AI-Driven space security: Future trends and strategic imperatives for critical infrastructures

Ulpia-Elena BOTEZATU[1,2], Ella-Magdalena CIUPERCĂ[1]

[1] National Institute for Research & Development in Informatics – ICI Bucharest, Romania

[2] Romanian Space Agency

ulpia.botezatu@ici.ro, ella.ciuperca@ici.ro

Abstract: This paper analyses the integration of Artificial Intelligence (AI) into the security strategies of critical and space infrastructures, emphasizing the transformative potential of AI in enhancing threat detection, response, and overall system resilience. It covers the fundamentals of space-related AI, its role in identifying and mitigating vulnerabilities, and recent case studies highlighting both successes and limitations. The paper proposes strategic improvements, discusses future trends in AI and space security, and delves into the ethical considerations associated with AI deployment in these domains. Through comprehensive analysis and real-world examples, this paper underscores the necessity of AI in safeguarding essential infrastructures against emerging threats.

Keywords: Artificial Intelligence, Space Security, Critical Infrastructures, Cybersecurity, Threat Detection.

Securitatea spațială bazată pe Inteligența Artificială: tendințe viitoare și imperative strategice pentru infrastructurile critice

Rezumat: Această lucrare analizează integrarea Inteligenței Artificiale (IA) în strategiile de securitate ale infrastructurilor critice și spațiale, evidențiind potențialul transformator al IA în îmbunătățirea detectării amenințărilor, a capacității de răspuns și a rezilienței generale a sistemelor. Studiul abordează fundamentele utilizării IA în domeniul spațial, rolul acesteia în identificarea și atenuarea vulnerabilităților, precum și studii de caz recente care ilustrează atât succesele, cât și limitările acestei tehnologii. Lucrarea propune îmbunătățiri strategice, analizează tendințele viitoare în domeniul securității spațiale bazate pe IA și explorează implicațiile etice ale implementării IA în aceste domenii. Printr-o analiză cuprinzătoare și exemple din realitate, lucrarea subliniază necesitatea adoptării IA pentru protejarea infrastructurilor esențiale împotriva amenințărilor emergente.

Cuvinte-cheie: Inteligență Artificială, Securitate Spațială, Infrastructuri Critice, Securitate Cibernetică, Detectarea Amenințărilor.

1. Introduction

In the modern era, critical infrastructures and space security are essential for maintaining national and international stability. These infrastructures include satellite communications, navigation systems, and terrestrial and space monitoring platforms, which are fundamental for various domains, ranging from the economy to national defence (Richelson, 2012). In an interconnected world, protecting these resources becomes a major priority, and artificial intelligence (AI) plays a crucial role in this equation.

Space security is a strategically important field, given that many critical technologies rely on satellites for optimal operation (Dolman, 2002). The protection of satellites and the data transmitted through them is essential for preventing and managing cyber and physical threats. Anti-satellite attacks and physical interferences represent significant risks, necessitating prompt and effective defence measures. AI can identify and neutralize these threats in their early stages, thus ensuring the integrity of space infrastructures (Johnson-Freese, 2017).

Artificial intelligence can fundamentally transform the protection of critical infrastructures through its ability to rapidly and accurately analyse large volumes of data. AI enables early detection of anomalies and potential threats, facilitating the prevention of incidents before they

https://doi.org/10.33436/v35i1y202501

impact essential infrastructures (Goodfellow, Bengio & Courville, 2016). Additionally, AI optimizes the allocation of defence resources and accelerates decision-making processes in crisis situations, which are vital aspects in both military and civilian contexts (Russell & Norvig, 2020).

Thus, integrating artificial intelligence into the strategies for protecting critical infrastructures and space security is indispensable for facing modern challenges. AI not only enhances threat detection and response but also increases the resilience and adaptability of these infrastructures in a constantly changing security landscape.

At the same time, space security has become a crucial aspect of global security, given the profound dependence of modern infrastructures on space capabilities. Space systems, including communication, navigation, and weather satellites, are now recognized as critical infrastructures essential for the efficient operation of vital services, ranging from navigation and telecommunications to environmental monitoring and disaster management (Johnson-Freese, 2016).

Space systems play a vital role in military decision-making and crisis coordination. They support not only communications and intelligence gathering but also precision in global navigation and targeting operations. Without access to these technologies, the ability to respond swiftly and effectively to international threats would be significantly diminished (Richelson, 2012). For example, during the Gulf War, satellite-based navigation and communication systems were crucial for coordinating coalition forces and executing precision strikes (Richelson, 2012).

The protection of these essential assets is complicated by the dual nature of the threats they face: both cyber and physical. Cyberattacks, such as hacking or signal interference, can disrupt communications and corrupt data. For instance, recent advancements in AI-driven cybersecurity have demonstrated improvements in mitigating such threats, yet the increasing sophistication of cyberattacks necessitates continuous innovation in AI defenses (Peled et al., 2023). On the other hand, physical threats, including potential anti-satellite attacks or the risk of collision with space debris, require rigorous preventive and reactive measures to ensure the continuity of these systems' operations (Weeden & Samson, 2017).

AI significantly enhances space security by improving situational awareness, threat detection, and response capabilities. AI algorithms analyse data from space surveillance networks to track the positions and trajectories of satellites and space debris. These systems predict potential collisions, providing timely alerts and enabling satellite operators to execute maneuvers, thus maintaining the functionality and safety of critical space assets (Oche, Ata & Ibekwe, 2021). For instance, machine learning algorithms are now utilized in automated space traffic management systems, offering real-time adjustments to satellite operations to mitigate collision risks. By integrating data from multiple sources, including ground-based radars and telescopes, AI systems offer a comprehensive picture of the orbital environment, facilitating effective collision avoidance strategies (Buczak & Guven, 2016; ESA, 2019). Advanced AI models also analyse the behaviour of objects in space, identifying irregular activities such as unexpected manoeuvres by satellites that may indicate hostile actions or malfunctions. Early detection systems powered by AI can quickly assess the threat level and suggest appropriate countermeasures, enhancing the resilience of space infrastructures. For example, AI-assisted space domain awareness platforms can classify anomalies in satellite behaviors, distinguishing between natural drifts and potential adversarial actions. By incorporating AI-driven predictive models, these systems can now anticipate and mitigate the impact of disruptive space weather events, including solar flares, ensuring operational continuity (Benvenuto et al., 2020; Jiao, Yu & Jiang, 2020).

