



Defending Space in and through Cyberspace

A Fragile Stability in Space

By Major Fotios Kanellos, GR AF, JAPCC

Introduction

In a recently published book titled '2034',¹ Admiral Stavridis and Elliot Ackerman, two former military officers with deep operational and diplomatic backgrounds, tried to describe how and, apparently, when a future war with China might start. The novel provides a frightening view of an Orwellian dystopian future where the two global powers, the United States (US) and China clash, whereby powerful new forms of cyberspace weaponry and stealth capabilities are employed. According to the scenario, the hypothetical future war starts when the Chinese block the

communications systems between the ships in the Pacific Ocean, thus blinding not just the entire fleet but also the US National Command Authority.

Although the book refers to a far-in-the-future nightmarish US-Chinese military conflict, one might claim that all the mentioned trends and disruptive technologies, no matter how fictional they seem, are real, present, and ready to be used in today's modern military arsenals. Effective communications and navigations services, provided by space-based systems, are extremely vital for advanced militaries, global economies, and societies. Climate and natural disaster monitoring,

early warning systems, weather forecasting, global imaging, commercial communications systems, precise positioning, navigation, and timing synchronization, as well as surveillance and reconnaissance, are just a few of the core space-based technologies which our daily lives are totally dependent on.²

A Newly Born Domain

Since the beginning of the 21st century, technological advancements have led to increasingly affordable space capabilities for various stakeholders, including governmental, academic, and commercial entities. Launching satellites into orbit is not the sophisticated and insanely expensive activity that used to be practiced only by a handful of state superpowers. Today, small businesses, private individuals and even academic institutions can afford to manufacture, launch, and operate satellites. This leads to the ever-expanding commercialization of space activities contrary to the military domination of the domain in years past.³ Notably, with the advent of 5G and 6G mobile networks, satellites are expected to play a far more central role to provide the nearly ubiquitous, instantaneous, and maximum connectivity those networks are promising.⁴

As recently as the 15th of September 2021,⁵ the private spaceflight company SpaceX launched four civilian passengers into orbit on the first-ever mission to space with an all-civilian crew. A few months earlier, two other private spaceflight companies, Virgin Galactic and Blue Origin, launched capsules into sub-orbital space, highlighting the evolution of human spaceflight and the ease of access to an area, which was previously dominated only by governments and their space agencies.⁶

Simultaneously, the rapidly increasing number of small satellites, nanosatellites, and microsatellites in outer space has exponentially multiplied the sheer volume, diversity, and global coverage of the produced data. To collect, process, and analyse this data, newer applications and services enabled by revolutionary technologies such as artificial intelligence, quantum computing, and automation had to be created. This new era

for space, known as the 'New Space Phenomenon',⁷ has created new business opportunities and opened new markets around the world,⁸ thus increasing the growth and dependency of civil and military actors on space systems and services.

In the face of these developments, on the 4th of December 2019, the NATO Alliance adopted NATO's Space Policy and recognized space as a new operational domain alongside air, land, sea, and cyberspace.⁹ Based on the use of satellites, NATO can now respond to crises faster, more effectively, and precisely. The recognition of Space as an Operational Domain emphasizes exactly its dynamic and rapidly evolving inherent capability to enhance the Alliance's deterrence and defence posture in an age of global competition.¹⁰

Space Threat Categories

Modern space services and capabilities such as the Global Navigation Satellite System and Satellite Communications, used by both the military and civilian sectors, are considered critical national infrastructures.¹¹ These core space-based technologies have become vital assets for public safety, economic welfare, and national security of all advanced countries. However, the threats and vulnerabilities of commercial satellites and other space assets have also increased significantly during recent years, especially due to the dynamically evolving cybersecurity threat landscape.

