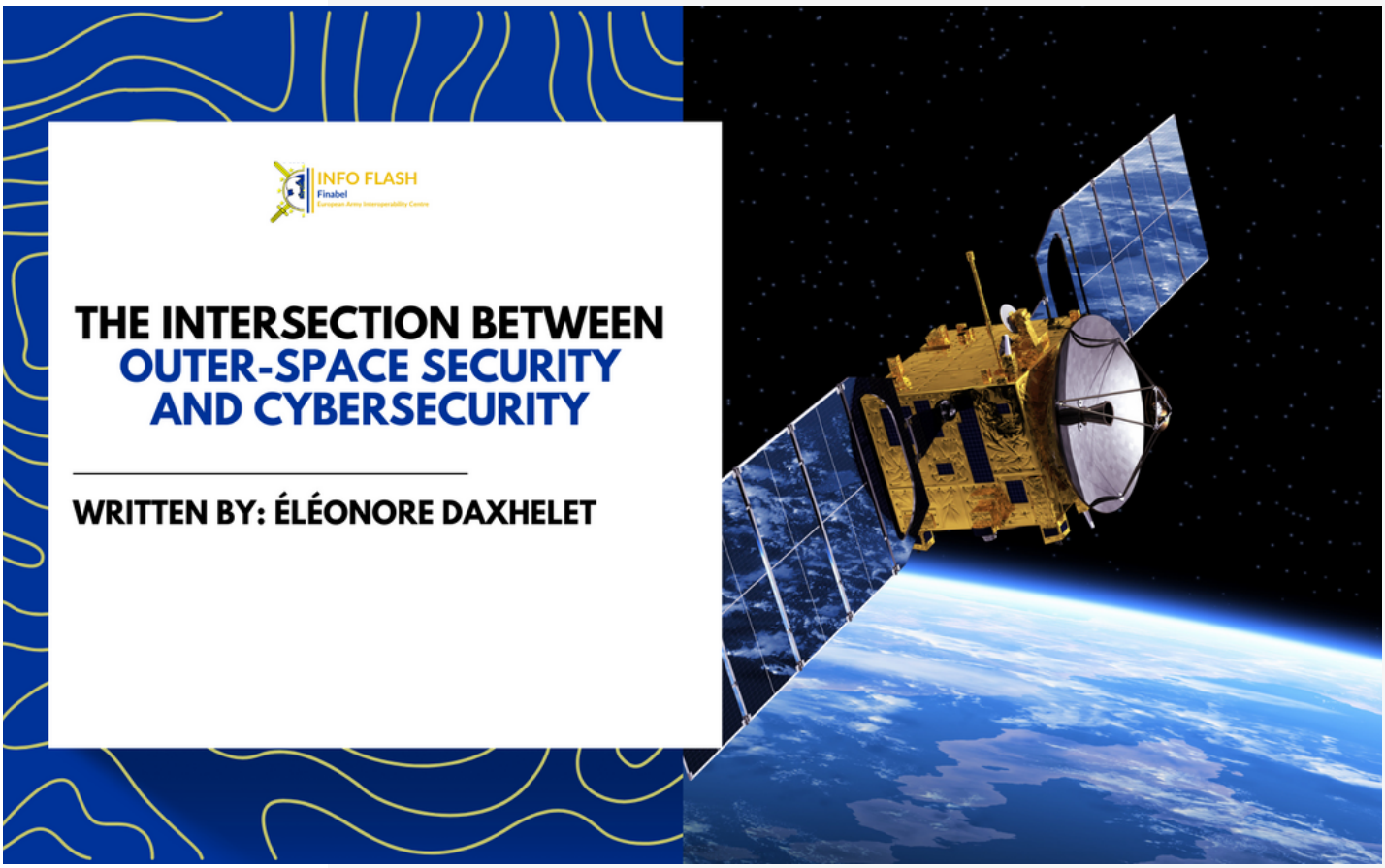
INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