In conclusion, space security is an integral component of global security, necessitating advanced technological solutions such as AI to protect critical space infrastructures. The integration of AI into space security strategies ensures enhanced threat detection, improved response capabilities, and greater resilience of these vital systems.

Recent technological advancements in AI have enabled the deployment of more sophisticated solutions for detecting cyberattacks, monitoring space activities, and optimizing defense resources. Additionally, the emergence of AI regulations, such as the EU AI Act, has started to shape the legal and ethical considerations of AI in space security. In this context, the

present study is structured as follows: Section 2 provides a comprehensive analysis of the fundamentals of AI in space security; Section 3 explores AI applications in identifying and mitigating vulnerabilities; Section 4 presents a review of future AI trends and challenges in space security; Section 5 examines the ethical and regulatory frameworks shaping AI deployment in space. Finally, Section 6 synthesizes key findings and provides strategic recommendations

2. Fundamentals of space-related Artificial Intelligence

Artificial Intelligence is a pivotal field within computer science that enables machines to perform tasks requiring human intelligence, such as pattern recognition, language interpretation, and decision-making. In recent years, AI has become increasingly sophisticated, integrating advanced machine learning, deep learning, and reinforcement learning techniques to tackle highly complex problems in security and defense applications. Lately, AI has become an indispensable tool in enhancing the security of critical infrastructures and space protection, offering innovative solutions to complex national and international security challenges (Russell & Norvig, 2020). Moreover, the intersection of AI with cloud computing, quantum computing, and edge computing has opened new avenues for real-time data analysis and autonomous decision-making, further strengthening the resilience of space operations.

AI plays a transformative role in improving the efficiency, reliability, and security of space systems. Its applications are diverse, spanning various sectors and addressing multiple facets of infrastructure management and security. In the context of space-related critical infrastructures, AI technologies significantly enhance monitoring and diagnostic capabilities:

- Predictive Maintenance: AI algorithms analyse vast amounts of operational data to identify patterns and anomalies indicating potential failures. Predictive maintenance models can forecast equipment breakdowns by recognizing early signs of wear and tear, allowing for timely interventions that prevent costly downtimes and enhance system reliability (Goodfellow, Bengio & Courville, 2016). The integration of AI-driven Digital Twins - virtual replicas of physical assets - has further optimized predictive maintenance by enabling real-time simulations and anomaly detection. For instance, NASA uses AI to monitor the health of its spacecraft systems, predicting and addressing potential issues before they escalate. Similarly, AI-driven predictive maintenance in electrical grids can foresee transformer failures, enabling pre-emptive repairs that prevent widespread power outages, thereby ensuring a stable energy supply essential for critical infrastructure (Afridi, Ahmad & Hassan, 2021);
- Cybersecurity: AI enhances cybersecurity measures by providing advanced threat detection and response capabilities. Machine learning models analyse network traffic in real-time, identifying suspicious activities and potential cyberattacks. Newer approaches, such as Generative Adversarial Networks (GANs) and adversarial AI, have been employed to simulate cyber threats and improve defensive mechanisms, allowing security protocols to pre-emptively adapt to evolving attack patterns. For example, AI systems can detect anomalies in satellite communication links, indicating possible cyber intrusions or signal jamming attempts. In 2019, the U.S. Department of Defence (2019) reported using AI to enhance the cybersecurity of its satellite systems, highlighting the role of AI in protecting critical space assets from cyber threats;
- Space Situational Awareness: AI is instrumental in monitoring satellite behaviour and managing the increasingly crowded orbital environment. AI algorithms process data from space surveillance networks to track the positions and trajectories of satellites and space debris. Recent developments in AI-powered Space Domain Awareness (SDA) have enabled automated classification of space objects, distinguishing between natural debris, malfunctioning satellites, and potential threats. These systems can predict potential collisions, providing timely alerts and enabling satellite operators to execute manoeuvres. This capability is crucial for maintaining the functionality and safety of both military and commercial satellites (Oche, Ata & Ibekwe, 2021). For instance, the

European Space Agency (ESA) employs AI-powered systems to track over 20,000 pieces of space debris, predicting collision risks and ensuring the safety of its satellites. Additionally, AI-assisted SSA platforms integrate data from heterogeneous sources, including ground-based telescopes, radar, and onboard satellite sensors, improving detection accuracy and threat assessment;

- Early Detection of Space Threats: Advanced AI models analyse the behaviour of objects in space, identifying irregular activities such as unexpected manoeuvres by satellites that may indicate hostile actions or malfunctions. By leveraging AI-driven behavioral analysis, defense agencies can establish automated early warning systems capable of identifying deviations in satellite trajectories that may signal adversarial intent. Early detection systems powered by AI can quickly assess the threat level and suggest appropriate countermeasures, enhancing the resilience of space infrastructures. For instance, neural networks trained on historical satellite movement patterns can now differentiate between standard orbital corrections and anomalous or adversarial maneuvers. By predicting these events and their potential impact, AI systems enable operators to take preventive measures and safeguard critical space assets (Benvenuto et al., 2020; Jiao, Yu & Jiang, 2020).

A specific example of AI's application in space situational awareness is its use in the Space Surveillance Network (SSN). The SSN employs AI algorithms to process data from ground-based sensors and track thousands of objects in orbit. By analysing this data, AI systems can predict potential collisions and assess the risk posed by space debris. This capability is crucial for ensuring the safety and longevity of satellites, as well as for maintaining the sustainability of the space environment (Oche, Ata & Ibekwe, 2021). Companies like SpaceX also utilize AI to manage the vast amount of data from their satellite constellations, ensuring optimal performance and collision avoidance.

The integration of AI into critical infrastructures and space security not only enhances their operational efficiency but also ensures their resilience against emerging threats. As AI technologies continue to evolve, their applications will likely extend beyond predictive maintenance and surveillance, encompassing autonomous mission planning, intelligent threat deterrence, and AI-augmented decision support systems for both civilian and military space operations.

