The Cybersecurity Profile of Critical Space Infrastructures – Key Concepts, Trends, and Frameworks

Clara COTRONEO[1], Adrian-Victor VEVERA[2]
[1]Global Governance Institute
[2]National Institute for Research and Development in Informatics - ICI Bucharest
C.cotroneo@globalgovernance.eu, victor.vevera@ici.ro

Abstract: Space systems are a key enabler for a wide variety of applications that are critical to infrastructure functioning. This has led to an evolving approaches to their security, including also their identification and designation as critical infrastructures within existing Critical Infrastructure Protection frameworks, including the latest EU efforts such as the Critical Entity Resilience Directive. At the same time, the requirements of space systems entail significant digitalization of these systems and of any critical infrastructure that uses them, especially if they are so integrated that we can say they are critically reliant on them. This raises the issue of cybersecurity for critical space infrastructures in the new security environment. This article traces the main factors leading to a worsening cybersecurity environment for space systems, and especially the impact of emerging digital technologies.
Keywords: space systems, resilience, cybersecurity, critical infrastructures, emerging digital technology.

INTRODUCTION

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 Aerospace, 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., 2018). The space economy encompasses the entirety of the research and development, manufacturing, launch, operation, and decommissioning of space services, including ground elements (OECD, 2019). It is a complex domain which is undergoing explosive growth due to technological change, economies of scale and a new space race between superpowers, as well as new country entrants into the space sector and corporations vying to achieve new capabilities.

https://doi.org/10.54851/v7i1y202502

From a critical infrastructure protection (CIP) perspective, space systems have become a key enabler for the functioning of numerous critical infrastructure (CI) sectors (Gheorghe et al, 2018). They achieve this based on progress in their capability, capacity, affordability, and availability. These capabilities, includinge command, control, coordination, communication, and data gathering capabilities are used in everything from the critical energy sector to the critical transport sector. Figure 1 presents one example, drawn from industry literature, illustrating the impact of global navigaition satellite system (GNSS), on various CIs.

