO Cooperation Agenda on cyber issues which encompasses cybersecurity for CSI. These ideas are summarized in Figure 3.



The EU Framework in CSI and cybersecurity

Critical Assets and Infrastructures

COPERNICUS
GALILEO
IRIS2 (GOVSATCOM)
EGNOS
EUMESAT (meteorological)
SSA Space Situational Awareness (EU and national)
Space Situational Surveillance and Tracking Launch sites (example: CSG Guiana)

Space-relevant agencies

EUSPA

ESA

DG DEFIS

National agencies

EU Satellite Center SATCEN

European GNSS Service Center

Cyber Agencies and instruments

ENISA
CERT-EU
EC3
ISACs
ECCC
CSIRT
EU Cyber Defence Coordination Centre
EEAS (through Cyber Diplomacy Toolbox)
MICNET
Hybrid Toolbox
Hybrid Rapid Response Teams

Key space legislation

EU Space Strategy for Security and Defence Regulation (EU) 2021/696

EU-ESA framework agreement

Secure Connectivity Programme

EU Space Law
Space Data Economy Strategy

Key cybersecurity legislation

CRA Directive
CER Directive
NIS 2 Directive

Regulation 2023/2841
Cyber Solidarity Act

AI Act

DORA

EU Policy on Cyber Defence

Figure 3. The EU Framework in CSI and cybersecurity

RECOMMENDATIONS FOR INCREASED CSI CYBERSECURITY AND RESILIENCE

The European Union must ensure “accessible, affordable and sustainable access to space services for European citizens and businesses as a precondition of continuity, resilience, growth and innovation” and it must also “achieve resilience to risks, vulnerabilities and threats deriving from its increasing reliance on space systems, both at the level of its militaries, and at the level of society and economy” while ensuring that the Armed Forces of the EU Member States “have safe and secure access to space services in order to maintain their qualitative edge in an environment beset by cyber and electronic warfare threats” (Thiele, 2022). Cybersecurity and cyber resilience will be important policy, technical and operational objectives.

There are two types of possible recommendations – those that pertain to the cybersecurity of CI in general and those that address CSI specifically by targeting systems, actors and processes that are part of it. Recommendations for CI cybersecurity are quite varied and have been represented strongly in scientific literature, as well as in the technical reports from the IT and cybersecurity industry. These include a focus on training and organizational security culture, raising awareness of the myriad threats especially with social engineering, threats targeting mobile devices and the new risks from “remote work” paradigms. On the technical side, experts have recommended investment (both financial and political/legislative) into centralized threat intelligence, standardized data formats, unified cybersecurity certifications, standardized update protocols and more. Other important measures can include real-time incident coordination hubs, attack alert networks (maybe even at the level of the EU) and, by integrating with new technologies, and drawing from previous chapters, we can employ AI-led automated vulnerability patching, along with cybersecurity exercises that include AI red teams.

When it comes directly to CSI, there is an important distinction to make between systems operate by EU-based entities and CSI operated by foreign entities, whether American, Chinese or any other country. The EU will find it much easier to build resilience governance for EU-based systems, especially for systems operated by or for the EU itself, such as the Copernicus

Earth Observation constellation, the Galileo global navigation satellite system, EGNOS, the European Geostationary Navigation Overlay Service, or the future GOVSATCOM secure government communications network, recently renamed as IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite). The EU could consider the following elements:

- The establishment of a dedicated ISAC for CSI which would include public and private EU operators of CSI as well as non-EU suppliers of services to the EU market, in line with the best practices recommended by the CER Directive and the NIS 2 Directive;
- The organization of cross-sector cybersecurity exercises on a regular basis incorporate elements related to the interdependencies between space and other CI sectors such as energy sectors (Yamin, Katt, and Nowostawski, 2021). The EU already organizes some space exercises, such as the Space Threat Response Architecture (STRA) (European External Action Service, 2024) exercise in the European External Action Service Headquarters in Brussels. The Space Threat Response Architecture Exercise has had six editions and is organized by the EEAS, together with the European Commission and EUSPA. The exercise tested the EU´s response capacity to a situation in which an EU space asset is subject of an attack targeting essential or critical services and concerns itself also with attribution and response in the context of the EU Cyber Diplomacy Toolbox;
- The development of a framework for a secure vendor ecosystem within the space sector in concert with partners with similar perspectives and values such as the US and the EFTA countries and in cooperation with industry associations. A sophisticated space sector will have a rich vendor ecosystem specializing in various components and processes, with many space entities acting as integrators of upstream products that consist of hardware and software, analogous to the situation in the energy sector. Having a trustworthy vendor ecosystem reduces from the start the scope of many hybrid threats related to economic warfare, cyber-attacks (especially supply chain attacks) and influence operations or ilicit technology transfers through foreign ownership of the vendors;
- The EU must accelerate the pace and the scope of its programmes to generate strategic space capabilities that enable it to replace its dependencies on non-EU owned space assets, while also controlling the level of investment in cybersecurity to maximize trust (Bucovetchi, 2020). This also falls under the rubric of "strategic autonomy".
- Better emergency access to satellite capabilities owned by other EU states through a pooling initiative similar to the Sentinel Asia initiative in Asia that Japan used when its ALOS-1 and ALOS-2 Earth Observation satellites malfunctioned during the Fukushima disaster (Caba-Maria et al., 2020). These initiatives can compensate for the deliberate or accidental disruption of critical space capabilities, especially during a crisis or emergency situation which is time sensitive.

Here, we could also add projects that raise awareness of threats to CSI among entities with critical dependencies on space services. These CI operators can diversify their providers, can implement measures to adapt to limited loss of functionality or they can even invest in alternatives to space services. For instance, entities relying on timing services from the atomic clocks on US GPS or EU Galileo satellites can buy their own atomic clock units and synchronize them online as a backup to space-based systems. Entities that require remote sensing can access existing institutional sensor networks on the ground to maintain some capabilities or they can invest in their own sensors for key areas. Satellite communications can be supplemented by fiber optics lines feeding into the public system and so on.

CONCLUSIONS

The EU has developed significant dependencies on space systems. These dependencies are founded in their critical role in facilitating dual green and energy transitions, the Energy Union, international finance and trade and much more. This role is made possible by growing satellite capabilities in remote sensing, PNT (positioning, navigation, timing), and communications. If we analyze the CER Directive and the NIS 2 Directives, we find the following: they share a taxonomy of critical European infrastructures which are all digitalized and that, in many instances, these CI systems are coordinated through upper layers of command, control and coordination systems that are space-based. Therefore, almost every terrestrial CI, from transport to energy and finance, is critically dependent on space systems. These CSI are complex and tightly integrated systems of space-based and terrestrial components, with significant exposure to the cyber threat environment. To this, we add the issue of dependence on non-European space services providers and the rapid development of the sector which is, overall, in our estimation, degrading the cyber risk profile of CSI. Space is a "contested, congested and competitive space environment" (Department of Defense and Office of the Director of National Intelligence, 2011) in which adversaries and systemic rivals are launching more and more cyber-attacks, of increased complexity, frequency and sophistication against space systems to degrade strategic capabilities and to coerce affected states into acquiescing to their demands. Not only are states developing ASAT capabilities, but they can also empower proxy actors, such as terrorist groups and organized crime entities, to initiate cyber or electronic based attacks that provide states with plausible deniability and prevent retaliation in kind.

In this environment, the EU must focus on developing strategic autonomy with regards to space capabilities in order to safeguard its economy and security, while also creating a resilience governance framework that adequately mobilizes all categories of stakeholders (including owners/operators) to improve space cybersecurity outcomes. This should include incentivizing necessary investment in resilience, rather than setting up an adversarial relationship in which the EU or Member States overregulate the security aspect and operators try to minimize their costs while complying with the letter of regulations.

The EU is also undergoing a significant development in its institutional framework which affects the topic of cybersecurity and space. Not only do we have space sector entities as critical European entities affecting two or more member states, but space systems are also included in the NIS 2 list of essential entities. The creation of EUSPA and of a General Directorate for Defense Industry and Space, to be followed soon by EU Space Law and Space Data Economy Strategy and overseen also by a new Commissioner for Defence and Space all attest to the growing importance of space in EU strategic thinking, planning and operations. The present article analyzed the high-level conceptual cybersecurity profile of critical space infrastructures. It advanced key recommendations for the EU to achieve greater resilience in the new technological, geopolitical and security context. Future research should focus on how cybersecurity can be promoted in the context of CSI specificities in operation and relative to the new trends in CI digitalization.