3. The role of AI in identifying and mitigating vulnerabilities

In the digital age, artificial intelligence (AI) has become a crucial tool for the security of critical infrastructures, both terrestrial and spatial. AI's ability to quickly and efficiently analyse large volumes of data enables early threat detection and rapid incident response, thereby enhancing the resilience and protection of these vital systems. By integrating AI-driven automation, response times to potential threats can be significantly reduced, improving the overall effectiveness of security operations. Furthermore, AI-driven threat intelligence can provide proactive risk assessments, allowing security teams to anticipate vulnerabilities before they are exploited.

By employing advanced machine learning algorithms and signal processing techniques, AI can identify patterns and signals indicative of imminent threats or vulnerabilities. In space infrastructures, for instance, AI is used for continuous satellite monitoring, detecting abnormal behaviours such as unauthorized manoeuvres or unexpected trajectory changes that may suggest interference or an attack. Recent advancements in reinforcement learning have further improved AI’s capability to autonomously adapt to new patterns of threats, ensuring faster and more reliable countermeasures. Additionally, AI-based behavioral anomaly detection models can now differentiate between natural satellite adjustments and potentially malicious maneuvers.

A notable example is the use of neural networks to detect and classify anomalous signals from satellites, which can indicate a cyberattack or technical malfunction. AI-powered anomaly detection systems leverage historical data and real-time telemetry to differentiate between benign deviations and potential threats. These systems can learn from past experiences and adapt to

emerging threats as they arise (Preetha et al., 2024). For example, adversarial AI techniques have been explored to simulate potential cyberattack strategies, allowing AI-driven defenses to pre-emptively adapt against evolving attack vectors. Lockheed Martin has developed AI systems that assess satellite health, anticipate potential failures, and autonomously respond to abnormal conditions without human intervention. This system uses convolutional neural networks (CNNs) to process sensor data from satellites, identifying deviations from normal operational patterns that may signal issues such as system malfunctions or potential cyberattacks (Athar et al., 2024). These AI systems now incorporate federated learning, which enables multiple satellite systems to share insights without exposing raw data, thereby enhancing cybersecurity while maintaining data privacy.

3.1. AI in terrestrial critical infrastructures

AI's role extends to terrestrial critical infrastructures, where it enhances the monitoring and protection of essential services. Critical infrastructures such as power grids, transportation networks, and water supply systems are increasingly reliant on AI technologies for improved security and operational efficiency:

- Predictive Maintenance: AI algorithms analyze operational data to identify patterns and predict potential failures. Predictive maintenance models can forecast equipment breakdowns by recognizing early signs of wear and tear, allowing for timely interventions that prevent costly downtimes and enhance system reliability. For instance, AI-powered sensor networks integrated with edge computing can now process data at the infrastructure level, reducing latency and enabling faster decision-making in real-time. Support vector machines (SVMs) and recurrent neural networks (RNNs) are used in predictive maintenance systems to analyse time-series data from sensors installed in infrastructure components. These models detect early signs of wear and tear, enabling pre-emptive repairs that prevent widespread power outages (Afridi, Ahmad & Hassan, 2021);
- Cybersecurity: AI enhances cybersecurity measures by providing advanced threat detection and response capabilities. Machine learning models analyse network traffic in real-time, identifying suspicious activities and potential cyberattacks. In addition to anomaly detection, AI-driven security orchestration platforms can now autonomously deploy countermeasures, isolating compromised systems before an attack spread. Deep learning algorithms, such as long short-term memory (LSTM) networks, are particularly effective in identifying patterns in network traffic that deviate from normal behaviour, flagging potential security breaches. Furthermore, AI-enhanced threat intelligence systems can now leverage global cyber threat feeds to predict attack patterns and recommend proactive security adjustments. AI systems can detect anomalies in communication links, indicating possible cyber intrusions or signal jamming attempts. In 2019, the U.S. Department of Defense (2019) reported using AI to enhance the cybersecurity of its satellite systems, highlighting the role of AI in protecting critical space assets from cyber threats.

4. Critical infrastructures and vulnerabilities

Critical infrastructures form the backbone of modern societies, underpinning essential services such as healthcare, security, transportation, and communications. These complex and interconnected systems are vital for economic stability and national security. Any disruption can have devastating effects on social and economic life (Rinaldi, Peerenboom & Kelly, 2001). Given their growing reliance on digital technologies and automation, ensuring their resilience requires a multidimensional approach integrating cybersecurity, predictive analytics, and robust risk assessment frameworks.

Despite their importance, critical infrastructures are susceptible to a wide range of risks and vulnerabilities, from natural disasters to terrorist and cyber-attacks. Increased digitalization and

reliance on information networks have amplified exposure to cyber threats, which can compromise sensitive data, disrupt service operations, or even cause physical damage (Cavelty, 2008). Moreover, the interconnectivity between different sectors means that a single failure in one domain - such as power distribution - can lead to cascading failures across other infrastructures, such as healthcare and telecommunications.

In May 2021, the Colonial Pipeline, which supplies nearly half of the East Coast's fuel, suffered a severe ransomware attack. The attackers, later identified as the cybercriminal group DarkSide, infiltrated the company's network, encrypting data and demanding a ransom to restore access. The pipeline's operations were halted for several days, leading to widespread fuel shortages, panic buying, and a sharp increase in gasoline prices across several states. This incident not only disrupted fuel supply but also had cascading effects on various sectors, including transportation and emergency services, highlighting the critical interdependencies within national infrastructure systems. Furthermore, the attack underscored the growing trend of supply chain vulnerabilities, as third-party software and service providers were also targeted, exacerbating the impact.

The Colonial Pipeline attack underscored the urgency of enhancing cybersecurity measures across critical infrastructures. It demonstrated that cyber threats could have physical and economic repercussions far beyond the immediate target. In response, the incident prompted significant policy discussions and actions at both federal and corporate levels to bolster defenses against such vulnerabilities. These responses included mandatory cybersecurity risk assessments, greater adoption of zero-trust architectures, and the development of AI-powered intrusion detection systems. This included the development of more comprehensive cybersecurity frameworks, increased investment in security technologies, and the adoption of more rigorous incident response strategies (Reeder & Hall, 2021). Additionally, this event catalyzed discussions on the necessity of international cooperation in mitigating cyber threats to infrastructure, particularly in establishing unified security standards for critical digital assets.