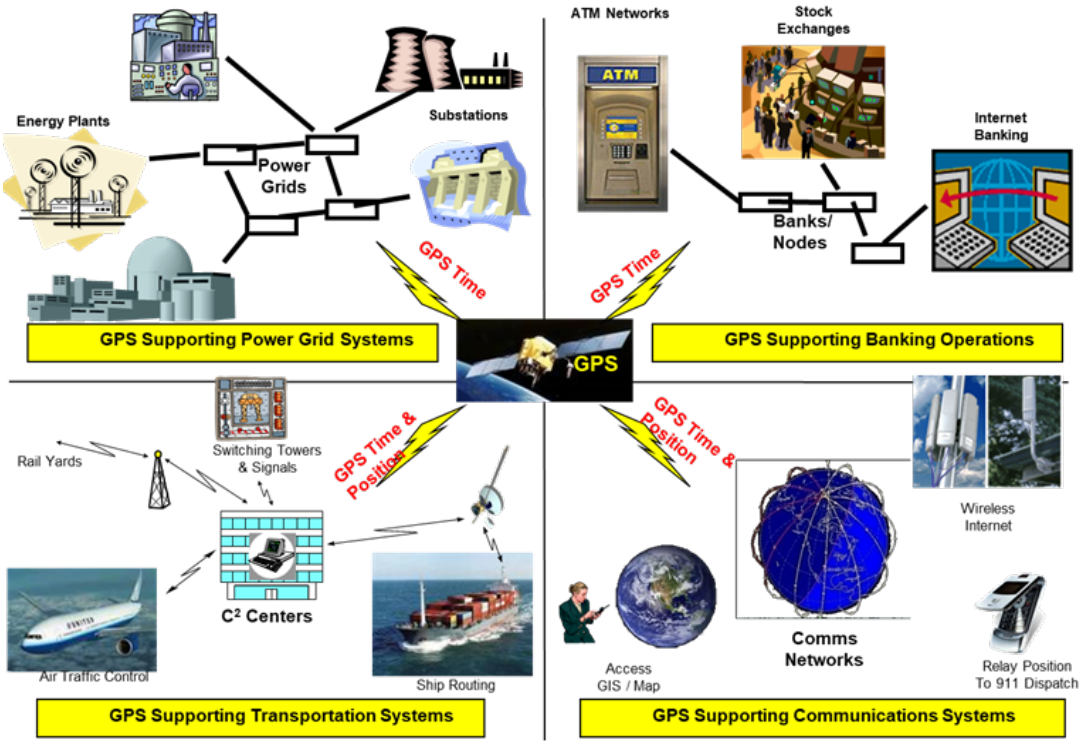

Figure 1. *The use of GNSS services in CI operation (source: Caverly, 2011)*

Infrastructures are composed of assets, systems, resources, and operating entities, and they produce goods and services while facilitating the operation of key societal functions in the economic, social, political or security realm (Georgescu & Bucovetchi, 2023). They are critical when their disruption or destruction would cause significant loss of human life, material damage, and loss of functionality. Some researchers have argued an additional critical infrastructure sector has emerged, that is critical space infrastructure (CSI) (Georgescu et al, 2019). CSI are identified as critical in the EU Directives, the Critical Entities Resilience Directive (CER) and the NIS 2 Directive. However, their functioning relies on digitalized and networked systems that enable them to provide critical services and functionality. The more developed the dependency on space systems on the part of a CIs, the more likely it is that they have been thoroughly digitalized and are therefore reliant on cyber systems for their critical functions. Working as part of a system-of-systems with CSIs also as a component (Gheorghe et al, 2018), this creates a significant exposure to cybersecurity threats, as well as to normal accidents arising from the complexity of these systems (Botezatu, 2024). In the current security environment, there are several sustainability issues in play for CSI, which threaten their operation globally and, by extension, can have significant cross-border impact on CIs (OECD, 2024; Sanchez et al., 2020). One of these issues is cybersecurity in the context

not only of growing cybercriminal activity, but also of growing competition between states which incentivizes hybrid attacks on CIs and a new focus on space security issues and space disruption (OECD, 2024).

The present article explores the issue of the deteriorating cybersecurity environment for CSI, drawing on the specialty literature to distill key factors and specificities affecting the space environment, to highlight differences from terrestrial infrastructures and to anticipate the possible directions of these security evolutions. Special attention is paid to the impact of the adoption of emerging digital technologies on CSI, with concrete proposals on a case-by-case basis to ameliorate the resulting issues.

THE DETERIORATING CYBER THREAT ENVIRONMENT

We have witnessed a severe deterioration of the cyber threat environment for CI in general and CSI in particular in recent years. This means that more potential attackers have the means to perpetrate cyberattacks, the motivation to do so and the specific knowledge required. The war in Ukraine is likely a catalyst for growing awareness of critical space dependencies, given the role of the Starlink wireless satellite communication in the effectiveness of the Ukrainian defense efforts (Georgescu, 2025). To this, we add the significant growth of the space economy as a pull-factor for greater cyber threats geared not just towards disruption but also profit extraction.

The growing inter-state competition in space is another important factor, since it has led to a high-profile race to develop (and irrefutably demonstrate) anti-satellite or ASAT capabilities beyond cyber-attacks, including electronic attacks, directed energy attacks and kinetic attacks (the most popular for state power establishment (Defense Intelligence Agency, 2022). The war in Ukraine has also showed that there is growing rhetoric designating space systems as legitimate targets of war to degrade military operations, even if these systems are dual-use and civilian entities also rely on them (Georgescu, 2025). Similarly, civilian preparedness and protection are increasingly reliant on space systems: examples are space-based technologies for early warning systems or the EU ESA's ARTES 4.0 programme for the deployment of space assets based applications for environmental surveillance, civil protection and border control. This matches the trend towards the normalization of hybrid disruption of civilian CIs in energy, transport, and more, even those that are not in active war zones.

A 2019 US Defense Intelligence Agency reported that "foreign governments are developing capabilities that threaten others' ability to use space [...] China and Russia, in particular, have taken steps to challenge the United States [...] [China] continues to improve its counterspace weapons capabilities and has enacted military reforms to better integrate cyberspace, space, and EW into joint military operations" (Defense Intelligence Agency, 2019). One study stated that "operations are reliant on the adequate provisioning of critical space services, and adversaries seek to disrupt this access in order to limit [...] capabilities, hamper the fulfilment of core missions and hinder active operations" (Tatar et al., 2020).

Military and security planners must contend with state actors generating "gray zone threats" and evading attribution or military responses through "measures under the threshold of war" while still aiming to severely disrupt CSI operation for military, economic and strategic reasons (Robinson et al., 2019). These measures are flexible enough to be activated on short notice against targets of opportunity to generate damage in very specific circumstances, such as by denying access to space services for a country in a crisis and emergency situation generated, for instance, by a natural disaster (Caba-Maria et al., 2020).

Even if they do not use them, states develop counterspace capabilities and advertise their existence through declarations or visible tests such as ASAT tests or, for instance, the famous "nesting satellites" of Russia where one system conceals another that can detach, perform a mission and then return, or the maneuvering satellites of China which have approached several Western satellites and also the International Space Stations. These are not just physical threats, because proximity enables

electronic and cybersecurity threats through jamming, signal duplication and manipulation, forced connections and entry through wireless connections (Harrison et al., 2022).