Of course, the weaponization of space is not only facilitated through the cyberspace domain. A US report, published in 2018, argues that China and Russia are developing space weapons¹² ranging from non-kinetic physical attacks to ground sites and infrastructure to kinetic direct ascent attacks against orbiting assets. Additionally, on the 27th of March 2019, India had successfully tested its first Anti-Satellite (ASAT) missile (mission Shakti),¹³ becoming only the fourth nation to possess such a capability. In recognition of the growing threat in the space domain, on 8 March 2021, France launched its first-ever military space exercise 'Aster X 2021' simulating various space events and scenarios.¹⁴


Among the many emerging threats to space systems, the most apparent, irreversible, and likely attributable are the kinetic physical threats. These threats include attacks on static Command and Control (C2) facilities, detonations of warheads near the orbital path of a targeted satellite, and direct ascent ballistic missiles against specific satellites. More advanced versions of a co-orbital attack may also include robotic arms able to grab another satellite, thus displacing or destroying it.¹⁵ After all, satellites are lightweight devices moving at incredible speeds on predictable paths and, therefore, are extremely fragile; even a miniscule projectile can destroy them.

The threat category, which may be considered the biggest and most likely threat to the space assets, is the non-kinetic one. Without any direct physical contact, these threats can attack satellites and ground stations at the speed of light, without being observed by third parties and, thus, are difficult to attribute to one particular nation. These threats include directed energy weapons capable of damaging sensitive components and blinding critical satellite sensors, electronic attacks

(jamming or spoofing) against radio frequency signals of the up- and down-links, and sophisticated cyberattacks targeting network components, processing units, and data streams.

Cyber Threats to Space Assets

As space has developed in modern times to become the 'ultimate high ground' of information-age warfare, so too has the space arms race intensified and focused on more interconnected and computational complex cyberattacks.¹⁶ During the 20th century, the so-called 'old space' or 'traditional space' systems were designed for long-lasting missions and tailor-made solutions.¹⁷ These systems were not built with sufficient security mechanisms that would protect them from the unique and constantly evolving characteristics and challenges of cyberspace threats.



The cyberspace domain consists of a fluid, highly contested, congested, cluttered, connected, and constrained environment. As a result, the cyber threat landscape is evolving with tremendous speed, bringing new vulnerabilities and challenges to the surface. Billions of connected Internet of Things (IoT) devices have enlarged the attack surface with a diversity of attack vectors.¹⁸ Moreover, cyberattacks can be almost instantaneous, global, asymmetric, invisible, and catastrophic without even reaching the threshold of an armed attack.

Different types of threat actors are persistently trying to exploit any possible weakness in and through cyberspace to maximize the destructive effects in the space domain. Nation-states, state-proxies, cyber terrorists, criminals, hacktivists and even insiders are considered potential actors to develop sophisticated offensive cyber capabilities targeting the vulnerabilities of space systems. The potential high impact supplemented by

the low costs and minimum resources needed entices threat actors towards cyberattacks as a primary means. Whilst many of the tactics, techniques, and procedures developed in the cyberspace domain can be extensively adapted, reused, and shared among adversaries, avoiding the need for new toolsets and skills.

