ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN SPACE WARFARE

Chief Assistant Vladimir Babanov, PhD, Department of National Security and Public Administration, Faculty of Law and History, South-West University "Neofit Rilski", Blagoevgrad

Abstract: *Space operations have been profoundly affected by the swift expansion of artificial intelligence (AI) into the realm of cybersecurity. The current paper examines leading contemporary research on the topic and explores the inevitable dual role of AI for both defense and offence in space warfare. It reveals the ways AI is implemented for advanced threat detection and response in orbit for an attempt to safeguard critical space apparatuses from cyberattacks. It becomes evident that robust and flexible technology as AI poses extreme threat to space infrastructure, built decades ago. Malicious actors and states themselves scramble to both take advantage over their adversaries and protect their own vulnerable space hardware. Drawing upon the extensive work in the field, the paper discusses the technological challenges, the strategic imperatives and the lack of international governance framework necessary to lift the fog from the topic of the complex implications of AI on space security and subsequently of what appears to be a warfare. The analysis underscores the urgency for technical and legal frameworks to regulate the dangerous balance between AI, cybersecurity and the growing stakes in the last frontier of strategic competition.*

Keywords: *artificial intelligence, cybersecurity, cyberattacks, international security.*

ИЗКУСТВЕН ИНТЕЛЕКТ И КИБЕРСИГУРНОСТ ВЪВ ВОЙНАТА В КОСМОСА

Главен асистент д-р Владимир Бабанов, Катедра „Национална сигурност и публична администрация", Правно-исторически факултет, Югозападен университет „Неофит Рилски" – Благоевград

Резюме: *Космическите операции са дълбоко повлияни от бързото навлизане на изкуствения интелект (ИИ) в сферата на киберсигурността. Настоящата статия разглежда водещи съвременни изследвания по темата и анализира неизбежната двойна роля на ИИ както в отбраната, така и в нападението при космическа война. Разкриват се начините, по които ИИ се прилага за усъвършенствано откриване и реагиране на заплахи в орбита, с цел защита на критични космически апарати от кибератаки. Става очевидно, че мощни и гъвкави технологии като ИИ представляват сериозна заплаха за космическата инфраструктура, изграждана преди десетилетия. Злонамерени актьори и определени държави се стремят едновременно да получат предимство над своите противници и да защитят собственото си уязвимо космическо оборудване. Основавайки се на значимите разработки в областта, статията разглежда технологичните предизвикателства, стратегическите императиви и липсата на международна нормативна рамка, необходими за изясняване на сложните последици от въздействието на ИИ върху космическата сигурност и това, което все по-ясно се очертава като форма на война. Анализът подчертава належащата необходимост от технически и правни механизми, които да регулират опасния баланс между ИИ, киберсигурността и растящите залози в последната граница на стратегическото съперничество.*

Ключови думи: *изкуствен интелект, киберсигурност, кибератаки, международна сигурност.*

Introduction

Since the beginning of the Cold war, space is indispensable part of the national security strategies of the Great Powers. It has transformed the domains of economy, science, culture and became an arena for severe competition and conflict (De Zoysa). The technological progress brought increased reliance on satellite infrastructure located in space for communication, surveillance, navigation and intelligence which are key ingredients for military advantage over the adversaries (Kravchenko et al., 2024). Hence, AI and cybersecurity are interlinked when protecting space operations. Due to this connection, all sensitive information present within the space domain is opportunity to increase the security of the space infrastructure. However, there are many unforeseen risks that arise with AI.

The detection and countering of cyberthreats for space infrastructure could be increased by inevitable integration of AI into space systems, making possible the autonomous decision-making and timely response directly in orbit (William et al., 2025). However, the current AI technology brings inherent vulnerabilities and introduces new attack surfaces which increases the challenges for cybersecurity of the space infrastructure (Breda et al., 2022; Breda et al., 2023). The implications will continue to multiply and complicate with the increasing integration of AI by the nations and private entities into their space assets.

The current paper seeks to provide an overview of the dynamics between AI integration and the cybersecurity for the space infrastructure and its systems in the context of the growing tension in space between leading nation-states and the yet unclear role of the growing number of private entities. The author attempts to separate the importance of AI's role to enhance space cybersecurity, examine some vulnerabilities, presented by AI's integration and discuss the lack of unified strategic governance of the processes internationally. By these vectors, the article tries to shed some light on the complex topic of space warfare which is enshrouded in uncertainties, deceit and unknowns.