The war in Ukraine has seen an acceleration of these trends, with Ukraine being the target of hybrid actions between the 2014 invasion that stalled and the 2022 invasion. These hybrid actions continued and were paired with conventional attacks on CI following the 2022 invasion (Cotroneo & Leonard, 2025). Ukraine's partners were also targeted for hybrid action against CI in order to generate loss of capabilities, economic damage and to deter assistance to Ukraine (Georgescu, 2025).

This phenomenon affected CSI, with several examples listed below (Harrison et al., 2022):

- Constant reports of jamming of radio, cell, and satellite signals in Ukraine;
- Commercial jammers that look like everyday objects identified in China, including jewelry and USB sticks (12 March 2021, China);
- GPS jamming of OSCE mission utilizing UAVs in Ukraine to monitor Russian build-up (6 April 2021, Russia);
- Cyprus-flagged oil tanker Berlina spoofed its own GPS-backed automatic identification system (AIS) signal in order to evade sanctions and transport illegal oil from Venezuela (28 May 2021);
- The GPS systems of a UK Royal Navy destroyer and a Dutch Royal Navy ship moored in Odessa during a NATO mission were falsified via spoofing to appear to be in Crimea (17 June 2021, Russia);
- A US Navy destroyer was spoofed to appear to be near Crimea rather than near Ukrainian held waters (30 June 2021, Russia);
- Instructions for GPS spoofing found online (25 September 2021);
- Chinese satellite SJ-21 launched in October 2021 performed exercises in orbital positioning with another unidentified system (01 November 2021, China);
- New facilities for electronic warfare built on Hainan Island (21 November 2021, China);
- An undersea cable between Norway and the Svalbard archipelago was severed. The state company Space Norway AS maintains the fiber-optic cable and operates the Svalbard Satellite Station. There was redundancy in place and the cable was repaired by 21 January 2022 (7 January 2022);
- Suspected hack of Viasat ground terminals in Eastern Europe, including Ukraine, on the day of the Russian invasion (24 February 2022). Later that year, a Russian official at the United Nations referred twice to "quasi-civilian" commercial satellites used for military purposes which "may become a legitimate target for retaliation". This was in direct reference to the Starlink system;
- In February 2022, Christopher Scolese, the then director of the US National Reconnaissance Office, advised satellite system operators to "ensure that your systems are secure and that you're watching them very closely because we know that the Russians are effective cyber actors" (Erwin, 2022);
- Russia added to its signals intelligence (SIGINT) capabilities by launching two more satellites in 2021 for the Liana constellation and by building the Sledopyt ground system to intercept radio communications from satellites orbiting above Russian territory.

CSI ARCHITECTURE CHANGES IN MORPHOLOGY AND TOPOLOGY

The use of new technology within CI systems-of-system can result in the radical reorganization of the system topology. As we will see in a later section, the use of blockchain technology in CSI can result in the elimination of ground control and telemetry stations (J.P. Morgan, 2021), (SimpleSwap, 2024). This is just one factor that can radically reorganize CSI and shift the architecture of individual systems, in response to new technologies, new capabilities, new demands and new economic factors.

New components can also appear in the CSI, such as high-altitude communications platforms complementing orbital ones or increasingly automated ground stations located in remote positions with their own security challenges. For instance, the growing number

of polar and Molnyia orbit satellite systems along with Sun-synchronous systems both for scientific research as well as military and dual-use applications has led to an increase in the number of Arctic telemetry and control stations for these systems. An example is the Pituffik Base of the US in Greenland (formerly Thule Base), which is today a Space Force Base dedicated primarily to the management of space components of C4ISTR systems (Airforce Technology, n.d.). This is a critical US base and the most Northern one it possesses, which is one of the reasons for the 2019 and 2025 Trump campaigns to acquire Greenland from Denmark. China's space partnerships also involve arctic satellite control centers (Robinson et al., 2019).

We are also seeing new space architecture in line with new demands and new capabilities. 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). Many of these satellites are quite small, trading size, resilience and functionality for network redundancy and variety, but nevertheless capable through advances in miniaturization. They range from smallsats to cubesats and nanosats (Georgescu et al., 2019). The most famous and extensive constellation is Starlink by SpaceX whose standard satellite class weighs just under 200 kg. This differs from the previous approach, where specialized research and development centers or contractors designed custom hardware and software systems in limited numbers for highly specific missions. These systems featured redundancies and shielding to enhance longevity and withstand the harsh conditions of space but were not necessarily well protected against cyber threats or intentional attacks. There are different reasons why commercial satellites are more vulnerable to cyber attacks than governmental ones, including:, their wider connectivity, reduced attention to cyber-security during the design phase, less careful control over supply chain and vendor security, a wider variety of users, less attention paid to active and passive security measures, operator security culture gaps and more (Georgescu et al., 2019). The new satellites are (Bryce Aerospace, 2022):

- Much smaller, launched 60 or more at a time if using a normal sized rocket;
- Much more numerous;
- Much easier to replace;
- Much less capable overall;
- Fewer redundant systems;
- Utilizing commercial-off-the-shelf hardware and software (COTS).