In July 2021, Germany experienced one of its most devastating natural disasters in recent history. Torrential rains led to severe flooding, particularly in the regions of North Rhine-Westphalia and Rhineland-Palatinate. The floods caused extensive damage to infrastructure, including roads, bridges, and railways, and disrupted essential services such as electricity and water supply. The disaster resulted in the loss of over 180 lives and caused billions of euros in damages. This extreme weather event aligned with broader trends of increasing climate-induced disruptions to infrastructure, emphasizing the urgent need for climate adaptation measures.

The floods exposed significant vulnerabilities in Germany's critical infrastructure to extreme weather events, a growing concern amidst the escalating impacts of climate change. Public utilities faced immense challenges in restoring services, and the disaster revealed gaps in emergency preparedness and response mechanisms. Moreover, it highlighted the limitations of existing risk assessment models, which failed to fully anticipate the scale of the disaster due to outdated predictive climate data. Moreover, the flooding highlighted the importance of integrating climate resilience into the planning and development of critical infrastructure. Modern AI-driven climate modelling tools are now being employed to enhance early warning systems and infrastructure design, ensuring adaptability to extreme weather conditions.

In the aftermath, there was a strong push towards enhancing disaster resilience. Efforts included revising infrastructure design standards to account for extreme weather conditions, investing in early warning systems, and improving coordination among emergency services. The European Union also launched initiatives to integrate climate vulnerability assessments into urban and regional infrastructure planning. The case also emphasized the need for comprehensive risk assessments and the implementation of adaptive measures to mitigate the effects of future climate-related disasters (Kreibich et al., 2017). Beyond structural reinforcements, digital twin technologies - virtual models of physical infrastructure - are increasingly being adopted to simulate extreme weather impacts and optimize resilience strategies.

5. Integrating AI in space security strategies

The integration of Artificial Intelligence (AI) technologies into the security strategies of critical and space infrastructures is essential for addressing the dynamic threats of the 21st century. AI optimizes incident detection and response through advanced data analysis and anticipates potential vulnerabilities via machine learning and predictive modelling. Furthermore, AI enables autonomous decision-making in high-risk scenarios, reducing reliance on human intervention and improving response efficiency. This section examines the role of AI in enhancing the security of critical space infrastructures, highlights real-world examples, and proposes strategic improvements.

Traditional security strategies are often limited by the speed and accuracy of data processing and interpretation. In contrast, AI can analyze complex datasets with unparalleled speed and precision, enabling security agencies to identify the patterns and signatures of cyber-attacks more effectively. This capability allows for proactive measures to counter threats before they impact vital infrastructures. Additionally, AI-driven security systems can adapt in real time, responding dynamically to evolving cyber threats and physical intrusions. In space security, AI can monitor satellite behavior and detect interference signals, enhancing overall situational awareness.

A notable example of AI integration into security policies is the U.S. Department of Defense's use of AI systems to enhance the cybersecurity of space assets, as detailed in the 2020 Defense Space Strategy. This strategy emphasizes the use of AI to "anticipate threats and dynamically respond to incidents" (U.S. Department of Defense, 2020). Another example is NATO's collaboration with the tech industry to develop AI systems that protect military communication networks, a critical component of infrastructure security (NATO Communications and Information Agency, 2021). These initiatives underline the strategic importance of AI in ensuring the integrity and functionality of space-based assets, which are increasingly targeted in cyber warfare and electronic warfare scenarios.

To maximize the benefits of AI in the security of critical and space infrastructures, the following strategic improvements are proposed:

1. Development of AI Centers of Excellence for Security: These centers would serve as hubs for innovation and collaboration between government agencies, industry, and academia. They would focus on developing cutting-edge AI technologies tailored to the specific needs of space and critical infrastructure security. Additionally, these centers could facilitate real-time threat intelligence sharing, improving coordinated responses to cyber and space-based threats.

2. Implementation of Standardized AI-Supported Security Protocols: Establishing standardized protocols for the validation and verification of AI-generated data is crucial. These protocols ensure that AI systems provide reliable and secure outputs, facilitating informed decision-making and effective threat response. This standardization would also help mitigate the risks associated with AI biases, ensuring that security algorithms function transparently and fairly across different operational environments.

3. Continuous Training and Education in AI: Security personnel must be trained to understand and efficiently operate AI systems. Ongoing education and training programs will help keep the workforce updated with the latest AI advancements and their applications in security contexts. Furthermore, AI-driven simulation environments could be utilized to train personnel in responding to cyber-physical threats in real-time, enhancing preparedness and decision-making capabilities.

AI's application in space security includes systems for anomaly detection in satellite communications. These systems use machine learning algorithms to monitor signals and detect deviations indicating potential interference or attacks. For instance, the European Space Agency (ESA) has implemented AI technologies to identify and mitigate unauthorized interference with satellites (Ibrahim et al., 2018). Advanced deep learning techniques have also improved AI’s ability to differentiate between benign anomalies and hostile interference, minimizing false positives in threat assessments.

In addition to satellite communications, AI significantly enhances the security of terrestrial critical infrastructures, where it enhances the monitoring and protection of essential services. Critical infrastructures such as power grids, transportation networks, and water supply systems are increasingly reliant on AI technologies for improved security and operational efficiency. AI algorithms analyse operational data to identify patterns and predict potential failures. Predictive maintenance models can forecast equipment breakdowns by recognizing early signs of wear and tear, allowing for timely interventions that prevent costly downtimes and enhance system reliability. AI-powered digital twins - virtual replicas of critical infrastructure - are increasingly used for real-time monitoring and predictive maintenance, improving resilience and proactive decision-making. For example, AI-driven predictive maintenance in electrical grids can foresee transformer failures, enabling pre-emptive repairs that prevent widespread power outages (Balaji & Kumar, 2019). As illustrated in Figure 1, the integration of AI leads to a significant improvement in security measures compared to traditional methods, demonstrating enhanced monitoring capabilities and proactive threat mitigation.