This article's novel contribution lies in the multi-layered profiling of cyber risks specific to CSI and the synthesis of EU-level institutional and policy developments into a unified strategic vision. By combining risk theory with institutional analysis, the paper proposes a practical roadmap toward enhancing CSI cybersecurity resilience and closing the gap between EU capabilities and governance. In doing so, it supports the Union's long-term goal of achieving strategic autonomy in space and cybersecurity.

Acknowledgement

The research for this article was conducted within the project „Resilient and Interoperable Communication Systems based on Distributed Technologies and Self-Sovereign Digital Identity (RoDID)," funded by the Advanced Research Program based on Emerging and Disruptive Technologies - Support for the Society of the Future (FUTURE TECH).

REFERENCE LIST

Acket-Goemaere, A., Brukardt, R., Klempner, J., Sierra, A., and Stokes, B. (2024) 'Space: The $1.8 trillion opportunity for global economic growth'. *McKinsey & Company*, 8 April. Available at: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-the-1-point-8-trillion-dollar-opportunity-for-global-economic-growth (Accessed: 28 March 2025)

Botezatu, U.-E. (2023) 'Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities', *Romanian Cyber Security Journal*, 5(1), pp. 67–76. Available at: https://rocys.ici.ro/documents/95/2023_spring_article_6.pdf (Accessed: 31 March 2025).

Botezatu, U.-E. (2024a) 'Space Cybersecurity: A Survey of Vulnerabilities and Threats', *Romanian Cyber Security Journal*, 6(2), pp. 53–60. Available at: https://doi.org/10.54851/v6i2y202405 (Accessed: 28 March 2025).

Botezatu, U.-E. (2024b) 'Cybersecurity in the Era of Space Domain Awareness', *Romanian Cyber Security Journal*, 6(1), pp. 29–38. Available at: https://doi.org/10.54851/v6i1y202403 (Accessed: 28 March 2025).

Bryce Space and Technology (2023) '2022 Global Space Economy at a Glance'. Available at: https://brycetech.com/reports/report-documents/Bryce_2022_Global_Space_Economy.pdf (Accessed: 28 March 2025).

Bucovetchi, O. (2020) 'Resilience of Critical Infrastructure Index Design Between Diversification and Uniformization', in *Space Infrastructures: From Risk to Resilience Governance*. IOP Publishing, pp. 57–181.

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. 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: 31 March 2025).

Caverly, R. J. (2011) 'GPS Critical Infrastructure Usage/Loss Impacts/Backups/Mitigation'. Presentation delivered on 27 April. Available at: https://www.swpc.noaa.gov/sites/default/files/images/u33/GPS-PNTTimingStudy-SpaceWeather4-27.pdf (Accessed: 28 March 2025).

Council of the European Union (2021) 'Council adopts position on €14.8 billion EU space programme for 2021-2027'. *Press release*, 19 April. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/04/19/council-adopts-position-on-148-billion-eu-space-programme-for-2021-2027/ (Accessed: 28 March 2025).

Council of the European Union (2023) 'Council Conclusions on the EU Policy on Cyber Defence'. *Official Journal of the European Union*, 22 May. Available at: https://www.consilium.europa.eu/media/64526/st09618-en23.pdf (Accessed: 31 March 2025).

Council of the European Union. (2023). *EU-NATO cooperation*. Available at: https://www.consilium.europa.eu/en/policies/eu-nato-cooperation/ (Accessed: 28 March 2025)

Department of Defense and Office of the Director of National Intelligence (2011) ‘National Security Space Strategy Unclassified Summary’. Washington, D.C. Available at: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy (Accessed: 31 March 2025).

European Commission (2022) ‘Joint Communication to the European Parliament and the Council: An EU Approach for Space Traffic Management: An EU Contribution Addressing a Global Challenge’. JOIN(2022) 4 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0004 (Accessed: 31 March 2025).

European Commission (2023) ‘Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents’. COM(2023) 209 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209 (Accessed: 31 March 2025).

European Commission (2024a) ‘The Draghi Report on EU Competitiveness’. Available at: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en (Accessed: 28 March 2025).