JULY 2023

THE INTERSECTION BETWEEN OUTER-SPACE SECURITY AND CYBERSECURITY



WRITTEN BY
ÉLÉONORE DAXHELET

EDITED BY
MIGUEL ANDRES REYES CASTRO

SUPERVISED BY
PAUL DYBJER

Introduction

The concept of space security first appeared during the Cold War, in the context of the space race between the USA and the USSR. Since the 1990s, the number of space actors has significantly increased, including new national, international and private stakeholders. Space technologies, especially satellites, have gained importance for several aspects of everyday life, and are crucial for commercial purposes, public services and military operations. Particularly in the latter case, space technologies represent a major asset for communication, surveillance and planning.

Due to their significance and the possibilities they offer, space assets are attractive targets in conflicts. Anti-satellite weapons, both kinetic and non-kinetic, are being developed and tested to destabilise and counter an opponent's space activities. These weapons can take the form of cyber-attacks; according to Oakley (2020, p. 155), "the space domain is the perfect place for cyber warfare". In addition, space assets are particularly vulnerable: "the cyber resilience of space assets is underestimated, and satellites are not sufficiently cyber-protected" (Pražák, 2021, p. 403).

As the reliance on space technologies for economic, civilian and military activities deepens and the number of actors increases, the risk of cyber-attacks against space assets is growing. This has major implications for national security, because critical infrastructure largely relies on space systems (Falco, 2018). In parallel, cyberspace is becoming increasingly relevant for the security sector with the advancement of hybrid warfare targeting critical infrastructures, both on Earth and in space. As a result, research on the intersection between cyberspace and outer space is emerging.

In this context, this paper aims at understanding the security aspect of the cyber-space intersection. It focuses on how space is becoming a battleground for cyberwarfare. The main objective is to better understand the vulnerability of space assets to cyber-threats and its consequences on national and international security, in order to grasp the security implications of space-based cyber-attacks.

Space and Cyberspace: Two Intertwined Domains

In December 2019, NATO officially recognised outer space as a strategic domain, alongside land, sea, air and cyberspace. Space security is, however, all but a new topic. It entered geopolitics as early as the 1950s, at the beginning of the Cold War (Baylon, 2014). Although outer space was originally hoped to be used solely for scientific purposes, both the USA and the USSR developed technologies that were able to disrupt the other's satellites and space missions (Baylon, 2014). Therefore, as initially prescribed in the Outer Space Treaty of 1967, "space security entails the possibility to access and use space for all nations" (Antoni, 2020, p. 10), thus highlighting the primary military and national aspect of space.

However, since the 1990s, new actors have entered the space domain, for commercial and civilian purposes mainly. Space has thus become a "contested, congested and competitive strategic domain" (Pražák, 2020, p. 397). The military aspect has nevertheless persisted, and "outer space is widely militarized" (Pražák, 2020, p. 397).

In addition, space is far from being a remote area; indeed, "space systems are essential to and underpin the critical infrastructure that enables our global economy and military presence, and act as a central point of failure across various industries" (Falco, 2018, p. 4). These systems directly affect daily life on Earth, including communications, GPS, weather forecasts and Earth monitoring, to name a few (Paulauskas, 2020). This is why "Earth orbit is now a major strategic arena in the conduct of international politics for all political actors on Earth itself" (Bowen, 2020, p. 2). Consequently, a new definition of space security must include "aside [from] the military dimension, also, economic, societal and environmental dimensions" (Sheehan, 2015 as cited in Antoni, 2020, p. 10).

Space systems represent an important asset for the defence sector. Satellite imagery is crucial for informing decision-making and for situational awareness. It provides significant information regarding an actor's infrastructure and movements, allowing for early warnings (Paulauskas, 2020). Satellites are also used for intelligence gathering and surveillance purposes. They also provide data regarding the battleground and weather conditions, which enhances mission planning (Paulauskas, 2020). Communication is also dependent on satellites. Overall, NATO (2023) has highlighted the importance of space for its deterrence politics. .

