The War in Ukraine from a Space Cybersecurity Perspective

ESPI European Space Policy Institute

Report:
Title: "ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective"
Published: October 2022
ISSN: 2218-0931 (print) • 2076-6688 (online)

Editor and publisher:
European Space Policy Institute (ESPI)
Schwarzenbergplatz 6 • 1030 Vienna • Austria
Phone: +43 1 718 11 18 -0
E-Mail: office@espi.or.at
Website: www.espi.or.at

Cover design: www.rainfall.ro
Internal layout design: www.copylot.at
Cover page picture credit: Shutterstock

TABLE OF CONTENTS

1 INTRODUCTION

On February 24th 2022, Russia invaded Ukraine by launching a series of attacks against Kyiv as well as several cities located at the border of Russia and Belarus.[1] Concurrently, Russia conducted a cyberattack against ViaSat's KA-SAT GEO satellite network, which was used by the Ukrainian army, thereby providing a concrete example of the use of cyber operations in complementarity with conventional military operations on land, sea, and air.[2]

In the space community, the KA-SAT cyberattack raised a broader debate regarding the cybersecurity of space systems and the protection of critical infrastructures.

Indeed, the digitization of space systems, the increasing relevance and criticality of space systems in military operations, and the growing integration of satellites into the digital infrastructure make them more vulnerable to cyber threats.

While space cybersecurity is not a new topic, protecting satellites against cyberattacks has been a difficult endeavour due to the peculiar nature of the orbital environment and the unique characteristics of space hardware. Satellite operators do not always know whether an interference is due to a natural space weather event or an attack. Operators cannot physically access the system in orbit to repair it or assess the damage of an attack. The space environment also render many traditional cybersecurity solutions inadequate as they have to withstand long-distance transmissions, limited processing capabilities, and massive signal footprint without significantly hampering latency and performance.[3]

Additionally, cyber threats on space systems have long been overlooked in public policies[4] and have only been recently acknowledged in space and defence policies, leaving some policy and legal gaps to ensure the proper cybersecurity of the space infrastructure.

The KA-SAT cyberattack and the war in Ukraine raise many outstanding questions regarding the cybersecurity of the space infrastructure from an industrial, political, legal, and military perspective.

The KA-SAT cyberattack may be considered as a good illustration of the current state of cybersecurity in the commercial space sector as well as a representative case of the evolution of the militarization of outer space through cyber means, enabling to highlight key trends and lessons to learn.

As the war in still ongoing and additional information are unveiled on a daily basis, it is important to note that the study is based on open-source information available at the time of writing (August 2022).

[1] Bloomberg. 2022. A Visual Guide to the Russian Invasion of Ukraine. [online] Available at: <shorturl.at/amopr> [Accessed 27 August 2022].
[2] Kostyuk, N. and Gartzke, E., 2022. Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. [online] Texas National Security Review. Available at: <https://bit.ly/3U1y3lq> [Accessed 16 August 2022].
[3] Targett, E., 2022. US agencies tells users to deploy 'independent encryption' across satellite comms. It's not that easy. [online] Available at: <https://bit.ly/3BbouxM> [Accessed 27 August 2022].; Wilde. G., 2022. Twitter. [online] Available at: https://twitter.com/gavinwilde [Accessed 27 August 2022].
[4] Livingstone, D. and Lewis, P., 2016. Space, the Final Frontier for Cybersecurity?. [online] Chatham House. Available at: <https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity> [Accessed 5 August 2022].

2 SETTING THE SCENE: UNDERSTANDING THE INTERDEPENDENCE AND COMMONALITIES BETWEEN SPACE AND CYBERSPACE

Cyberspace and outer space share many commonalities as they are open, shared, limitless, cross-border, and rather intangible and unregulated domains, which are both used for military, civil, and commercial purposes.

In the past few decades, several phenomena have been occurring in both space and cyberspace, which resulted in an increased vulnerability of space systems to cyberattacks and an increased attack surface:[9]

The shift from broadcast to broadband

The satellite communication sector has greatly evolved in the past few years, shifting from Direct Broadcast Services (DBS) and Direct-To-Home (DTH) services using GEO satellites to internet satellite broadband using LEO constellations to respond to the changing users' needs stemming from the digital revolution. **Space is becoming part of the broader digital infrastructure and is increasingly integrated with terrestrial networks**.[10] As the digital infrastructure is the backbone of the economy, society, and the military, it makes satellites floating targets for cyberattacks.