European Commission (2024b) ‘Mission letter to Andrius Kubilius, Commissioner-designate for Defence and Space’. Available at: https://commission.europa.eu/document/download/1f8ec030-d018-41a2-9759-c694d4d56d6c_en?filename=Mission%20letter%20-%20KUBILIUS.pdf (Accessed: 28 March 2025)

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2023) ‘European Union Space Strategy for Security and Defence’. Joint Communication to the European Parliament and the Council, JOIN(2023) 9 final, 10 March. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0009 (Accessed: 28 March 2025)

European Community and European Space Agency (2004) ‘Framework Agreement between the European Community and the European Space Agency’. *Official Journal of the European Union*, L 261, pp. 64–68. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22004A0806%2803%29 (Accessed: 28 March 2025)

European External Action Service (2024) ‘Space: EU carries out Space Threat Response Architecture 2024 Exercise (STRA-X-24)’. *EEAS*, 13 March. Available at: https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-2024-exercise-stra-x-24_en (Accessed: 31 March 2025).

European Parliament (2024) *Strategy on the Space Data Economy*. Available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-strategy-on-space-data-economy (Accessed: 28 March 2025).

European Parliament and Council of the European Union (2022) ‘Regulation (EU) 2022/2554 on digital operational resilience for the financial sector’. *Official Journal of the European Union*, L 333, 27 December, pp. 1–79. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (Accessed: 31 March 2025).

European Parliament and Council of the European Union (2022a) ‘Directive (EU) 2022/2557 on the resilience of critical entities’. Official Journal of the European Union L 333, pp. 164–198. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (Accessed: 31 March 2025).

European Parliament and Council of the European Union (2022b) ‘Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)’. *Official Journal of the European Union*, L 333, pp. 80–152. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Accessed: 31 March 2025).

European Parliament and Council of the European Union (2023) ‘Regulation (EU, Euratom) 2023/2841 on measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union’. *Official Journal of the European Union*, L 2841, 18 December, pp. 1–27. Available at: https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng (Accessed: 31 March 2025).

European Parliament and Council of the European Union (2024) ‘Regulation (EU) 2024/1689 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)’. *Official Journal of the European Union*, L 1689, 12 July, pp. 1–81. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (Accessed: 31 March 2025).

European Union (2014) ‘Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support’. *Official Journal of the*

European Union, L 158, 27 May, pp. 227–234. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014D0541 (Accessed: 28 March 2025)

European Union (2021) 'Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme'. *Official Journal of the European Union*, L 170, 12 May, pp. 69–148. Available at: https://eur-lex.europa.eu/eli/reg/2021/696/oj/eng; european-space-law.com (Accessed: 28 March 2025)

European Union (2023) 'Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027'. *Official Journal of the European Union*, L 79, 17 March, pp. 1–39. Available at: https://eur-lex.europa.eu/eli/reg/2023/588/oj/eng (Accessed: 28 March 2025).

European Space Law (2024) *European Union Space Law (EUSL)*. Available at: https://www.european-space-law.com/ (Accessed: 28 March 2025).

Fiott, D. (2021) 'Securing the Heavens: How can space support the EU's Strategic Compass?', *EU Institute for Security Studies Brief*, April. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_9_2021_0.pdf (Accessed: 31 March 2025).

Georgescu, A. (2020) 'Critical Space Infrastructures - New Perspectives on Space Policy', in Schrogl, K.-U. (ed.) *Handbook of Space Security: Policies, Applications and Programs*. 2nd edn. Cham: Springer International Publishing, pp. 227–244. ISBN: 978-3-030-23209-2.

Gheorghe, A.V., Georgescu, A., Bucovețchi, O., Lazăr, M., and Scarlat, C. (2018) 'New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk', *International Journal of Disaster Risk Science*, 9(4), pp. 555–560. Available at: https://doi.org/10.1007/s13753-018-0197-2 (Accessed: 28 March 2025).

Georgescu, A., Gheorghe, A.V., Piso, M.-I., and Katina, P.F. (2019) *Critical Space Infrastructures: Risk, Resilience and Complexity*. Topics in Safety, Risk, Reliability and Quality, vol. 36. Cham: Springer International Publishing. ISBN: 978-3-030-12603-2.