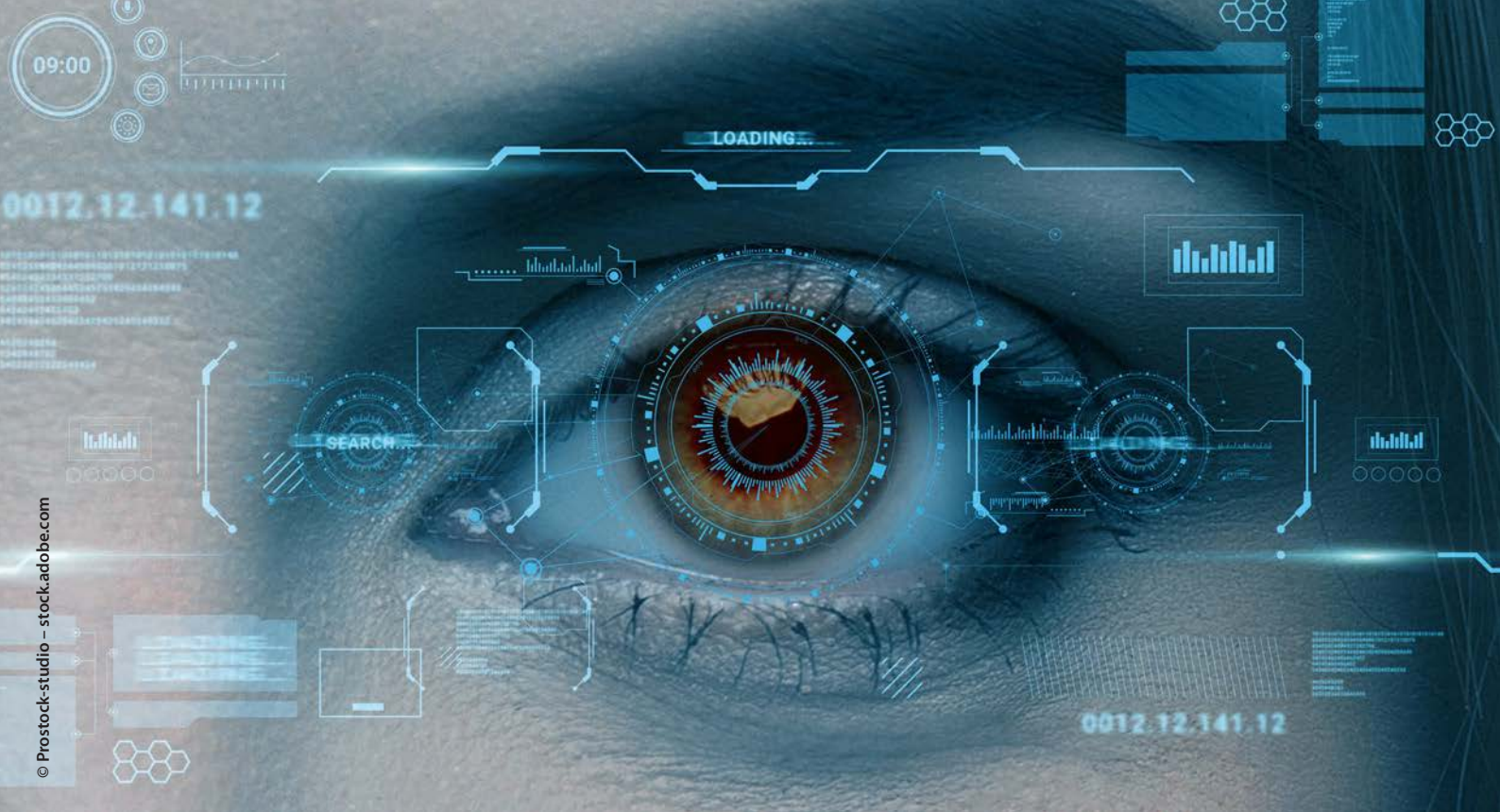
Cybersecurity requirements have to be applied to all segments that comprise an operational space system. These segments include the space, ground, link, and user portions. Significantly, the last three components rely on data systems and networks that can be compromised by injecting malicious code. Some of the most common types of cyberattacks, the distributed denial-of-service, man-in-the-middle, ransomware attacks, botnets, Advanced Persistent Threats (APTs) and the use of privacy-enhancing technologies, have developed so much that the conventional network defence tools, such as intrusion detection and prevention systems, and antiviruses may seem obsolete.¹⁹

Cyber Kill Chain

Well-resourced and trained adversaries targeting highly sensitive and national security information tend to conduct multi-year intrusion campaigns using advanced tools and techniques described as APTs. An APT method can stay undetected in a system or network until it fulfils its predetermined goals.²⁰ Those APT actors, following a kill chain model, attempt long-term and multiple intrusions and adjust their strategy based on the results – positive or negative – of these attempts.