In 2023, 2,860 smallsats were launched (Bryce Aerospace, 2024). These satellites now represent 90% of all launches and are a big reason for the rapid increase in the total number of satellite systems in recent years, as seen in table 1. Despite their lower capabilities, their sheer numbers and the adaptability of their platforms mean that many of these satellite constellations can become critical providers of services for commercial, civilian, and military actors. For instance, commercial space has become "a great equalizer,

Table 1. *Union of Concerned Scientists Open Source Satellite Database (Union of Concerned Scientists, 2025)*

Satellite Quick Facts (01.05.2023 compared to 31.03.2019)			
Total number of operating satellites: 7,560/2,062			
United States: 5,184/901	Russia: 181/153	China: 628/299	Other: 1,572/709
LEO: 6,768/1,338	MEO: 143/125	Elliptical: 59/45	GEO: 590/554
Total number of US satellites: 5,184/901			
Civil: 30/38	Commercial: 4,741/523	Government: 167/164	Military: 246/176

allowing Ukrainian forces to have the necessary intelligence, surveillance, and reconnaissance and command and control to better understand Russian force disposition, communicate and stay connected globally, and strike with precision" and the war in Ukraine has been dubbed the first "commercial space war"; even the Wagner mercenary group is known to have purchased imagery from Chinese company Spacety to support combat operations in Ukraine (Center for Strategic and International Studies, 2023). Estimates for 2024 ranged from 10,000 to 14,000 satellites in orbit (ABI Research, 2024). By January 2025, the Starlink megaconstellation that is also in use by the Ukrainian military consisted of 6,874 active satellites with another 100 inactive (Space.com, 2025). By 2032, it is estimated that there will be 480 yearly launches servicing an inventory of 43,000 satellites (ABI Research, 2024).

Other design changes with impact on CSI vulnerability to cyber attacks will become apparent with time. For instance, the above mentioned wide connectivity means that we can see growing use of wireless communications between system components on satellite platforms to minimize physical connections and to reduce the number of vulnerable components to the hazards of the space environment. This is already happening on Earth in offshore critical infrastructures to minimize entry points for corrosive salt water. In an Internet-of-Things paradigm, CI operators can include thousands if not millions of sensors and minimize costs through wireless communications to reduce the cost of cabling and of retrofitting old facilities. This introduces both the prospect of jamming, as well as intrusion points for attackers through the wireless network.

COTS is a major source of cybersecurity issues for CSI, which is also a trend for CIs in general (Falco, 2018). According to Nussbaum & Berg (2020), the use of COTS introduces new vulnerabilities to space infrastructure, including for the already mentioned small satellites. The previously developed bespoke systems had "security through obscurity", where potential attackers were stymied by one-of-a-kind or limited run hardware and software in dedicated architectures requiring significant documentation to understand. The potential for infiltration and damage was much lower because of this barrier to attacker knowledge. Newer systems trade this security for efficiency, cost-effectiveness and higher capabilities from commercial products that have a wider market and a correspondingly higher development budget and update cycle. We are at the point where smallsats are running Android variants, the same operating system powering 90% of the world's smartphones, almost all the components are mass market or rugged versions of mass market products, and many software elements come from open-source libraries. The 2023 hacking of an ESA nanosatellite shows how vulnerable these COTS-based systems are, especially since the use of COTS products, including open-source libraries, means that the skillsets and competencies of hackers are transferable from one system to another, even in radically different fields (Interesting Engineering, 2023). The use of COTS elements also involves the inadvertent inclusion of vulnerabilities from back doors, day-one hacks, and other security issues the product line faces. Some of the components have software elements which are also unpatched and unpatchable and are meant to be replaced in low timeframes rather than having software updates, which can lead to growing risk as attackers become more familiar with the vulnerabilities. For satellites, these include sensor systems, but terrestrial CI (including terrestrial components of CSI such as ground stations) can install vulnerable systems through inclusion of Wi-Fi controlled LED lighting systems, smart appliances for kitchens and support facilities, or smart versions of heating-ventilation-air conditioning (HVAC) systems.

EMERGING TECHNOLOGY IMPACT ON CYBERSECURITY IN CSI

This section presents a non-exhaustive emerging digital technology that affects the cybersecurity systems of CSI.

Artificial Intelligence Uses in CSI

The various types of AI systems or techniques have been described as having transformative potential in all industries and across many

walks of life (Schmidt, 2021). They have the potential to reorganize complex systems and their operating organizations, leading to an even greater degree of automation than is already practiced, and edging from decision-support mechanisms to automated decision-making mechanisms. The cybersecurity impact of AI adoption is, consequently, estimated to be at a very high level (Brattberg, Csernatoni and Rugova, 2020).