Georgescu, A., Gurău, M.M., Bucovetchi, O. and Dinu, A. (2024) 'The European Cybersecurity Framework for Critical Energy Infrastructures', in Barichella, A. and Yada, J. (eds) *The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions*. Palgrave Studies in Energy Transitions. Cham: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-031-04196-9_9-1 (Accessed: 31 March 2025).

Harrison, T., Johnson, K., Moye, J., and Young, M. (2021) 'Space Threat Assessment 2021'. Center for Strategic and International Studies, April. Available at: https://www.csis.org/analysis/space-threat-assessment-2021 (Accessed: 28 March 2025).

Organisation for Economic Co-operation and Development (OECD) (2019) *The Space Economy in Figures: How Space Contributes to the Global Economy*. OECD Publishing, Paris. Available at: https://doi.org/10.1787/c5996201-en (Accessed: 28 March 2025).

Organisation for Economic Co-operation and Development (OECD) (2024) *The Economics of Space Sustainability: Delivering Economic Evidence to Guide Government Action*. OECD Publishing, Paris. Available at: https://doi.org/10.1787/b2257346-en (Accessed: 28 March 2025).

Pulfer, R., Bucovetchi, O.M.C., and Gheorghe, A.V. (2015) 'The Governance Risk and Compliance (GRC) Model within a Dynamic Business Environment'. *Proceedings of the 26th International Business Information Management Association (IBIMA) Conference*, 11–12 November, Madrid, pp. 2651–2658. ISBN: 978-0-9860419-5-2.

Sadlier, G., Flytkjær, R., Halterbeck, M., Varma, N., and Pearce, W. (2015) 'Return from Public Space Investments: An Initial Analysis of Evidence on the Returns from Public Space Investments'. London Economics. Available at: https://londoneconomics.co.uk/wp-content/uploads/2015/11/LE-UKSA-Return-from-Public-Space-Investments-FINAL-PUBLIC.pdf (Accessed: 28 March 2025).

Thiele, R. (2022) 'Going Space – An ambitious, necessary Agenda for European Prosperity and Security'. *EuroDefense Network*, 11 September. Available at: https://eurodefense.eu/2022/09/11/going-space-an-ambitious-necessary-agenda-for-european-prosperity-and-security/ (Accessed: 31 March 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, 102450. Available at: https://doi.org/10.1016/j.cose.2021.102450 (Accessed: 31 March 2025).

Alexandru GEORGESCU is a Senior Researcher (ranked CS2 or R3) with the Department for Cybersecurity and Critical Infrastructure Protection of the National Institute for Research and Development in Informatics. He has an eclectic background, having studied Economics, then Geopolitics, and has obtained a PhD in Risk Engineering for Critical Infrastructure Systems. His PhD thesis was developed into a book published by Springer and awarded the 2020 Book prize of the International Academy of Astronautics. He is actively involved in advancing Critical Infrastructure Protection and Resilience issues through cooperation at international level and has worked on international projects for the European Space Agency and others. He was a Denton Transatlantic Fellow with the Center for European Policy Analysis in Washington DC and a Visiting Fellow with the Shanghai Institutes for International Studies. Since 2019, he is moderating a Working Group on the Protection of Defense-related Critical Energy Infrastructures within the European Defence Agency's Consultation Forum for Sustainable Energy in the Security and Defence Sectors. In this position, he has contributed to policy documents, project proposals and studies on Critical Infrastructure Protection, including from the perspective of cyber resilience and hybrid threats. He is affiliated with the Romanian Association for the Promotion of Critical Infrastructure Protection, with the Romanian Association for Space Technology and Industry and is the Secretary General of Eurodefense Romania.

Andreea DINU is the Head of the Cybersecurity Department at the National Institute for Research and Development in Informatics – ICI Bucharest. She brings extensive expertise in cybersecurity for critical infrastructure, with a strong focus on ensuring the resilience and security of essential systems against advanced and emerging cyber threats. With a solid technical background, Andreea has been actively involved in numerous national and international research projects spanning cybersecurity, artificial intelligence, high-performance computing, and quantum computing. Her work has resulted in a wide range of scientific publications that demonstrate her significant contributions to advancing these fields. In addition to her technical and research achievements, Andreea is engaged in cyber diplomacy, supporting international collaboration, policy alignment, and trust-building in the digital space. She contributes to shaping cybersecurity strategies that reflect both national interests and global stability.