A kill chain 'is a systematic process to target and engage an adversary to create desired effects.'²¹ According to the US military targeting doctrine, this process consists of the following steps: Find, Fix, Track, Target, Engage, and Assess. This integrated, end-to-end process is similar to a 'chain' in which all links must be fulfilled to complete the task.

Similarly, the cyber kill chain model describes the phases from conceptualization through to achieving the desired effects with respect to computer network attacks or espionage and was first introduced by Lockheed Martin.²² These phases include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2 and Actions on Objectives. Following these steps, the aggressor tries to develop a payload to breach a trusted boundary, gain authorization inside the trusted environment, and take actions towards his original objectives. These objectives may



be data exfiltration, disrupting the confidentiality of the victim's environment, or violations of data integrity and availability.

A Cyber-ASAT Case Study

One of the most critical areas of spaceflight operations is the collection and use of Space Situational Awareness (SSA) data. Almost all space stakeholders, including the US, Russia, China, and the European Space Agency, have developed modern SSA platforms. These platforms are responsible for delivering timely and accurate information from the space environment to protect both orbit and ground infrastructure.²³ Today, millions of objects of various sizes are travelling in Earth's orbit, at velocities in excess of 8 km/s that can cause catastrophic failures to satellites and launchers. Reliable tracking and prediction of potential collisions with those objects are essential for the spaceflight controllers to navigate the satellites accordingly.

However, a study from 2019 tested the development of a simulated cyber-ASAT capability that could leverage orbital simulations and genetic algorithms to artificially alter debris collision forecasts and cause direct

harm to critical space systems without firing a single rocket.²⁴ This research proved that a sophisticated cyberattack, based on the intrusion kill chains described above, can gain access to SSA's database and manipulate the objects' coordinates. A continuous, updated and transnational SSA data repository needs an extensive network of sensors distributed around the planet, providing an extensive and dynamic attack surface with numerous entry points to exploit.

An attacker taking advantage of backdoors in the network perimeter can alter the datasets so that a near-miss between the targeted satellite and a debris object can be misinterpreted as a collision. As a result, the controller will try to execute unnecessary corrective manoeuvres consuming valuable resources of the satellite and, thus, shortening its lifetime. Vice versa, the attacker may conceal a projected collision with debris depriving the controller of the ability to respond in a timely manner and save the satellite.

Conclusion

Since space systems, both military and commercial, have been considered essential parts of the NATO Nations' critical infrastructure, it is vital to address all cyber

concerns and challenges effectively for their protection. Specific cybersecurity principles and practices must be applied in every phase of the space component's development life cycle process. As the lifespan of satellites may exceed 15 years, it is critical to integrate, already from the design stage, sophisticated cybersecurity – and cryptographic – solutions, which allow the controllers to remotely install updates and to be able to respond to incidents when necessary.

The development and implementation of comprehensive cybersecurity plans for all system elements will provide the requirement for high-level cybersecurity hygiene across a whole range, from detecting network intrusions to managing the supply chain risks of all manufactured products. Therefore, the Alliance must protect their space assets and ensure continuity of operations by strengthening the national and collective resilience of their respective critical infrastructure. ●