The digitisation and digitalisation of space

Space systems have become increasingly digitised. Spacecraft have gone from analogue electronics to digitized systems, which are increasingly using IP protocols, software-defined radios, digital payload, and on-board data processing.[11] This trend is growing with new technologies such as cloud ground stations or fully software-defined satellites. As a result, many space operations move from the physical to the software layer of cyberspace. This growing connectivity exposes space systems to cyberattacks and increases the attack surface. In addition, **the space sector at large has been progressively digitalised.** Most processes in the design, manufacturing, testing, control, and operations of satellites are now based on digital technologies. This dependence on digital technologies led to the extension of the attack surface throughout satellites' life cycles.[12]

Defining cyberspace

To understand cyber threats on space systems, it is important to define cyberspace. It is often described as composed of three layers, which are interrelated and in which attacks on one layer can generate effects on the others:[5]

A physical layer: the equipment, infrastructure, and hardware, such as computers, data centres, submarine-cables, smartphones, and satellites that enable data to flow through cyberspace.[6] These infrastructures are geographically located and therefore can be physically attacked and destroyed.

A logical or software layer: the lines of codes in various programming languages or binary information that machines will transform data into readable information for the end user. It also refers to software and protocols such as the TCP/IP protocol that will allow machines to interact with one another and enable the information to be distributed in the form of data packets.[7]

A cognitive or social layer: the actual information, digital content and data exchanged in cyberspace as well as end users, their digital identities, and their interactions.[8]

[5] Ventre, D. 2017. Cyberguerre in : Durieux, B., et al., 2017. Dictionnaire de la guerre et de la paix. Paris: PUF. p.339.
[6] Limonier, K., 2018. Ru.Net, Géopolitique Du Cyberespace Russophone. Les Carnets de l'Observatoire, L'inventaire.
[7] Douzet, F., 2014. La géopolitique pour comprendre le cyberespace. Hérodote.
[8] Kempf, O., 2014. Alliances et mésalliances dans le cyberespace. Paris: Économica.
[9] Poirier, C., 2020. Interdependences Between Space and Cyberspace in a Context of Increasing Militarization and Emerging Weaponization of Outer Space—A French Perspective in: Froehlich, A., 2020. Outer space and cyberspace. Springer.
[10] Nardon, L., 2017. European Space Programs and the Digital Challenge, Etudes de l'Ifri, Ifri.
[11] Blount, P., 2017. Satellites Are Just Things on the Internet of Things. Air and Space Law, 42(Issue 3), pp.273-293.
[12] Poirier, C., 2022. ESPI Series on Cybersecurity. [online] IISL Space Law Knowledge Constellation. Available at: <https://constellation.iislweb.space/clemence-poirier-espi/> [Accessed 18 August 2022].

The militarisation of space and cyberspace

Outer space has been militarised since the dawn of the space age. This is an old phenomenon, which can be defined as the use of space for military purposes and to support military operations on Earth. During the Cold War, this militarisation was first seen from a kinetic perspective in line with the development of ballistic missiles and nuclear weapons. From the 1990s, the militarization of outer space was mostly perceived from an operational perspective. Space systems started to be considered as critical enablers of military operations on Earth.[13] Earth observation, navigation, and satellite communications became essential for command and control, intelligence, reconnaissance, surveillance, precision strikes, deploying troops and synchronizing weapons on the battlefield. **It is only recently that the militarisation of space started to be considered from a cyber perspective**[14] with the official acknowledgment of cyber threats on space systems in space policies (EU, 2016; France, 2019; Estonia, 2020; UK, 2021). Today, a new phenomenon is emerging, the weaponization of outer space, which is defined as the deployment and use of weapons in outer space.[15] The weaponization of outer space is currently characterised by discrete threats below the threshold of violence and *casus belli* such as hostile approaches, cyber or electronic attack on space systems.[16] **Space and cyberspace are also interlinked to the extent that space is now militarised and weaponised through cyber means.** This phenomenon is consistent with the militarisation of cyberspace. In the 1980-1990s, the militarization of cyberspace was very limited both in terms of attacks, capabilities, and threat agents, which were mostly individual hackers and a few States. By the end of the 1990s, the militarization of cyberspace expanded to more threat agents, in particular criminal groups looking to make money through viruses and computer worms. This period also saw the emergence of hacktivists, which were conducting cyberattacks to serve a cause. From the early 2000s, cyberspace has been significantly militarized by a wide range of threat agents such as hackers, criminal groups, State actors, and their proxies to conduct targeted and sophisticated attacks to serve economic, political, social, and military interests.[17] Since the 2010s, **cyberspace is not only militarised but also progressively fragmented and territorialized** as several States are making sovereignty claims on parts of cyberspace and attempting to gain the ability to disconnect their internet infrastructure from the world wide web.[18]

Space and cyberspace as warfighting domains

Space and cyberspace are competed, congested, and contested domains. Both space and cyberspace have been progressively acknowledged in defence policies, strategies and doctrines, as warfighting domains, alongside land, sea, and air. This acknowledgement means that the perspective of an open conflict in these domains is possible. However, it does not mean that space and cyberspace are strictly separated from other domains. Space and cyberspace are not only integrated into other domains but also encompass and link domains together in joint operations. At the European level, **the EU Cyber Defence Policy Framework of 2018**, recognizes cyberspace as a warfighting domain, outlining that *"cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space."* **The Strategic Compass of 2022** also considers both outer space and cyberspace as operational domains in which the EU can act.[19] As defence issues remain the prerogative of EU Member States, some of them have also recognized space and cyberspace as warfighting domains. At the international level, the North Atlantic Treaty Organization (NATO) recognized cyberspace as an operational domain as early as 2016. In 2019, it adopted a space policy, in which space is also