CSI can integrate AI in numerous areas because of the high level of automation and digitalization of CSI functioning. AI may have the following roles:

- resilience-by-design in CSI systems;
- industrial control system coordinator for complex and distributed CSI;
- coordinator of important secondary functions such as threat identification and response coordination for cyber-attacks;
- an AI agent can also serve as a liaison between different entities and systems in the information and decision-making flow of CI systems-of-systems.

For instance, the interaction between the critical energy infrastructures, which will integrate AI for industrial control systems, grid management, predictive maintenance and more, and the CSI will necessitate interaction with AI systems powering CSI in order to benefit from the same speed and capacity of decision-making and data analysis. These evolutions will increase efficiency and output, while decreasing cost per output, however they will also entail cybersecurity risks stemming from AI use. These are very diverse and our knowledge of them is continuously evolving. They encompass both deliberate disruption of normal AI functioning, as well as defects in the functioning of the AI systems. They include dataset poisoning, model extraction and IP theft, disruption of mission critical systems leading to loss of functionality, data manipulation and compromised decision chains (Sambucci and Paraschiv, 2024). The "black box" nature of AI systems leads to skill gaps and lack of capacity within organizations to properly assess risks, defend against attacks and restore functionality.

AI can also be used by attackers as a tool to enable new cybersecurity threats (Sambucci and Paraschiv, 2024). For example, AI can enhance system probing, automate and refine cyberattacks, adapt to defensive measures, and generally increase the sophistication and complexity of attacks. Independently of a particular cyber-attack, AI can be used to scan software databases to identify vulnerabilities and backdoors that can be used for any number of future attacks on CSI or other CI (Sambucci and Paraschiv, 2024). AI can also be used to facilitate other forms of cyberattacks and vulnerability exploitation – personalized phishing campaigns, criminal Large Language Models that can produce harmful and disruptive content, including facilitating the writing of dedicated malware for specific systems such as CSI and deepfake technology to enable social engineering for attacks.

Conversely, these same AI capabilities can be leveraged for defense, helping to counter cyberattacks, detect AI-generated content used in social engineering or deepfake operations, and identify and resolve vulnerabilities in software libraries and databases. The same efforts at regulating AI and the impact of AI on cybersecurity are also relevant to mitigating the impact of AI adoption on CSI. While the Trump Administration has elected to rescind the Biden-era "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence", other governance elements such as voluntary AI codes, agency and department-level regulations and programs for international coordination remain. The main European elements for AI governance are the AI Act (European Union, 2024), the Coordinated Plan on Artificial Intelligence (European Commission, 2018), and various ancillary elements such as voluntary standards and codes of conduct like the four-point risk scale for AI applications developed by a dedicated high-level expert group on AI in the EU (European Commission, 2019). Many 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). For the EU, the overarching formula used is "ethical and trustworthy AI". As for the other digital emerging technologies on the list, cybersecurity framework elements in the EU also apply such as the NIS 2 Directive and the Cyber Resilience Act.

Blockchain Technology Use

Distributed Ledger Technology (DLT) or Blockchain is seeing increased use in applications not related to cryptocurrencies and financial products. With the technology just now edging towards mass applications, regulation and legitimacy, we are seeing more and more use cases being developed, including in origin control for supply chains, maintenance system management, access management for users and differential access to data and privileges, auditing and transparency systems and the reinforcement of privacy and commercial secrets (Georgescu and Cirnu, 2019). Distributed ledger technology can make a valuable contribution to CSI through the decentralization that it affords, and which can have a significant cybersecurity impact (Wainscott-Sargent, 2019). On the economics side, blockchain use can generate new efficiencies – the entire supply chain for CSI can be run on the blockchain, with security and transparency; DLT can also reduce latency in communications through the elimination of centralized ground control infrastructure (itself a cybersecurity risk point) (J.P. Morgan, 2021), (SimpleSwap, 2024). It can enable more efficient allocation of CSI capabilities (such as in constellations) both in an economic and operational sense (IBM, 2019), while improving maintenance processes and providing added transparency and auditing capacity (through on-chain analysis and blockchain intelligence in the wider sense but also preserving privacy through the use of encryption keys). Experiments with DLT in satellites have proven the ability to use multi-access user communication to enable finetuning of system access by administrators, while the use of smart contracts provides an added layer of responsive use of CSI capacity with lower costs (Mital et al., 2018). Zero trust architectures are also necessary in the more crowded field of space services users. On another level, given the hesitation of various organizations in sharing datasets, an intersection between blockchain and AI can enable the secure sharing of machine learning parameters while maintaining data access privileges (Jones, 2023). This enables more collaborative work in fields such as Earth Observation while preserving access to proprietary data (Mital et al., 2021). The use of blockchain technology holds the promise of preventing "single point of failure" events through decentralized architectures, greater data integrity and auditability, more secure software updates, all of which improve cybersecurity outcomes (Decent Cybersecurity, 2024).