At the same time, cyberspace has also penetrated many aspects of contemporary society. Just as space, it was initially "conceived for research collaboration between universities and government think tanks in the 1960s before undergoing explosive growth for mainstream commerce from the 1990s onwards" (Baylon, 2014, p. 7). Since then, cyberspace has expanded and has been widely recognised as a strategic domain. Cyberspace and outer space are highly intertwined and dependent on one another, affecting society in a fundamental way (Baylon, 2014). Indeed, "the internet increasingly depends on space-enabled communication and information services. Likewise, the operation of satellites and other space assets relies on internet-based networks" (Filder, 2018).

All these new dynamics in outer space, from the intensification of the use of space assets to the increase in the number of players, "have increased the level of vulnerability of cyberspace and space-based infrastructures" (Al-Rodhan, 2020, p. 2). Some nation states have already integrated a military dimension to their space strategy and are developing counter-space technologies, like Russia or China (NATO, 2023). Furthermore, because of the low cost and high effectiveness of cyber-attacks, cybercrime is also a major challenge for space security (Filder, 2018; Baylon, 2014; Oakley, 2020).

Due to their central role for the functioning of critical infrastructures and their reliance on cyberspace, space systems are attractive targets. They can easily serve as "a central point of failure to massive systems" (Falco, 2018, p. 6). Furthermore, security regulations regarding the cybersecurity of space assets are lacking, whilst space systems cover a vast area available for potential attacks (Falco, 2018). As a hacker's main goal is to minimise costs while maximising impacts (Falco, 2018), space assets appear as ideal targets to initiate cyberwarfare operations (Oakley, 2020). In this context, "space warfare is a realistic prospect because space technologies are at the heart of military weapon systems, intelligence, logistics and economics, and the tools for harassing or disabling satellites are spreading" (Bowen, 2020, p. 1). Cyber-threats are especially a significant challenge to space security, encompassing serious national security implications.

Cyber-Threats in Outer-Space

The centrality of space systems to many industries and critical infrastructure make them attractive targets. Indeed, by impacting a central point of failure, a cyber-attack on a satellite can impact multiple systems (Falco, 2018), greatly damaging society. Furthermore, cyber-attacks are relatively cheap, especially in the space domain. Other anti-satellite weapons (ASATs), like missiles or electromagnetic pulses, require budget, time and specific infrastructures. However, in space, contrary to other warfighting domains, cyber-attacks are more beneficial than kinetic attacks from a cost-benefit perspective (Oakley, 2020, p. 155).

As explained by Manulis et al (2020), typical satellite architecture is composed of two main segments. The ground segment includes both the facilities, ground station and control centre of the space asset, i.e. the provider terminals, and the final user, i.e. the customer terminals. The space segment represents the space mission in itself, i.e. the satellite in orbit, either alone or as part of a constellation.

The space system is thus a large target, "comprising a space-based segment, a ground control terminal, data links and the actual user. It is enough to take out one segment and the system becomes useless" (Paulauskas, 2020). In this context, space cyber threats seem to be the most effective, because they can target and have an impact on each of the segments making up a space mission (Paulauskas, 2020).

Cyber-attacks on the terrestrial segment

According to Manulis *et al* (2020, p. 292), "compromising the ground station is ultimately the easiest way to control a satellite as it provides the equipment and software required to legitimately control and track it". Several ways to do so exist, for instance, ground facilities can be physically attacked by gaining unauthorised access (Manulis *et al*, 2020). This could give an attacker direct access to the space mission and provide the opportunity to steal important data and information. Another example is "computer network exploitation", which allows a hacker to compromise the network to which a station is connected and gain unauthorised access to mission operations, via phishing for instance (Manulis *et al*, 2020, p. 293).