[13] Todd, H. et al, 2020. Space Threat Assessment 2020. CSIS. p.4
[14] Unal, B., Zatti, S., 2020. Cybersecurity of space-based weapons systems. Webinar. SGAC Space and Cybersecurity PG.
[15] Pasco, X., 2017. Le nouvel âge spatial. De la Guerre froide au New Space. Paris: CNRS Ed.
[16] Becht, O. and Trompille, S., 2019. Rapport d'information sur le secteur spatial de défense. Assemblée nationale. Paris.
[17] Healey, J., 2013. A fierce domain. Conflict Studies Association.
[18] Douzet, F., et al. 2020. Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol during the Ukrainian Crisis. 2020 12th International Conference on Cyber Conflict (CyCon).
[19] Council of the European Union. 2022. A Strategic Compass for Security and Defence. 7371/22

considered as an operational domain.[20] This recognition leads to the release of defence strategies and doctrines dedicated to these domains, changes in postures (defensive, counter-offensive, offensive), new capabilities and uses, and changes in governance (cyber, space commands).

The concept of multidomain operations

Space and cyberspace are poised to become more interdependent in armed conflicts with the emergence of concepts such as "multidomain operations". This is particularly relevant in the context of this report as the concept of multidomain operations was developed following the annexation of Crimea in 2014 as a way for the United States to counter and defeat *"near-peer adversaries"* such as China and Russia.[21] These countries are conducting *fait accompli* operations by using Anti-Access/Area Denial (A2/AD) capabilities (jamming, spoofing, cyberattacks) against systems that embody the operational superiority of Western armies such as aerial and space systems, while targeting assets or or territories, which are below the threshold of armed conflicts, thereby paralyzing Western armies.[22] To regain superiority and freedom of action, multidomain operations were therefore conceptualized by the United States as *"operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives".*[23] According to Philippe Gros and Thibault Fouillet from the Foundation for Strategic Research, **space and cyberspace are considered as critical enablers of this doctrine to connect and synchronize all systems and weapons together on the battlefield through a global architecture of interdependent networks.**[24] It is about creating and converging effects in space and cyberspace but also integrating space and cyberspace in other domains to generate a "physical saturation" (coordinated operations in several domains) to lead to a "cognitive overload" and paralyze the adversary's decision-making loop and overcome their A2/AD capabilities. Similar doctrines are currently being considered by European countries and by Russia (New Generation Warfare).[25]

Defining a cyberattack on a space system

There is no universal definition of a cyberattack, let alone of a cyberattack on a space system. Similarly, there is no universal definition of a space weapon and therefore no definition of a cyber weapon in outer space. However, the NATO CCDCOE Tallinn Manual 2.0 attempted to provide a definition of a cyberattack on a space system, distinguishing **"space-enabled cyber operations"** from **"cyber-enabled space operations"**. Cyber operations enabled by space assets are activities, which rely on cyber infrastructures based on space systems but do not generate effects in outer space. This usually only involves the use of satellite communications as a means of connectivity or data relay to conduct a cyber operation. However, space operations enabled by cyber means are considered as the conduct of space operations through cyber means, which are generating effects in outer space. It includes cyber operations, which attempt to disturb, take control, destroy, or affect the functioning of a space system.[26]

[20] NATO. 2022. NATO's overarching Space Policy. [online] Available at: <https://bit.ly/3BIWiUN> [Accessed 8 August 2022].
[21] Feickert, A., 2021. Defense Primer: Army Multi-Domain Operations (MDO). Congressional Research Service.
[22] Fouillet, T., 2020. La Constellation Multi-Domaine, Séminaire Multidomaine. Séance 4. IESD ; Bouhet, P., 2019. Le multidomaine. Fondements et Hypothèses. DSI Hors-série n°67, p.68-69
[23] U.S Army. 2018. The US Army in Multi-Domain Operations 2028. TRADOC. Pamphlet 525-3-1. p.GL-7
[24] Gros, P., Fouillet, T., 2020. L'armée française face au tournant multi-domaine. Séminaire Multidomaine. Séance 6. IESD
[25] Fouillet, T., .2020. op cit.
[26] Schmitt, M., 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. NATO Cooperative Cyber Defence Centre of Excellence.

3 THE KA-SAT CYBERATTACK: LESSONS TO LEARN FOR SPACE CYBERSECURITY

On February 24th, only one hour before invading Ukraine, Russia launched a cyberattack on ViaSat's KA-SAT satellite network, which was used by the Ukrainian army.