Operationally, blockchain will be especially useful in the context of the increase in the number of mega-constellations made up of numerous, cheap, standardized satellites such as nanosats (Jones, 2023).

However, we should not discount 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, centralized blockchain networks running proof-of-authority algorithms with a much smaller number of validation nodes makes it more likely that a brute force attempt can compromise their functioning and introduce numerous possibilities of sabotage into the system (Vacusta and Nica, 2023).

Quantum Computing

Commercial quantum computing capabilities, which are closer and closer to becoming a reality, can represent a major threat to CSI, since secure telecommunication is a critical link between CSI components, as well as facilitator of the production of critical goods and services in CI sectors that integrate CSI. Quantum computers will be able to solve problems that are far too complex for classical computer architectures, and this includes solving the algorithms behind encryption keys that protect our data

and the Internet's infrastructure (Laing and Charles, 2024). While the available hardware is not yet fulfilling its promise to render current encryption obsolete, it is only a matter of time, given hardware advances, so much so that cyber criminals are now using data-theft strategies such as "Harvest Now, Decrypt Later", where they steal encrypted data on purpose in the hope that it is still relevant by the time they have access to quantum decryption capabilities that can deliver the data (European Parliamentary Research Service, 2024). An analysis by consulting company Booz Allen Hamilton predicted, under an optimistic scenario, that current standard encryption technique will be breakable in the 2027-2030 interval and a consensus view has it happening between 2030 and 2040 (Townsend, 2022), (Parker, 2023). "Quantum transition" strategies will be necessary at the level of CSI or of larger CI incorporating them in order to address the security impact of commercially available quantum decryption, combined AI-quantum security threats, and other issues. Such a strategy would identify not just intermediate measures using existing technologies (zero-trust architectures, offline backups, greater key sizes etc.) until "quantum safe" products and services are available (Deloitte, 2022). The ideal is to achieve quantum-secure status, where the encryption becomes unbreakable in a usable timeframe even by quantum computers, if that is even possible. Already, the U.S. National Institute of Standards and Technology (NIST) is evaluating 69 potential new methods for what it calls "post-quantum cryptography (PQC)" (NIST, 2023). NIST released its first four quantum-proof algorithms in July 2022. However, soon after that, CRYSTALS-Kyber public-key encryption and key encapsulation mechanism that had been recommended by NIST had been broken using AI technology combined with side-channel attacks (Townsend, 2023).

CONCLUSIONS

Space systems are critical enablers for military and civilian infrastructures, including governmental and commercial systems-of-systems taking advantage of the often-unique capabilities that these systems possess in terms of data gathering, timing, positioning and more. Many frameworks now recognize them as critical infrastructures in themselves. Given the digitalization of both CSIs and CIs in general, cybersecurity is very important for the overall resilience profile of our societies and CSIs are increasingly targeted by malicious actors, including state-backed actors, in order to disrupt, degrade or undermine the functioning of CSIs. This article focuses on CSI-specific factors in the evolution of the cybersecurity threats to CIs, including through the adoption of emerging digital technologies. Future research should address resilience-enhancement measures in the context of these changes and their practical implementation in the unique context of space system operation, including in political, ownership and governance dimensions.

ACKNOWLEDGEMENT

This research was made possible partially through the support of the RO-CCH project, which provided valuable direct data on the current cybersecurity maturity level of the Romanian healthcare institutions. The authors would like to extend their gratitude to all the healthcare organisations and experts who participated in the surveys and shared their insights.

REFERENCE LIST

ABI Research. (2024) *Over 480 orbital launches and 43,000 active satellites expected by 2032.* https://www.abiresearch.com/press/over-480-orbital-launches-and-43000-active-satellites-expected-by-2032/ [Accessed 25th March 2025].

Airforce Technology. (n.d.) *Thule: Inside the US military base in Greenland.* https://www.airforce-technology.com/features/thule-military-base-in-greenland/ [Accessed 25th March 2025].

Bingen, K. A., Johnson, K., Young, M. (April 2023) *Space threat assessment 2023*. Washington, Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2023

Botezatu, U.-E. (2024) Space cybersecurity: a survey of vulnerabilities and threats, *Romanian Cyber Security Journal*, 6(2), 53–60. doi: org/10.54851/v6i2y202405.

Brattberg, E., Csernatoni, R. & Rugova, V. (2020) *Europe and AI: Leading, lagging behind, or carving its own way?* Carnegie Europe, 9 July. https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236 [Accessed 28th March 2025].