Hackers can also choose to target the user and "the technology that was enabled by the space system" rather than directly compromising the space asset (Falco, 2018, p. 7). As detailed by Falco (2018), it is possible to hack into a satellite provider, in order to identify and steal IP addresses of satellite internet users. This allows a hacker to initiate connections, while rendering detection difficult, as the normal user's performance is not noticeably affected. Nevertheless, this kind of attack can cause serious damages, such as intercepting or injecting data into systems connected to the targeted IP address, potentially leading to the override or crash of critical systems (Falco, 2018). This method has been used for instance by the Russian cyber-espionage group *Turla*, to carry out and "hide cyber-espionage operations against countries ranging from the US to the former Eastern Bloc" (Falco, 2018, p. 7).

Cyber-attacks on the space segment

Although space assets are difficult to physically attack once launched, they can still be the target of cyber threats (Manulis *et al*., 2020). Falco (2019) has reviewed several examples of US satellites that have been hacked or interfered with. In some cases, hackers "achieved command and control of the satellites" for several minutes (Falco, 2019, p. 5). One example is the 2011 NASA's Jet Propulsion Laboratory (JPL) attack, during which "hackers gained full operational control" (Falco, 2019, p. 5). According to a report on the incident (Falco, 2019, p. 5):

"The intruders could: 1) modify, copy, or delete sensitive files; 2) add, modify, or delete user accounts for mission-critical JPL systems; 3) upload hacking tools to steal user credentials and compromise other NASA systems; and 4) modify system logs to conceal their actions."

The hacking of satellites can thus have serious security consequences. It could be the case that by gaining full operational access to a small satellite with propulsion, for instance, a malicious actor could direct it to force a collision with other satellites (Falco, 2018; Al-Rodhan, 2020; Baylon, 2014). This would add waste in an already crowded domain, threatening other satellites by risking collision with the resulting debris (Pražák, 2021; Pellegrino, Stang, 2016). This, however, can be a difficult task and require specific expertise (Manulis et al., 2020).

Hackers can also perpetuate sophisticated jamming operations by using "Software-Defined Radios (SDR) and digital signal processing software for radio functionality" (Manulis et al, 2020, p. 294). Indeed, insufficient checks in the processing of these frames can create a vulnerability known as a buffer overflow, i.e. when more data is written into a memory buffer than it can handle, causing the excess data to overwrite adjacent memory locations. This can lead to unpredictable behaviour and potentially enable attackers to execute malicious code or disrupt the normal operation of the system. This could result in a denial-of-service condition, jamming communications (Manulis et al, 2020).

Cyber-attacks on communications between segments

Finally, it is possible for hackers to disrupt the communication system between the space engine and the ground facilities or user. A first kind of attack is "the interception of data over a communication channel", or eavesdropping (Manulis et al, 2020, p. 293). This can have major security implications if the communication intercepted concerns important information on military operations. Since the channels of communications between ground and space systems are simply signals sent into the atmosphere, they are susceptible to being intercepted (Manulis et al., 2020). This is particularly problematic if the information is not properly encrypted, making it difficult to read and understand.

A second possible attack is jamming, which "is the act of overpowering a RF signal of a particular frequency with a higher power one of the same frequency, in order to disrupt communications between the ground station and satellite, or vice versa" (Manulis et al, 2020, p. 293). It can, for instance, serve to compromise GPS systems. As described by Falco (2018, p. 8), GPS systems "rely on satellites to triangulate specific positions on Earth. Introducing noise into the receiver spectrum of the GPS satellite can cause the failure of a GPS receiver on earth to provide a reading."

A last, and more advanced cyber-attack, is spoofing. Contrary to jamming, spoofing requires to manipulate the signal received from or by a satellite, rather than simply disrupting it (Falco, 2018). It can be defined as "the art of transmitting a signal, appearing to be legitimate, but sending erroneous data for your own purposes" (Manulis et al, 2020, p. 294). Because spoofing is less detectable than jamming, the signal appears to work as intended and the trust in the systems and the signal remains intact (Falco, 2018). Consequently, this renders such an attack more dangerous.