3.1 The KA-SAT cyberattack

Targeted systems and companies. The attack did not target the KA-SAT satellite itself, but one single *"consumer-oriented partition of the KA-SAT network"*, which is owned by the U.S. company Viasat but operated by Eutelsat's subsidiary Skylogic.[27] This raises questions on the responsibilities and liabilities of each company for ensuring proper cybersecurity.

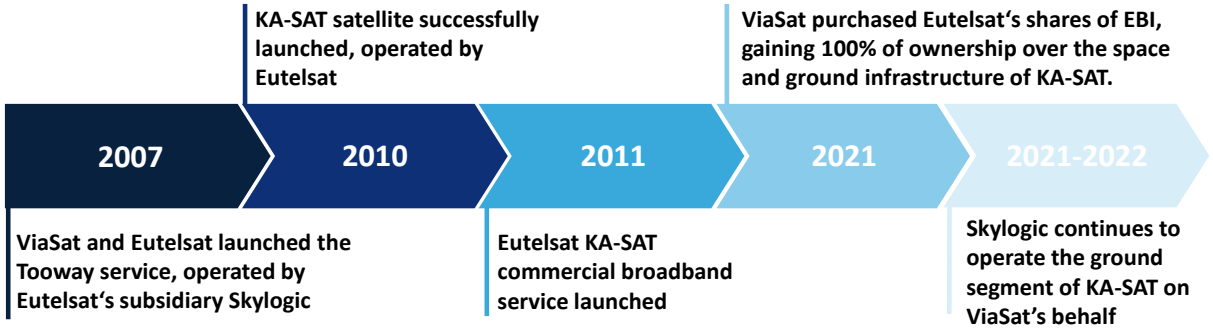

Figure 1: Timeline of KA-SAT's ownership

Operational mode. While some details are still missing due to limited information provided by ViaSat, the attack seems to have taken place in two stages.[28]

1st stage	**Entry point:** users' modems	A Denial of Service (DoS) attack was conducted against internet modems[29] (Tooway, SurfBeam2, SurfBeam2+), which were located in Ukraine and used by the Ukrainian government, the armed forces, and security services. High volumes of malicious traffic were pushed into the network by illegitimate SurfBeam2/2+, making it difficult for legitimate modems to stay online.[30]
2nd stage	**Entry point:** VPN appliance	Then, the attacker entered a ground-based network by exploiting a misconfiguration of a Virtual Private Network (VPN) appliance, which enabled the attacker to gain remote access to the management segment of ViaSat's KA-SAT network. After compromising this entry point, the attacker went deeper into the network (lateral movement), reaching a specific segment that was used to manage and operate the network.[31] It enabled the attacker to gain control of the management segment and execute commands, which facilitated the upload of a wiper malware (named AcidRain)[32] onto users' modems, subsequently erasing the hard drive of KA-SAT's internet modems, disconnecting them from the KA-SAT network and rendering them unusable.[33]

[27] ViaSat. 2022. KA-SAT Network cyberattack overview. [online] Available at: <https://bit.ly/3QHsBax> [Accessed 9 August 2022].
[28] SentinelOne. 2022. A Modem Wiper Rains Down on Europe. [online] Available at: <https://bit.ly/3d4ua4X> [Accessed 9 August 2022].
[29] SentinelOne 2022. Op cit.
[30] ViaSat. 2022. Op cit.
[31] ViaSat. 2022. Op cit.
[32] The Record. 2022. Viasat confirms report of wiper malware used in Ukraine cyberattack. [online] Available at: <https://bit.ly/3S1A8lT> [Accessed 13 August 2022].
[33] Splunk. 2022. Threat Update: AcidRain Wiper. [online] Available at: <https://splk.it/3qwdbeN> [Accessed 24 August 2022].

Security researchers' hypotheses. As information on the attack remain scarce, cybersecurity researchers have also defined some potential scenarios regarding some aspects of the attack:

The TR-069 Protocol: According to security researcher Ruben Santamarta (Reversemode), ViaSat has been implementing the TR-069 protocol on its internet modems since 2013 following a contract signed with Axiros.[34] It seems that ViaSat's SurfBeam internet modems have unpatched vulnerabilities that enable to install and run application on them without a signature verification or a firmware update, which seems consistent with the upload of the Acid Rain wiper malware.[35]