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

Bryce Aerospace. (2022) *Smallsats by the numbers 2022*. https://brycetech.com/reports/report-documents/Bryce_Smallsats_2022.pdf [Accessed 25th March 2025].

Bryce Aerospace. (2024) *Smallsats by the numbers 2024.* https://brycetech.com/reports/report-documents/Bryce_Smallsats_2024.pdf [Accessed 25th March 2025].

Caba-Maria, F., Georgescu, A., Mureșan, L. &Mușetescu, R.C. (coord.) (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. 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 25th March 2025].

Caverly, R.J. (27 April 2011) *GPS critical infrastructure usage/loss impacts/backups/mitigation.* https://www.swpc.noaa.gov/sites/default/files/images/u33/GPS-PNTTimingStudy-SpaceWeather4-27.pdf [Accessed 25th March 2025].

Cookson, C. (11th July 2016) *Nano-satellites dominate space and spread spies in the skies*, FT Research. https://www.ft.com/content/33ca3cba-3c50-11e6-8716-a4a71e8140b0 [Accessed 25th March 2025].

Decent Cybersecurity (2024) *Blockchain in the Stratosphere: Pioneering the Future of Software-Defined Satellites.* https://decentcybersecurity.eu/blockchain-in-the-stratosphere-pioneering-the-future-of-software-defined-satellites/ [Accessed 28th March 2025].

Defense Intelligence Agency. (2019) *Challenges to security in space.* https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf [Accessed 25th March 2025].

Defense Intelligence Agency. (2022) *Challenges to security in space*. Washington, DC: Defense Intelligence Agency. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf [Accessed 25th March 2025].

Deloitte. (2022) *Future Forward Readiness: Quantum Risk.* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-future-forward-readiness-quantum-risk.pdf [Accessed 28th March 2025].

European Commission. (2018) *Coordinated Plan on Artificial Intelligence.* COM(2018) 795 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0795 [Accessed: 28 March 2025].

European Commission. (2019) *Ethics guidelines for trustworthy AI.* High-Level Expert Group on AI, European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai [Accessed 28th March 2025].

European Parliamentary Research Service. (2024) *Cryptographic security: Critical to Europe's digital sovereignty.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf [Accessed 28 March 2025].

European Union. (2024) *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 various regulations and directives (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [Accessed 28 March 2025].

Erwin, S. (2022) NRO warns satellite operators of possible Russian attacks, *SpaceNews*, 23 February. https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-asukraine-crisis-unfolds/ [Accessed 25th March 2025].

Falco, G. (2018) *Job One for Space Force: Space Asset Cybersecurity*. Cyber Security Project, Belfer Center, Harvard University, 12 July. https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity [Accessed 28th March 2025].

Georgescu, A. (2022) Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic example, *International Journal of Cyber Diplomacy*, 3, 13–22. doi: org/10.54852/ijcd.v3y202202

Georgescu, A. (2025) A critical infrastructure protection perspective on the conflict in Ukraine: recommendations for a resilient post-war Ukraine, in Nate, S. (ed.) *Ukraine's journey to recovery, reform and post-war reconstruction*. Cham: Springer (Contributions to Security and Defence Studies). doi: org/10.1007/978-3-031-66434-2_19

Georgescu, A., Bucovețchi, O. (2023). *Critical Infrastructure Protection – conceptual approaches.* Editura SITECH, ISBN 978-606-11-8547-4, Craiova, Romania.

Georgescu, A. and Cirnu, C.E. (2019) Blockchain and critical infrastructures – challenges and opportunities, *Romanian Cyber Security Journal*, 1(1), 93–100.

Georgescu, A., Gheorghe, A., Piso, M.-I. & Katina, P.F. (2019) *Critical space infrastructures: risk, resilience and complexity. Topics in Safety, Risk, Reliability and Quality,* Series 36. eBook ISBN: 978-3-030-12604-9. [Accessed 28th March 2025].

Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., & 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, 555-560.

Harrison, T., Johnson, K., O'Connor, A. and Young, M. (2022) *Space threat assessment 2022.* Washington, DC: Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220404_Harrison_SpaceThreatAssessment2022.pdf?K4A9o_D9NmYG2Gv98PxNigLxS4oYpHRa [Accessed 28th March 2025].

IBM. (2019) *Space tech: Transforming satellite launches with blockchain.* https://www.ibm.com/think/insights/space-tech-transforming-satellite-launches-with-blockchain [Accessed 28th March 2025].

Interesting Engineering. (2023) *Cybersecurity researchers gain control of ESA nanosatellite in an ethical hacking exercise.* https://interestingengineering.com/culture/hackers-gain-control-esa-nanosatellite [Accessed 28th March 2025].