Emerging threats in space as a security domain

Space has long transitioned from an environment of scientific interest to a frontier of great importance for international security and warfare. The dependency on space infrastructure for societies' functioning is beyond recognized and the targeting of internet satellites over Ukraine by Russian cyberattacks in 2022 proves it in real warfare (BOTEZATU & CIUPERCĂ, 2025; Carlo et al., 2022). Disrupting the integrity of space infrastructure means paralysis of the opponent, which positions it among the prioritized targets in case of a conflict.

The classic concept of information warfare has been supplemented by a plethora of additional measures to include the space domain and shape a new way of war- the hybrid warfare. It is not limited to information campaigns but relying heavily on cyberattacks, deception and coercion through cyberspace. Space satellites can be targeted by such methods of hybrid warfare together with ground control elements to bring data manipulation, denial of service or even physical damage through advanced exploits (De Zoysa; Kravchenko et al., 2024). What is typical for such attacks is the cascading effects they bring upon military command and intelligence services. Becoming increasingly overwhelming to countermeasure, leveraging AI as a potential compensator emerges as a possible solution. However, the strategic cost of securing space infrastructure requires careful integration to existing cybersecurity measures and space hardware. (Botezatu & Ciupercă, 2025).

Blue Team AI: Enhancing Space Cybersecurity

As such possible lever in the struggle for space, AI is already used to detect, analyze and respond to complex threats but not without human in the loop in most cases. William et al. (2025) points out the AI's ability to leverage its analytical capability to detect and predict cyberthreats in orbit by identifying anomalies in the incoming data and recommending system hardening measures. AI's ability to swiftly process data from satellite networks and identify patterns of malicious actions is unmatched by the current human-driven methods for space systems cybersecurity.

Furthermore, AI has proven to be successful in providing adaptive security mechanisms for securing the space infrastructure (Botezatu & Ciupercă, 2025). AI is being implemented in vulnerability assessment, intrusion detection systems (IDS) and patch management to offload the human factor tremendously from repetitive tasks (Botezatu, 2023). The goal is to neutralize adversaries' efforts to jam, spoof or even hijack the onboard systems of the space infrastructure. AI's speed is the biggest advantage in the contemporary security landscape. (Kravchenko et al., 2024). AI also enables a proactive and autonomous security stance which ensures uninterrupted operability of the security systems.

Red Team AI: Risks in Space Applications

Cybersecurity is not only about defensive anticipation of cyberattacks – the ability to proactively and deliberately seek vulnerabilities and adversaries in cyberspace is gaining ever more traction. In this regard, AI presents a significant promise to enhancing cybersecurity efforts, but its integration introduces an unknown scope of new risks and vulnerabilities to be exploited. AI’s duality is an enormous consideration before the security strategists and their approach to the issue is yet to be found (Wilson, 2020). Breda et al. (2022 and 2023) attempt to detail the cyber vulnerabilities looming when AI is applied to space systems. The insecure data and computational resources represent the most significant vulnerabilities for AI adoption.

As AI represents a large attack surface, a compromise would limit the capability to protecting and maintaining space infrastructure operational. For example attacks in the form of input data misalignments can initiate unexpected model behavior and failure of operations. As in this example, a data poisoning is commonly used to showcase how little effort is needed to input crafted manipulations in data used by AI model that leads to its subsequent failure (Breda et al., 2023). That said, the optimism on AI usage for cybersecurity enhancement should be reconsidered and taken extremely serious due to the emergence of such a significant single point of failure.

Yet, the challenges for securing the AI itself are still technically substantial. Updating and patching AI systems on hardware in orbit and their limited computational power is just a few to mention. Combined with the harsh environment in lower earth orbit where radiation can cause malfunction of hardware or damage data, AI’s usage becomes extremely difficult (Breda et al., 2023; Carlo et al., 2022). Taking into account these vulnerabilities require the invention of a sophisticated technical framework to secure the AI systems themselves and protect them from compromise (Carlo et al., 2022). Without adequate security, AI is a vulnerability for cyberattacks itself thus turning its strategic advantages and capabilities into major flaws in the unforgiving reality of space warfare.

Technological Dual-Use and Strategic Dilemmas

The integration of AI in both offensive and defensive actions is in development and the stage of the process for each country is yet unclear. Establishing international clarity is hampered by the differences in opinions of the same countries, which take a massive risk to gain edge in the

AI arms race. This is the reason AI regulation is still vague in the countries with space programs, excluding the European union.