The VPN Attack Vector: Ruben Santamarta further explained that ViaSat only mentioned the exploitation of a "misconfiguration" in a VPN appliance, but acknowledged that the attack came from the Internet, suggesting that the attack was external and did not come from an insider threat. As the ground segment of KA-SAT is managed by Skylogic, the attacker may have exploited vulnerabilities in VPN appliances on its ground infrastructure. Santamarta outlined that Skylogic relies on VPN provider Fortinet and its FortiGate appliances.[36] In 2021, Fortinet was the victim of a data breach, which led to the leak of around 500,000 VPN credentials stolen from around 87,000 FortiGate SSL-VPN devices (7.96% from Italy).[37] These credentials were obtained through the exploitation of an old vulnerability on systems, which did not implement a patch provided by Fortinet in May 2019. The vulnerability enabled an attacker to download system files via special crafted HTTP resource requests. The 2021 leak was attributed to a Russian-speaking cybercrime group.[38] The NSA, the CISA, and the FBI also outlined that this vulnerability was being exploited by the Russian Foreign Intelligence Agency (SVR).[39] Therefore, the attacker of KA-SAT may have exploited this unpatched vulnerability on Skylogic's VPN appliances, and/or the attacker may have previously collected valid VPN credentials from this data breach.[40]

Consequences on users. The attack created ripple effects across Europe. Thousands of customers in Ukraine, including the Ukrainian Government, the Ukrainian army, and the Ukrainian security services, as well as tens of thousands of other satellite broadband services were impacted. Around 9,000 subscribers of NordNet's (a subsidiary of the French telecom company Orange) satellite broadband service, which relied on satellite internet connection provided by ViaSat, were affected in France.[41] In addition, a third of the 40,000 subscribers of the British broadband provider BigBlu (subsidiary of Eutelsat) were affected in Germany, France, Hungary, Greece, Italy, and Poland.[42] The German energy company Enercon saw the remote monitoring and control access of its 5,800 wind turbines become unavailable as they were managed by a SCADA system relying on the KA-SAT network. Some satellite modems were rendered unusable and could not be repaired or updated remotely. As of May 2022, thousands of customers were still left without internet connection. According to Viasat, end-user data and devices such as computers or mobile phones were not accessed by the attacker. Additionally, the KA-SAT satellite itself and its ground stations do not seem to have been hacked, compromised, damaged, or involved in the attack.[43]

[34] Nichols, T., 2013. Axiros, ViaSat to Produce First Deployment of TR-069 Protocol over a Satellite Network [online] Via Satellite. Available at: <https://bit.ly/3d9vHXf> [Accessed 14 August 2022].
[35] Reversemode. 2022. VIASAT incident: from speculation to technical details.. [online] Available at: <https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html> [Accessed 19 August 2022].
[36] Reversemode. 2022. Ibid.
[37] Abrams, L., 2021. Hackers leak passwords for 500,000 Fortinet VPN accounts. [online] BleepingComputer. Available at: <https://bit.ly/3db544m> [Accessed 24 August 2022].
[38] Fortinet Blog. 2021. Malicious Actor Discloses FortiGate SSL-VPN Credentials. [online] Available at: <https://bit.ly/3eM2jXq> [Accessed 27 August 2022].
[39] Brook, C., 2021. NSA Urges Organizations to Patch Five Vulnerabilities Exploited by Russia. [online] Digital Guardian. Available at: <https://bit.ly/3xm3Zxw> [Accessed 24 August 2022].
[40] Reversemode. 2022. Op cit.
[41] Cyber Peace Institute. 2022. Timeline of Cyberattacks and Operations. [online] Available at: <https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline> [Accessed 25 August 2022].
[42] Lausson, J., 2022. La cyberattaque ayant déconnecté des Français aurait profité d'une erreur dans le satellite Ka-Sat. [online] Numerama. Available at: <https://bit.ly/3Djqarl> [Accessed 19 August 2022].
[43] ViaSat. 2022. Op cit.

The public attribution of the KA-SAT cyberattack

The attribution of cyberattacks, which refers to the digital forensic process that enables to track and identify an attacker[44], is an essential aspect of cyberdefense and cyber warfare, and a prerequisite for retaliation. The decision to publicly attribute an attack (by naming the attacker) remains a political decision motivated by several reasons such as deterring future attacks, naming and shaming an adversary, demonstrating attribution capabilities, etc.

The KA-SAT cyberattack was first unveiled by General Friedling, Head of the French Space Command, on March 3rd during a press briefing of the French Ministry of Armed Forces. However, France did not publicly attribute the attack due to its singular public attribution strategy.[45] **Unlike Five Eyes countries, which have a "name and shame" approach to public attribution, France almost never communicates on the attacks that target its systems or networks and rarely attributes attacks publicly.**[46] France does not publicly attribute attacks coming from Nation-States and usually uses diplomatic channels to confront the attackers.[47] Gen. Tisseyre, Head of the Cyber Command, explained that France considers that public attribution is not a goal in itself because the accused State will deny these accusations and will ask for proof that cannot be shared publicly without revealing France's attribution capabilities or without admitting to spying or hacking back to trace the origins of the attack.[48] Additionally, **France considers that public attributions may negatively impact attribution capabilities and cyber situational awareness as they eventually push malicious actors to adopt new and more discreet methods, which are more difficult to track and monitor for authorities**. The technical attribution of an attack is often based on previously identified patterns, methods, and techniques used by States and their proxies.