Security Aspect	AI-Enhanced Security	Traditional Security
Speed of Threat Detection	High	Moderate
Accuracy of Threat Analysis	Very High	Moderate
Resource Optimization	Efficient	Manual allocation
Adaptability to New Threats	Quick adjustments	Time-consuming updates

Figure 1. Comparative view on security with and without AI

AI also enhances cybersecurity measures by providing advanced threat detection and response capabilities. Machine learning models analyse network traffic in real-time, identifying suspicious activities and potential cyberattacks. These models are now complemented by AI-driven automated security orchestration and response (SOAR) systems, which autonomously deploy countermeasures when cyber threats are detected. AI systems can detect anomalies in communication links, indicating possible cyber intrusions or signal jamming attempts. In 2019, the U.S. Department of Defence (2019) reported using AI to enhance the cybersecurity of its satellite systems, highlighting the role of AI in protecting critical space assets from cyber threats.

Furthermore, AI applications in the security of navigation and Earth observation infrastructures involve deep learning algorithms to detect and classify objects in satellite images, which is crucial for national security and disaster management. Emerging AI technologies now integrate multi-modal satellite data, fusing optical, infrared, and radar imagery to enhance object detection and situational awareness in real time. Digital Globe’s project employs convolutional neural networks to identify real-time changes on Earth, providing critical information to government agencies (Zhu et al., 2017).

NASA utilizes AI for simulating and managing incidents within its critical infrastructure. For example, AI optimizes incident responses through modelling and simulating attack scenarios, allowing for rapid and efficient response. By integrating reinforcement learning, NASA's AI-driven simulation systems can now autonomously refine response strategies based on real-time threat data. These AI applications enhance the security and resilience of SCADA (Supervisory Control and Data Acquisition) systems, which are crucial for critical infrastructure, including terrestrial space activities such as satellite launches and tracking station management (Anderson et al., 2022).

6. Future trends in AI and space security

As AI technologies continue to evolve, several emerging trends and anticipated breakthroughs are expected to shape the future of space security. These advancements will further enhance the capabilities of AI systems in monitoring, threat detection, and response, providing more robust solutions for safeguarding critical infrastructures. Moreover, the integration of AI with

other advanced technologies, such as blockchain and digital twins, is expected to create new security paradigms that enhance transparency, traceability, and predictive analysis in space operations:

- Quantum Computing: Quantum computing promises to revolutionize AI by providing unprecedented computational power. This will enable the processing of vast amounts of data at speeds previously unimaginable, significantly improving the accuracy and efficiency of AI algorithms used in space security. Quantum AI can enhance predictive modelling, anomaly detection, and real-time data analysis, offering superior capabilities in managing space-related threats (Preskill, 2018; Pirandola et al., 2020). Additionally, quantum encryption techniques will play a pivotal role in securing satellite communications, ensuring resilience against cyber threats that target conventional cryptographic systems;
- Edge AI: The deployment of AI at the edge, closer to the data source, will reduce latency and enhance the speed of decision-making processes. In space security, edge AI can be implemented on satellites and space stations, allowing for real-time data processing and immediate response to detected threats without relying on ground-based systems. This decentralization of AI processing will improve resilience and operational efficiency (Shi et al., 2016). Furthermore, edge AI will enable autonomous satellite constellations to coordinate with minimal ground intervention, increasing the robustness of space situational awareness (SSA) systems;
- AI-Driven Autonomous Systems: The future will see an increase in AI-driven autonomous systems capable of performing complex tasks without human intervention. These systems will be essential in space security for tasks such as on-orbit satellite maintenance, debris removal, and autonomous threat response. Enhanced autonomy will reduce the need for human presence in hazardous environments, thereby increasing safety and efficiency (Chien & Wagstaff, 2017). Moreover, AI-powered swarm intelligence is expected to enable multiple autonomous agents - such as drones, satellites, and robotic probes - to collaboratively monitor, protect, and repair space assets in real time;
- Enhanced Cybersecurity Measures: As cyber threats continue to evolve, AI will play a crucial role in developing more sophisticated cybersecurity measures. Future AI systems will employ advanced machine learning techniques, such as generative adversarial networks (GANs) and reinforcement learning, to predict and counteract cyberattacks more effectively. These technologies will enhance the protection of both terrestrial and space-based critical infrastructures (Goodfellow et al., 2020). Additionally, AI-powered deception technologies - such as honeypot AI traps - will be deployed to mislead cyber adversaries, providing early warning signals and strengthening defense mechanisms against advanced persistent threats (APTs).

Beyond these advancements, AI will increasingly intersect with other emerging technologies, expanding the capabilities of space security frameworks:

- Digital Twins for Predictive Space Security: AI-powered digital twins - virtual replicas of space systems - will provide enhanced simulation and predictive analytics for identifying potential vulnerabilities before they manifest in real-world operations. These models will enable scenario-based training, mission planning, and proactive risk mitigation strategies for critical space assets;
- AI and Blockchain for Secure Space Communications: The integration of AI with blockchain technology will bolster the security of satellite networks by enabling decentralized and tamper-proof data transmissions. This approach will be particularly valuable for securing military and governmental satellite communications against unauthorized access or data manipulation (Szabadföldi, 2021);
- Neuromorphic Computing for AI in Space: The development of neuromorphic

processors - designed to mimic the architecture of the human brain - will significantly improve the efficiency of AI in space applications. These processors will allow AI-driven security systems to function with lower power consumption and enhanced real-time processing, making them ideal for deployment on energy-constrained space assets.