Concluding remarks: The Importance of Space Cybersecurity

Cyber-attacks targeting space systems have major security implications, especially for the security and defence sector, which greatly depend on them. As stated by Paulauskas (2020), "without space, operational commanders would be mostly deaf and blind". This explains why space systems have been and will continue to be targets of cyber-operations. Indeed, this type of attack is the most effective way of disrupting a space mission and related terrestrial activities.

However, despite space being essential to the functioning of modern society and the defence sector, "neither international law nor diplomacy has grappled effectively with space cybersecurity" (Filder, 2018). The European Union recognised space as a strategic domain in its 2022 Strategic Compass (European Commission, 2023), and called for an "EU Space Strategy for Security and Defence that will allow the EU to protect its space assets, defend its interests, deter hostile activities in space and strengthen its strategic posture and autonomy" (EEAS, 2023). Finally, NATO also adopted a Space Policy in 2019 (NATO, 2023). However, cyber threats in space are not fully grasped and regulations for the cybersecurity and cyber-resilience of space assets are lacking. In the end, due to the high cost of space systems and their significance for the functioning of critical infrastructure, industries, society and the security sector, investing in space cybersecurity should be a requirement for national security.

Bibliography

Al-Rodhan, N. (2020). Cyber security and space security. The Space Review, 26. https://www.academia.edu/download/63439749/Cyber_security_and_space_security_SPACE_REVIEW_2020052620200527-100914-8wj8nx.pdf.

Antoni, N. (2020). Definition and Status of Space Security. In Schrogl, K.U. (Ed.) Handbook of Space Security. Springer, Cham. https://link-springer-com.dcu.idm.oclc.org/referenceworkentry/10.1007/978-3-030-22786-9_126-2.

Baylon, C. (2014). Challenges at the intersection of cyber security and space security: Country and International Institution Perspectives. [Research Paper]. Chatham House. https://nsarchive.gwu.edu/sites/default/files/documents/5023659/United-Kingdom-Government-Chatham-House-Research.pdf.

Bowen, B. E. (2020). War in space: Strategy, spacepower, geopolitics. Edinburgh University Press. https://doi-org.dcu.idm.oclc.org/10.1080/03071847.2022.2055389.

European External Action Service (2023, April 14). EU Space Strategy for Security and Defence. European External Action Service. https://www.eeas.europa.eu/eeas/eu-space-strategy-security-and-defence-0_en.

European Commission (2023, June 07). EU Space Strategy for Security and Defence for a stronger and more resilient European Union. European Commision. https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-and-defence_en.

Falco, G. (2018). Job one for space force: Space asset cybersecurity [Paper]. Belfer Center for Science and International Affairs, Harvard Kennedy School. http://osa-public.s3.amazonaws.com/papers/csp_falco_space_asset-final.pdf.

Falco, G. (2019). Cybersecurity principles for space systems. Journal of Aerospace Information Systems, 16(2), 61-70. https://arc.aiaa.org/doi/abs/10.2514/1.I010693.

Fidler, D. P. (2018). Cybersecurity and the new era of space activities. Digital and Cyberspace Policy Program. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3665&context=facpub.

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., Davis, A. (2021). Cyber security in new space: analysis of threats, key enabling technologies and challenges. International Journal of Information Security, 20, 287-311. https://link.springer.com/article/10.1007/s10207-020-00503-w.

NATO (2023, May 23). NATO's Approach to Space. NATO. https://www.nato.int/cps/en/natohq/topics_175419.htm.

Oakley, J.G. (2020). Cybersecurity for Space. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5732-6.

Paulauskas, K. (2020, March 13). Space: NATO's Last Frontier. NATO. https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html.

Stang, G., & Pellegrino, M. (2016, July 7). Space Security for Europe [Report N° 29]. European Union Institute for Security Studies. https://www.iss.europa.eu/content/space-security-europe

.

Pražák, J. (2021). Dual-use conundrum: Towards the weaponization of outer space? Acta Astronautica, 187, 397–405. https://doi-org.dcu.idm.oclc.org/10.1016/j.actaastro.2020.12.051.