On May 10th, the United States and the European Union officially publicly attributed the KA-SAT cyberattack to Russia.[49] The U.S. statement provided additional details and attributed the attack to Russian military cyber operators, without naming a specific agency or group.[50] Estonia joined the EU statement and attributed the attack to Russian Military Intelligence (GRU).[51] **Security researchers identified clear similarities between methods and codes used in the KA-SAT cyberattack and other wiper malware related to the GRU and/or GRU-affiliated hacker groups.**[52] However, States did not provide additional technical evidence of the attribution. It is worth noting that at the international level, there is no institutionalized framework or mechanism for publicly attributing attacks. As a result, there are no obligations under international law to disclose evidence of attribution. Attacks can be attributed by States, cybersecurity companies, industrial stakeholders, or civil society actors.[53] Yet, diverging strategies for public attribution can sometimes discourage responsible behaviour in cyberspace, undermine public attribution, and paralyse victims in their response and retaliation, therefore more cooperation may prove useful.

[44] Assumpção, C., 2020. The Problem of Cyber Attribution Between States. [online] E-International Relations. Available at: <https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/> [Accessed 17 August 2022].
[45] Ministère des Armées, 2022. Point Presse du ministère des Armées du jeudi 3 mars 2022. [online] Youtube. Available at: <https://www.youtube.com/watch?v=zAmfuydWqXU> [Accessed 18 August 2022].
[46] Lachaud, B., Valetta-Ardisson, A., 2018. Cyberdéfense. Rapport information n°1141. Assemblée Nationale.
[47] Delerue, F., Desforges A., Géry, A., 2019. A Close Look At France'S New Military Cyber Strategy. [online] War on the Rocks Available at: <https://bit.ly/3qERCIR> [Accessed 18 August 2022].
[48] Lagneau, L., 2020. La Chancelière Allemande Attribue Publiquement La Responsabilité D'une Cyberattaque À La Russie. [online] *Zone Militaire*. Available at : <https://bit.ly/3RFFsLU> [Accessed 18 August 2022].
[49] European Council. 2022. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. [online] Available at: <https://bit.ly/3xjqEue> [Accessed 19 August 2022].
[50] CISA. 2022. Strengthening Cybersecurity of SATCOM Network Providers and Customers. [online] Available at: <https://www.cisa.gov/uscert/ncas/alerts/aa22-076a> [Accessed 20 August 2022].
[51] Välisministeerium. 2022. Estonia joins the statement of attribution on cyberattacks against Ukraine |. [online] Available at: <https://vm.ee/en/news/estonia-joins-statement-attribution-cyberattacks-against-ukraine> [Accessed 10 August 2022].
[52] SentinelOne. 2022. Op cit.
[53] Egloff, F., et al. 2019. Public Attribution of Cyber Incidents. CSS Analyses in Security Studies. ETH Zurich

3.2 The KA-SAT cyberattack: a representative case of the current state of cybersecurity in the commercial space sector

The KA-SAT attack is representative of the state of cybersecurity in the space sector, in particular in the supply chain and on the user segment. The KA-SAT cyberattack was conducted through an exploitation of vulnerabilities, which are similar to previous and current threats identified on space systems in both the supply chain and the user segment. This section will provide example of comparable vulnerabilities identified in the space supply chain (1) and the user segment (2).

The supply chain: the weakest link?

According to UNIDIR, the supply chain is increasingly vulnerable to cyber risks due to its rising complexity; its cross-border interdependency; and the growing digital management of supply chains themselves. Attacks on the supply chain can occur on the software supply chain, which may include the insertion, modification, or removal of information, code, software, or functionality to a system or component during the development, upgrade, or update of a system to change its intended functions. Attacks can also occur on the hardware supply chain, which can involve the introduction, intentional or not, of components or electronic chips that contain defects, vulnerabilities, or backdoors in order to sabotage a system or to spy on it.[54] In many assembly lines, workers and subcontractors do not know in which system the components will be installed and whether the use will be military, dual or civil. However, an adversary can access an assembly line with precise knowledge of the components and the final system, and intentionally hide defective components, surveillance microchips, or other electronic chips containing vulnerabilities or backdoors.[55]

According to Scott Millwood, cyberattacks in the telecommunication industry almost always happen in the supply chain. Similarly to the KA-SAT case, attacks against VPN networks are also rather common in the aerospace sector. For instance, in 2019, Airbus suffered from a series of cyberattacks, which all exploited vulnerabilities in the IT networks of Airbus' subcontractors such as Assystem, Rolls Royce, Expleo, etc. The attackers targeted the VPN networks, which connected the suppliers to Airbus' network and accessed confidential data, including regarding military systems.[56]