7. Ethical considerations

The deployment of AI in space security raises several ethical considerations that must be addressed to ensure responsible and fair use of technology. These considerations include data privacy, autonomy in decision-making, and the implications of AI in warfare. Furthermore, as AI systems become increasingly sophisticated, the need for ethical governance, transparency, and bias mitigation becomes paramount to prevent unintended consequences in security applications:

- Data Privacy: The use of AI in space security involves the collection and processing of vast amounts of data, raising concerns about data privacy and protection. Ensuring that data is handled ethically and in compliance with privacy regulations is paramount. Strategies must be implemented to anonymize sensitive information and prevent unauthorized access to data (Floridi et al., 2018). Moreover, AI-powered encryption and privacy-preserving AI models, such as federated learning, offer potential solutions to enhance data security without compromising operational efficiency;
- Autonomy in Decision-Making: AI systems, especially those used in defense and security, often operate with a high degree of autonomy. This raises ethical questions about the extent to which machines should be allowed to make critical decisions without human oversight. Establishing clear guidelines and ethical frameworks for autonomous AI decision-making is essential to ensure accountability and prevent unintended consequences (Binns, 2018). Additionally, hybrid AI-human decision-making models are being explored to ensure human oversight in high-risk scenarios, balancing efficiency with ethical responsibility;
- Implications of AI in Warfare: The use of AI in military applications, including space security, has significant implications for warfare. AI can enhance the capabilities of autonomous weapons systems, leading to ethical dilemmas regarding the use of lethal force by machines. It is crucial to develop international regulations and agreements that govern the deployment of AI in military contexts, ensuring that the technology is used responsibly and ethically (Arkin, 2009). Recent discussions at the United Nations and NATO highlight the growing need for AI arms control agreements to regulate autonomous military technologies in space-based security operations;
- Transparency and Accountability: Ensuring transparency in AI algorithms and decision-making processes is vital for building trust and accountability. Stakeholders must be able to understand and verify how AI systems reach their conclusions, particularly in high-stakes scenarios involving national security. Developing explainable AI (XAI) systems can help achieve this goal by making AI decisions more interpretable and transparent (Doshi-Velez & Kim, 2017). Furthermore, standardized auditing mechanisms and AI ethics certifications could enhance trust in AI applications within space security.

A visualization summarizing the information above is presented in Figure 2, which outlines key ethical considerations while using AI. These include concerns related to transparency, accountability, bias mitigation, and the responsible use of AI-driven decision-making in critical infrastructure security.

Ethical Consideration	Description
Data Privacy	Ensuring secure handling of sensitive information and data.
Autonomy in Decision-Making	Establishing guidelines for AI autonomy in critical decisions.
Implications in Warfare	Addressing ethical dilemmas related to AI use in military contexts.
Transparency and Accountability	Ensuring transparency in AI algorithms and decision-making processes.

Figure 2. Ethical considerations while using AI

To address these ethical concerns, it is essential to establish robust AI governance frameworks that ensure responsible deployment. The following measures are recommended:

1. Development of AI Ethics Guidelines. National and international bodies should collaborate to establish guidelines that define the ethical use of AI in space security. These guidelines should be aligned with existing legal frameworks, such as the EU AI Act and the UN Convention on Certain Conventional Weapons (CCW).
2. Implementation of AI Bias Audits. AI models used in space security should undergo rigorous bias audits to ensure that their decision-making processes do not disproportionately affect certain nations or entities. AI fairness techniques, such as adversarial debiasing and counterfactual fairness, can be incorporated into security AI systems.
3. AI Explainability Requirements. The development and deployment of AI models should prioritize explainable AI (XAI) techniques to ensure that AI-driven security decisions are interpretable and justifiable.
4. Human-in-the-Loop (HITL) Integration. AI systems in space security should incorporate HITL frameworks to ensure that human operators retain ultimate decision-making authority over high-stakes security scenarios.

8. Conclusions

The integration of Artificial Intelligence (AI) into the security strategies of critical and space infrastructures represents a significant advancement in technological capabilities, offering substantial benefits in threat detection, response, and overall system resilience. AI has not only improved operational efficiency but also enhanced predictive capabilities, allowing security systems to proactively address potential threats before they materialize. The successes observed in various case studies demonstrate AI's potential to revolutionize the monitoring and protection of these vital systems.

Successes in AI applications are evident in the enhanced ability to detect and respond to threats against critical and space infrastructures. AI algorithms enable faster and more accurate data analysis, essential in critical situations. For example, the processing of vast amounts of satellite data to identify potential hazards or anomalies in real-time has significantly improved situational awareness and response times (Goodfellow, Bengio & Courville, 2016). AI-driven automation has also facilitated the reduction of human workload in high-risk security operations, ensuring more effective resource allocation and rapid threat mitigation.These capabilities underscore AI's role in maintaining the security and functionality of critical infrastructures.

However, limitations remain, including the dependency on large volumes of high-quality data for training algorithms and the risks associated with insufficient or inappropriate training data. Bias in AI models remains a significant challenge, potentially leading to inaccurate threat

assessments or discriminatory decision-making in security applications. Cybersecurity challenges also pose significant risks to the effectiveness of AI systems. Inadequate data can lead to false positives or negatives in threat detection, undermining the reliability of AI solutions (Russell & Norvig, 2020). Additionally, adversarial AI techniques, where malicious actors manipulate AI models by introducing deceptive inputs, highlight the need for robust defenses against AI-targeted cyberattacks. Addressing these limitations is crucial to fully realizing the potential of AI in critical infrastructure security.

The lessons learned from these implementations highlight the need for continuous integration of new research in AI. Collaboration between governmental agencies, industry, and academia is essential to advance AI technologies and develop robust strategies for mitigating associated risks. Moreover, policy-driven frameworks such as the EU AI Act and emerging global AI governance initiatives will play a crucial role in defining the ethical and legal boundaries for AI deployment in security-sensitive environments. A multidisciplinary approach to AI implementation ensures that technological advancements are grounded in practical, real-world applications and supported by frameworks addressing ethical, legal, and security concerns (Floridi, 2023).

In conclusion, the successful integration of AI into the security strategies of critical and space infrastructures necessitates ongoing research, collaboration, and strategic planning. By addressing the current limitations and leveraging the lessons learned, stakeholders can enhance the resilience and security of these essential systems. Future AI advancements in quantum security, edge AI, and autonomous defense networks will further strengthen the ability to safeguard critical infrastructures from evolving threats. The future of AI in critical infrastructure security promises continued innovation and improvement, providing robust solutions to emerging threats and challenges.