Jones, H. (2023) *Revolutionizing Satellite Security: NASA's Groundbreaking Project to Integrate AI, Blockchain & Nanosatellites.* Forbes, 16 November. https://www.forbes.com/sites/hessiejones/2023/11/16/revolutionizing-satellite-security-nasas-groundbreaking-project-to-integrate-ai-blockchain--nanosatellites/ [Accessed 28th March 2025].

J.P. Morgan (2021) *Onyx by J.P. Morgan launches blockchain in space.* https://www.jpmorgan.com/technology/news/blockchain-in-space [Accessed 28th March 2025].

Laing, T. & Charles, T. (2024) *Anticipating the Quantum Threat to Cryptography*. HP Wolf Security Blog, 21 February. https://threatresearch.ext.hp.com/anticipating-the-quantum-threat-to-cryptography/ [Accessed 28th March 2025].

Mital, R., de La Beaujardiere, J., Mital, R., Cole, M., & Norton, C. (2018) *Blockchain application within a multi-sensor satellite architecture*. NASA Technical Reports Server. https://ntrs.nasa.gov/api/citations/20180006549/downloads/20180006549.pdf [Accessed 28th March 2025].

Mital, R., de La Beaujardiere, J., Cole, M., & Norton, C. (2021) *Blockchain Use Case in Multi-sensor Satellite Architecture. IEEE Aerospace Conference.* https://ieeexplore.ieee.org/document/9581969 [Accessed 28th March 2025].

National Institute of Standards and Technology - NIST. (2023) *NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers.* https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers [Accessed: 28th March 2025].

Nussbaum, B. & Berg, G. (2020) Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure. *In Space infrastructures: From risk to resilience governance*. IOS Press. pp. 91-99.

OECD. (2019) The space economy in figures: how space contributes to the global economy. Paris, *OECD Publishing.* doi: org/10.1787/c5996201-en

OECD. (2024) *The economics of space sustainability.* https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-economics-of-space-sustainability_5236a39b/b2257346-en.pdf [Accessed: 28th March 2025].

Parker, E. (2023) When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret. *RAND Corporation,* 13 September. https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html [Accessed: 28 March 2025].

Robinson, J., Robinson, R., Davenport, A., Kupkova, T., Martinek, P., Emmerling, S. & Marzorati, A. (2019) *State actor strategies in attracting space sector partnerships: Chinese and Russian economic and financial footprints.* Prague: Prague Security Studies Institute. http://www.pssi.cz/download/docs/686_executive-summary.pdf [Accessed: 28 March 2025].

Sadlier, G., Flytkjær, R., Halterbeck, M., Varma, N. & Pearce, W. (2018) *Return from public space investments: an initial analysis of evidence on the returns from public space investments.* London: London School of Economics. https://londoneconomics.co.uk/wp-content/uploads/2015/11/LE-UKSA-Return-from-Public-Space-Investments-FINAL-PUBLIC.pdf [Accessed 28th March 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), 131–148. doi: org/10.33436/v34i3y202410

Llopis Sanchez, S., Mazzolin, R., Kechaoglou, I., Wiemer, D., Mees, W. & Muylaert, J. (2020) Cybersecurity space operation center: Countering cyber threats in the space domain. *Handbook of Space Security: Policies, Applications and Programs* (pp. 921-939). Cham: Springer International Publishing.

Schmidt, E. (coord.) (2021) *Final Report - National Security Commission on Artificial Intelligence.* NSCAI, Washington, DC, US. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf [Accessed: 28th March 2025].

SimpleSwap (2024) *The Use of Blockchain Technology in Satellite Communication*. https://simpleswap.io/blog/the-use-of-blockchain-technology-in-satellite-communication [Accessed 28th March 2025].

Space. (2025) *Starlink satellites: Facts, tracking and impact on astronomy.* https://www.space.com/spacex-starlink-satellites.html [Accessed 28th March 2025].

Tatar, U., Gheorghe, A.V., Keskin, O. & Muylaert, J. (eds.) (2020) *Space infrastructures: from risk to resilience governance. Amsterdam: IOS Press* (NATO Science for Peace and Security Series D: Information and Communication Security, vol. 57). ISBN: 978-1-64368-073-6.

Townsend, K. (2022) *Quantum Computing Is for Tomorrow, But Quantum-Related Risk Is Here Today*. SecurityWeek, 3 January. https://www.securityweek.com/quantum-computing-tomorrow-quantum-related-risk-here-today/ [Accessed 28th March 2025].

Union of Concerned Scientists. (2025) UCS Satellite Database. https://www.ucsusa.org/resources/satellite-database [Accessed 28th January 2025].

Vacusta, B. & 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), 65–74. doi: org/10.54851/v5i2y202307 [Accessed 28th March 2025].

Wainscott-Sargent, A. (2019) Blockchain: The Next Big Disruptor in Space. *Via Satellite*. https://interactive.satellitetoday.com/blockchain-the-next-big-disruptor-in-space/