Cyberattacks on the space supply chain are poised to become more common because of New Space. According to James Pavur from the University of Oxford, New Space brings new cybersecurity risks throughout the supply chain. The space sector used to be a very secretive sector, comprising mostly defence companies, which were manufacturing unique and expensive hardware and software for very specific space missions. The barrier of entry was very high as it was difficult and expensive for an attacker to access the component of a satellite or access information about the company. **New Space companies are more communicative than traditional space actors and share more information about their systems, supply chain, contracts, employees, etc., which may give critical information to a malicious actor to launch an attack.** In addition, today's space systems are increasingly equipped with cheaper Commercial off the Shelf (COTS) components and standardised hardware and software, which enable a potential attacker to buy them to look for vulnerabilities. It also means that if a vulnerability is found in one component, all satellites using this COTS component become vulnerable. The emergence of Open-Source Satellite Operating Systems such as NASA's Core Flight System can also enable an attacker to look for vulnerabilities.[57]

[54] Demidov O., Persi Paoli, G., 2020. Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses. UNIDIR
[55] Bailey, B., 2019. Defending Spacecraft in the Cyber Domain, Aerospace Corporation.
[56] Millwood, S., 2018. What Space Missions Can Learn From Cyber-Security Breaches (and Counter-measures) in the Telecommunications Industry. 69th International Astronautical Congress. IAF.
[57] SGAC. 2020. Space for IoT. Webinar. [online] SGAC Space and Cybersecurity PG.

The user segment: known vulnerabilities keep being exploited

ViaSat's internet modems seemed to contain known and unpatched vulnerabilities that were exploited by Russia to target the KA-SAT network. The exploitation of these vulnerabilities represents common issues on the user segment. **In the past decade, security researchers and cybersecurity companies, in particular IOActive, have warned the telecommunication industry over the presence of critical software and hardware vulnerabilities in SATCOM user terminals.** These warnings have largely remained underestimated.[58] The table below describes research findings on SATCOM user terminals:

IOActive, *"SATCOM Terminals Hacking by Air, Sea, and Land"*, Black Hat, 2014	IOActive scanned several Inmarsat and Iridium SATCOM terminals such as Inmarsat-C, Very Small Aperture Terminals (VSAT), Broadband Global Area Networks (BGAN), BGAN Machine-to-Machine, FleetBroadband (FB) systems, SwiftBroadband systems, and Classic Aero Service systems. **These user terminals are actively used in the maritime and aviation sectors, in emergency services, in oil and gas, and in the military, including within NATO forces.** For instance, BGAN terminals contained many vulnerabilities such as hardcoded credentials, undocumented and insecure protocols, and backdoors. These vulnerabilities could allow an attacker to inject malicious code to install a malware on a laptop connected to the terminal that would retrieve geolocation data from the built-in GPS to determine where the soldiers are located, putting the troops at risk of enemy's kinetic attacks as well as impacting their ability to communicate with their commanders.[59] **IOActive warned the five companies, which develop these terminals, but only one company was truly responsive**.[60]
IOActive, *"Last Call for SATCOM Security"*, Black Hat, 2018	In 2018, IOActive found additional vulnerabilities in SATCOM user terminals, which are used in the aviation, maritime, and military domains. In the aviation sector, identified vulnerabilities on Airborne SATCOM equipment for in-flight Wi-Fi may enable an attacker to disrupt, intercept, and modify in-flight Wi-Fi traffic, attack crew and passenger's devices, and take control over the SATCOM antennas onboard of the aircraft. In the military domain, identified vulnerabilities on user terminals exposed to the Internet could enable an attacker to identify the location of troops on the ground; disrupt, intercept, or modify satellite communications; and conduct cyber physical attacks on user terminals. **These types of terminals were used in active conflict areas.** In the maritime sector, IOActive scanned Antenna Control Units (ACUs), which are used to support services such as Global Xpress, Maritime VSAT, and FleetBroadband. Among other things, IOActive found that Intellian's firmware was publicly available online and open for modification by any user. In addition, IOActive found hardcoded and undocumented credentials that can be used to access the ACU. Randomly scanned ACUs were infected by the Mirai botnet[61], which is a malware that can turn connected devices into remotely controlled bots to launch DDoS attacks on other systems.[62] **IOActive outlined that telecom companies were more open to patch these vulnerabilities than in 2014, but many remained skeptical about their findings**.[63]

[58] IOActive. 2022. Missed Calls for SATCOM Cybersecurity: SATCOM Terminal Cyberattacks Open the War in Ukraine. [online] Available at: <https://ioactive.com/missed-calls-for-satcom-cybersecurity/#_ftn14> [Accessed 22 August 2022].
[59] IOActive. 2014. A Wake-up Call for SATCOM Security. [online] Available at: <https://bit.ly/2ToP5Bq> [Accessed 18 August 2022].
[60] IOActive. 2022. Op cit.
[61] CloudFlare. n.d. What is the Mirai Botnet?. [online] Available at: <https://bit.ly/3BB1NVa> [Accessed 21 August 2022].
[62] IOActive. 2018. Last Call for SATCOM Security. [online] Available at: <https://bit.ly/3QDiPXg> [Accessed 16 August 2022].
[63] IOActive. 2022. Op cit.