REFERENCES

Afridi, Y. S., Ahmad, K. & Hassan, L. (2021) Artificial Intelligence Based Prognostic Maintenance of Renewable Energy Systems: A Review of Techniques, Challenges, and Future Research Directions. *arXiv* preprint arXiv:2104.12561.

Anderson, R. J. et al. (2022) Artificial Intelligence in SCADA Systems Security: A Review and Future Directions. *Journal of Network and Computer Applications*. 184, Article 103074. doi: 10.1016/j.jnca.2021.103074.

Arkin, R. C. (2009) *Governing Lethal Behavior in Autonomous Robots*. CRC Press.

Athar, A., Mozumder, M. A. I., Abdullah, S., Ali, S. & Kim, H.C. (2024) Deep Learning-Based Anomaly Detection Using One-Dimensional Convolutional Neural Networks (1D CNN). In Machine Centers (MCT) and Computer Numerical Control (CNC) Machines. *PeerJ Computer Science*. 10, e2389. doi: 10.7717/peerjcs.2389.

Balaji, P. & Kumar, P. (2019) AI-based Predictive Maintenance in Power Grids. *International Journal of Electrical Power & Energy Systems*. 107, 424-435. doi: 10.1016/j.ijepes.2018.11.034.

Benvenuto, F., Campi, C., Massone, A. M. & Piana, M. (2020) Machine Learning as a Flaring Storm Warning Machine: Was a Warning Machine for the September 2017 Solar Flaring Storm Possible? To be published in *Solar and Stellar Astrophysics* [Preprint] https://arxiv.org/abs/2007.02425 [Accessed 3th March 2025].

Binns, R. (2018) Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*. doi: 10.1145/3287560.3287598

Buczak, A. L. & Guven, E. (2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. In *IEEE Communications Surveys & Tutorials*. 18(2), 1153-1176. doi: 10.1109/COMST.2015.2494502.

Cavelty, M. D. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

Chien, S. & Wagstaff, K. L. (2017) Robotic space exploration agents. *Science Robotics*. 2(7), eaam4181. doi: 10.1126/scirobotics.aam4181.

Dolman, E. C. (2002) *Astropolitik: Classical Geopolitics in the Space Age*. Routledge.

Doshi-Velez, F. & Kim, B. (2017) Towards a rigorous science of interpretable machine learning. To be published in *Machine Learning* [Preprint] https://arxiv.org/abs/1702.08608 [Accessed 3th March 2025].

ESA (2019) *Automating collision avoidance* https://www.esa.int/Space_Safety/Space_Debris/Automating_collision_avoidance. [Accessed 3th March 2025].

Floridi, L. (2023) *The Ethics of Artificial Intelligence*. Oxford University Press.

Floridi, L. et al. (2018) AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*. 28(4), 689-707. doi: 10.1007/s11023-018-9482-5.

Goodfellow, I., Bengio, Y. & Courville, A. (2016) *Deep Learning*. MIT Press.

Goodfellow, I. et al. (2020) Generative Adversarial Networks. *Communications of the ACM*. 63(11), 139-144. doi: 10.1145/3422622.

Ibrahim, S. K., Ahmed, A., Zeidan, M. A. E. & Ziedan, I. E. (2018) Machine Learning Methods for Spacecraft Telemetry Mining. *IEEE Transactions on Aerospace and Electronic Systems*. 55(4), 2732-2747. doi:10.1109/TAES.2018.2876586. https://www.karlancer.com/api/file/1683234116-ENAX.pdf.

Jiao, Z., Sun, H., Wang, X., Manchester, W., Gomboni, T., Hero, A., & Chen, Y. (2020) Solar Flare Intensity Prediction with Machine Learning Models. *Space Weather*. 18(7), e2020SW002440. Doi: 10.1029/2020SW002440.

Johnson-Freese, J. (2017) *Space Warfare in the 21st Century: Arming the Heavens*. Routledge.

Kreibich, H., Müller, M., Schröter, K. & Thieken, A. H. (2017) New Insights into Flood Warning Reception and Emergency Response by Affected Parties. *Natural Hazards and Earth System Sciences.* 17(12), 2075-2092. doi:10.5194/nhess-17-2075-2017.

NATO Communications and Information Agency (2021) Summary of the NATO Artificial Intelligence Strategy, https://www.nato.int/cps/en/natohq/official_texts_187617.htm [Accessed 3th March 2025].

Oche, P.A. & Ata, E.G. & Ibekwe, N. (2021) Applications and Challenges of Artificial Intelligence in Space Missions. *IEEE Access*. (99):1-1. Doi: 10.1109/ACCESS.2021.3132500. https://www.researchgate.net/publication/356771832_Applications_and_Challenges_of_Artificial_Intelligence_in_Space_Missions

Peled, R., Aizikovich, E., Habler, E., Elovici, Y. & Shabtai, A. (2023) Evaluating the Security of Satellite Systems. To be published in *Criptography and Security* [Preprint] https://arxiv.org/abs/2312.01330.

Pirandola, S. et al. (2020) Advances in Quantum Cryptography. *Advances in Optics and Photonics*. 12(4), 1012-1236. doi: 10.1364/AOP.361248.

Preetha, S. B. K., Sai, J. V. M., Raj, V. S., Sekhar, M. J. & Lavanya, R. (2024) Anomaly Detection in Satellite Power System using Deep Learning. In *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2024*. pp. 1-5. doi: 10.1109/CONECCT62155.2024.10677120.

Preskill, J. (2018) Quantum Computing in the NISQ Era and Beyond. Quantum, 2, 79. doi: 10.22331/q-2018-08-06-79.

Reeder, J. R. & Hall, T. (2021) Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defense Review*. 6(3), 15-39. Retrieved from https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf.

Richelson, J. T. (2012) *America's Space Sentinels: DSP Satellites and National Security*. University Press of Kansas.

Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001) Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. 21(6), 11-25. doi: 10.1109/37.969131.

Russell, S. & Norvig, P. (2020) *Artificial Intelligence: A Modern Approach*. Pearson.

Shi, W., et al. (2016) Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*. 3(5), 637-646. doi: 10.1109/JIOT.2016.2579198.

Szabadföldi, I. (2021) Artificial Intelligence in Military Application – Opportunities and Challenges. *Land Forces Academy Review*. 26(2), 157-165. doi: 10.2478/raft-2021-0022.