In their study, Graham and Thangavel (2023) showcase the necessity for responsible AI development embedded into space programs in the wake of avoiding unpredictable consequences for all stakeholders. Self-inflicted damage with AI origin is extremely likely possibility and the lack of common frameworks ensures a volatile environment where the nation-states scramble to develop advanced AI capabilities without solid safety nets (Breda et al. 2023).

There is a huge imbalance of what AI can contribute to space infrastructure security and the risks it poses to anyone using it to compromise or enhance systems. Processing vast databases is among its main advantages for critical missions, but it is prone to mistakes (William et al., 2025; Botezatu & Ciupercă, 2025) This property makes all AI models vulnerable to data poisoning and model poisoning, which might undergo undetected and render the output inoperable and potentially dangerous (Breda et al., 2023). The space environment itself is extremely hostile and comprises a restricting factor due to extreme difficulty for maintenance operations and updates deployment (Carlo et al., 2022). A compromised space system with AI in its operations is a worst-case scenario, whose outcome vary extremely.

In this context, the dilemma stands as either all stakeholders establish common rules and frameworks for ethical AI integration into space operations or everyone for acts for themselves with all risks and consequences from countries' maximum effort to gain advantage in the space domain. The second option presents a danger to the UN Outer Space Treaty from 1967 and can unlock space militarization with unseen proportions. Increased contesting for space through AI is a lucrative possibility for the main stakeholders, but the risks for their own systems are being considered heavily.

Conclusion

AI adoption holds a promise for progress in many spheres of human life. Fortification of space systems is among them but not without risks. It has its place in the activities of threat detection, incident response and others for countering the multiplying threats from militarizing space. But its deployment should not be rushed and premature due to legal unclarities and existing technical hurdles. It also brings susceptibility to attacks of different kinds, which are hard to neutralize as is also implementing defensive mechanisms in real time. The lack of international governance additionally complicates the issue and creates further instability.

For the future of space security AI does not hold clear concept. The technology is still very unreliable for such sensitive activities. Moreover, the exclusion of humans from the processes and their absence from the loop is close to impossible. Full automation is even further away given the fact that responsible, reliable and ethical AI development always includes human supervision. Utilization of AI for security of space infrastructure rises questions of technical, legal and geopolitical importance and its deployment could be either postponed or processed further into implementation as malicious usage of AI should always be considered.

Bibliography:

1. BOTEZATU, U. E. (2023). AI-Centric secure outer space operations. Bulletin of" Carol I" National Defence University (EN), 12(03), 205-221. [CrossRef].
2. BOTEZATU, U. E., & CIUPERCĂ, E. M. (2025). AI-Driven space security: Future trends and strategic imperatives for critical infrastructures. Romanian Journal of Information Technology & Automatic Control/Revista Română de Informatică și Automatică, 35(1). [CrossRef].
3. Breda, P., Markova, R., Abdin, A., Jha, D., Carlo, A., & Mantı, N. P. (2022, September). Cyber vulnerabilities and risks of AI technologies in space applications. In 73rd International Astronautical Congress (IAC), Paris, France. [CrossRef].
4. Breda, P., Markova, R., Abdin, A. F., Mantı, N. P., Carlo, A., & Jha, D. (2023). An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI. Journal of Space Safety Engineering, 10(4), 447-458. [CrossRef].
5. Carlo, A., Mantı, N., Bintang, A. S. W. A. M., Casamassima, F., Boschetti, N., Breda, P., & Rahloff, T. (2022). Understanding Space Vulnerabilities: Developing Technical and Legal Frameworks for AI and Cybersecurity in Space. [CrossRef].
6. De Zoysa, S. Final Frontier of Strategic Information Warfare and Cybersecurity Challenges to Satellites and Space Infrastructure. [CrossRef].
7. Graham, T., & Thangavel, K. (2023, October). Artificial Intelligence in Space: An Analysis of Responsible AI Principles for the Space Domain. In International Astronautical Congress, Baku, Azerbaijan. [CrossRef].
8. Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. Multidisciplinary Science Journal, 6. [CrossRef].
9. William, B., Adebayo, T., & Ibrahim, A. (2025). ARTIFICIAL INTELLIGENCE IN SPACE SECURITY: LEVERAGING AI TO DETECT AND RESPOND TO CYBER THREATS IN ORBIT. [CrossRef].

10. Wilson, C. (2020). Artificial intelligence and warfare. In 21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies (pp. 125-140). Cham: Springer International Publishing. [CrossRef].