1. F. Fukuyama, '2034', 7 July 2021, <https://www.americanpurpose.com/blog/fukuyama/2034/>, (accessed 8 October 2021).
2. J. Fritz, 'Satellite Hacking: A guide for the Perplexed', Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012–May 2013, pp. 21–50, 2013.
3. T. Lohela, 'Addressing hybrid threats in the interconnected air and space domains', Hybrid CoE Record 27, February 2021.
4. M. Griffith and C. Hocking, 'Seizing Opportunities: Four National Security Questions to Ask about the Use of Satellites in 5G Networks', September 2021, <https://www.wilsoncenter.org/publication/seizing-opportunities-four-national-security-questions-ask-about-use-satellites-5g>, (accessed 8 October 2021).
5. D. Chow, 'SpaceX makes history with first all-civilian spaceflight', 16 September 2021, <https://www.nbcnews.com/science/space/spacex-makes-history-first-civilian-spaceflight-rcna2027>, (accessed 8 October 2021).
6. D. Chow, 'Virgin Galactic's rocket reaches edge of space with Richard Branson on board', 11 July 2021, <https://www.nbcnews.com/science/space/branson-virgin-galactic-space-launch-n1273547>, (accessed 8 October 2021).
7. Ibid. 3.
8. T. Harrison et al., 'Defense against the Dark Arts in Space', Center for Strategic & International Studies, February 2021, <https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons>, (accessed 8 October 2021).
9. Ibid. 3.
10. NATO, 'NATO's approach to space', https://www.nato.int/cps/en/natohq/topics_175419.htm, (accessed 8 October 2021).
11. Space Policy Directive – 5 (SPD-5), September 2020, <https://fas.org/irp/offdocs/nspm/spd-5-fs.pdf>.
12. G. Baram and O. Wechsler, 'Cyber Threats to Space Systems', June 2020, JAPCC Read Ahead 2020, <https://www.japcc.org/cyber-threats-to-space-systems/>, (accessed 8 October 2021).
13. Drishti IAS News, 'Mission Shakti, ASAT and India', May 2019, <https://www.drishtias.com/daily-updates/daily-news-editorials/mission-shakti-asat-and-india>, (accessed 8 October 2021).
14. M. Delaporte, 'ASTER X 2021: Putting French Military Space Strategy in the New Space Orbit', April 2021, available at <https://operationnels.com/2021/04/10/aster-x-2021-putting-french-military-space-strategy-in-the-new-space-orbit/>, (accessed 8 October 2021).
15. Y. Tadjdeh, 'U.S. Strengthening Space Domain Awareness', National Defense Magazine, July 2021, <https://www.nationaldefensemagazine.org/articles/2021/7/30/us-strengthening-space-domain-awareness>, (accessed 8 October 2021).
16. J. Pavur and I. Martinovic, 'The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space', 11th International Conference on Cyber Conflict, CCD COE, May 2019, https://www.researchgate.net/publication/334422193_The_Cyber-ASAT_On_the_Impact_of_Cyber_Weapons_in_Outer_Space, (accessed 8 October 2021).
17. H. Grest, 'New Space', JAPCC Journal 29, <https://www.japcc.org/new-space-advantage-or-threat-for-the-military/>, (accessed 8 October 2021).
18. L. Maglaras and I. Kantzavelou, 'Cybersecurity Issues in Emerging Technologies', October 2021, CRC Press.
19. A. Nisioti et al., 'From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods', IEEE, July 2018, <https://ieeexplore.ieee.org/document/8410366>, (accessed 8 October 2021).
20. E. Hutchins et al., 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', Lockheed Martin, January 2011, <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>, (accessed 8 October 2021).
21. Ibid.
22. P. MacKenzie and F. Kanellos, 'A Comprehensive Approach to Countering Unmanned Aircraft Systems: Cyberspace Operations', JAPCC Book 2020, <https://www.japcc.org/c-uas-cyberspace-operations/>, (accessed 8 October 2021).
23. Ibid. 16.
24. Ibid.

Major Fotios Kanellos

graduated from the Hellenic Air Force (HAF) Academy in 2003 as an Electrical Engineer specializing in Telecommunications and Computer Science. He holds three Master degrees, one in Technical-Economic Systems from the National Technical University of Athens (NTUA), one in Environmental Sciences from the University of Patras and another in European and International Studies from the National and Kapodistrian University of Athens.

He served as an inspection engineer for T-2 C/E aircraft and system engineer for the T-6A Flight Simulator at the Hellenic Air Training Command in Kalamata. His previous appointment was at the HAF Support Command managing IT and Cybersecurity projects. Currently, he is the Cyberspace SME at the JAPCC.