U.S. Department of Defense (2019) *DoD Command, Control, and Communications (C3) Modernization Strategy*. Retrieved from https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf [Accessed 3th March 2025].

U.S. Department of Defense (2019) *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19–23*. Retrieved from https://media.defense.gov/2019/jul/12/2002156622/-1/-1/1/dod-digital-modernization-strategy-2019.pdf.

U.S. Department of Defense (2020) *DoD Space Strategy*. https://www.defense.gov/Spotlights/DOD-Space-Strategy/ [Accessed 3th March 2025]

Weeden, B. C. & Samson, V. A. (2017) Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM). *Space Policy*. 42, 13-24. doi: 10.1016/j.spacepol.2017.11.001.

Zhu, X. X. et al. (2017) Deep Learning in Remote Sensing: A Comprehensive Review and List of Resources. *IEEE Geoscience and Remote Sensing Magazine*. 5(4), 8-36. doi: 10.1109/MGRS.2017.2762307.

Ulpia-Elena BOTEZATU is the Chair of the Scientific and Technical Subcommittee of the UN Committee on the Peaceful Uses of Outer Space (COPUOS) and currently serves as a researcher at both the National Institute for Research & Development in Informatics – ICI Bucharest and at the Romanian Space Agency. Recently, she has been appointed as Chair of the Action Team on Lunar Activities Consultation (ATLAC) within the UN Office for the Outer Space Affairs (UN OOSA). She has made significant contributions to the field of space security, with a particular focus on the cybersecurity of space activities. As the Chair of the Scientific and Technical Subcommittee of COPUOS, she addresses critical issues related to the protection of space assets from cyber threats. In her roles, Dr. Botezatu works on developing strategies to secure space infrastructure against potential cyber-attacks and enhancing space situational awareness to detect and mitigate these threats. Her work with intergovernmental organizations - such as European Space Agency, the European Commission, the EU Space Surveillance and Tracking Partnership, the International Organization for Standardization, and NATO's Science and Technology Organization, involves collaboration on cybersecurity measures for space systems, ensuring that international space activities remain secure and peaceful. Dr. Botezatu's upcoming book will explore the intersection of space and urban environments, shedding light on how cybersecurity plays a crucial role in the sustainable development of both domains. Her pursuit of a degree in international space law further underscores her commitment to establishing robust legal frameworks that support the secure and peaceful exploration of outer space.

Ulpia-Elena BOTEZATU ocupă funcția de Președinte al Subcomitetului Științific și Tehnic al Comitetului ONU pentru Utilizarea Pașnică a Spațiului Extraatmosferic și activează ca cercetător la Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București și la Agenția Spațială Română. Contribuțiile sale în domeniul securității spațiale se concentrează, în principal, pe securitatea cibernetică a activităților spațiale și, în calitate de Președinte al Subcomitetului ONU, pledează pentru protecția activelor spațiale împotriva amenințărilor cibernetice. Dr. Ulpia-Elena Botezatu dezvoltă strategii pentru securizarea infrastructurii spațiale împotriva atacurilor cibernetice și pentru conștientizarea situațională a mediului spațial, pentru detectarea timpurie și atenuarea acestor amenințări. Colaborează cu organizațiile interguvernamentale privind măsurile de securitate cibernetică pentru sistemele spațiale, printre care se numără: Agenția Spațială Europeană, Comisia Europeană, Parteneriatul UE pentru Supraveghere și Urmărire Spațială, Organizația Internațională pentru Standardizare și Organizația NATO pentru Știință și Tehnologie. Cartea sa viitoare va aborda tema intersecției dintre spațiu și mediul urban și va evidenția practicile esențiale de securitate cibernetică pentru dezvoltarea durabilă a ambelor domenii. Urmare a unui program de studiu în drept spațial internațional este un alt exemplu al angajamentului său de a construi un cadru legal solid care să susțină explorarea sigură și pașnică a spațiului extraatmosferic.

Ella-Magdalena CIUPERCĂ is the Head of Service of Critical Infrastructure Protection at the Romanian National Institute for Research & Development in Informatics – ICI Bucharest. She is a Senior Researcher grade I and a university professor specialised in intelligence, security, and social psychology. She earned her Ph.D. in Sociology from Bucharest University (2004),

completed postdoctoral research in security studies between 2009-2012, and is qualified to supervise Ph.D. candidates in intelligence and security studies. Dr. Ciupercă has authored over one hundred journal and conference papers, books and technical reports in the field of social sciences, security and intelligence. She also serves as a member of editorial boards and scientific committees for national and international journals and conferences and was involved in organizations focused on the standardization and quality assurance of higher education. Throughout her career, she has held several management positions in higher education, including Dean of Faculty of Intelligence Studies and Head of Doctoral School at the Romanian National Intelligence Academy ″Mihai Viteazul″. Her research interests encompass women's studies, human-computer interaction, critical infrastructure, social innovation, cognitive biases, and social influence.

Ella-Magdalena CIUPERCĂ este Șef Serviciu Protecție a Infrastructurilor Critice în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Este cercetător științific gradul I și profesor universitar specializat în informații, securitate și psihologie socială. A obținut doctoratul în sociologie la Universitatea din București (2004), a finalizat cercetări postdoctorale în studii de securitate, între anii 2009-2012 și are abilitare pentru conducere de doctorate în domeniul studiilor de informații și securitate. Dr. Ella Ciupercă a publicat peste o sută de articole în reviste și volume de conferințe, cărți și rapoarte tehnice în domeniul științelor sociale, al securității și al informației. De asemenea, este membru în consilii editoriale și comitete științifice pentru reviste și conferințe naționale și internaționale și a fost implicată în organizații axate pe standardizarea și asigurarea calității învățământului superior. De-a lungul carierei sale, a deținut mai multe poziții de management în învățământul superior, inclusiv Decan al Facultății de Studii de Informații și Șef al Școlii Doctorale la Academia Națională de Informații „Mihai Viteazul”. Interesele sale de cercetare includ studiile de gen, interacțiunea om-calculator, infrastructura critică, inovația socială, erorile cognitive și influența socială.