IOActive, *"Wideye Security Advisory and Current Concerns on SATCOM Security"*, 2022	In March 2022, IOActive decided to release additional research on **vulnerabilities found in SATCOM terminals developed by Addvalue Technologies Ltd. (Wideye) for Inmarsat's iSatHub service, which are similar to the vulnerabilities exploited in the KA-SAT case. IOActive disclosed these vulnerabilities with the company three years ago. However, the company remained unresponsive.** IOActive scanned two terminals: the Wideye iSavi, which is a user terminal developed for Inmarsat iSatHub service as well as BGAN services (voice, text, internet connection); and the SABRE Ranger 5000, which is a machine-to-machine terminal commonly used for providing remote access to equipment and is often used in SCADA applications for critical infrastructures (e.g., pipeline, wellsite, wind turbines monitoring, water management, early warning systems for natural disasters, etc.). Following a security assessment and dynamic penetration testing, several vulnerabilities and security issues were discovered. Vulnerabilities included possibilities for a malicious actor to compromise the terminal, to access the remote management settings, to recover access credentials, to run arbitrary code and upload new firmware, to record GPS coordinates to locate the terminal and its user, etc. **Despite contacting the company and providing security solutions and fixes, most of the vulnerabilities were still present when IOActive published its report**.[64]
Lennert Wouters, *"Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal"*, 2022	In August 2022, KU Leuven researcher Lennert Wouters unveiled hardware vulnerabilities on Starlink terminals, which enabled him to conduct a voltage fault injection attack. A voltage glitch requires physical access to the targeted system and consists in creating disturbances on the power supply line to bypass security checks or generate side-channels that leads to data leaks, including the firmware code. Wouters attached a homemade printed circuit board (PCB) to a Starlink dish, and used voltage fault injection during the execution of the system-on-chip ROM bootloader, which enabled him to bypass the firmware signature verification and run his own code. Glitching the bootloader enabled him to gain root access to the terminal with possibilities to upload a malware, modify settings, or disturb communications. **Wouters discovered the issue in 2021 and notified SpaceX, which promptly and positively reacted by introducing a firmware update and paying the researcher through its Bug Bounty programme for identifying the vulnerabilities.** However, the issue cannot be entirely fixed remotely, and terminals remain vulnerable. New terminals would have to be developed to ensure these vulnerabilities are patched.[65]

Table 1: Research findings on SATCOM user terminals

Examples provided above demonstrate that the vulnerabilities exploited in the KA-SAT case are rather common in the space sector. These examples also show that known vulnerabilities, which were disclosed to companies and for which fixes were provided, have remained unpatched. Additionally, IOActive's research reveals that basic cybersecurity standards are not implemented by design and many open-source information can be found online to exploit and take control of SATCOM user terminals. **The unresponsiveness of the space sector to IOActive's research also shows the lack of cooperation between the space and cybersecurity communities.** While some space companies are increasingly aware of cybersecurity, many efforts remain to be done to better protect space systems.

[64] IOActive. 2022. Cyberattacks on SATCOM: Understanding the Threat. [online] Available at: <https://bit.ly/3U5g1Fa> [Accessed 21 August 2022].
[65] Nast, C., 2022. The Hacking of Starlink Terminals Has Begun. [online] WIRED. Available at: <https://www.wired.com/story/starlink-internet-dish-hack/> [Accessed 29 August 2022].

3.3 Lessons to learn from the KA-SAT cyberattack and the war in Ukraine

"There are only two types of companies – those that were hacked, and those that will be" - FBI	The KA-SAT cyberattack may be the wake-up call that the space community needed to speed up cybersecurity	*"A software security system is only as secure as its weakest component"* - CISA

3.3.1 Direct lessons to learn from the KA-SAT cyberattack

Commercial space systems are easy targets for cyberattacks during armed conflicts

The KA-SAT cyberattack demonstrates that commercial space systems are essential tools to support military operations on Earth, but also prime targets to (cyber)attack. Russia officially declared it would consider private satellites as legitimate targets for retaliation in wartime.[66] While military satellites are usually well-protected, commercial satellites are often crippled with vulnerabilities in the space, ground, and user segment. Commercial satellites are not subject to the same level of governance, cybersecurity, and secrecy as military satellites, even though they are increasingly used for military purposes.[67] According to UNIDIR Researcher Laetitia Cesari Zarkan, a cyberattack against a commercial satellite may be more dangerous than a cyberattack against a military satellite. Military satellite operators are also used to being attacked and even expect to be. As a result, there is a better chance that they know how to react to an attack, which is not always the case in the commercial sector.[68] In fact, some **space companies have voiced their concerns regarding this point at the beginning of the war in Ukraine, outlining that there was no clear process for reporting and responding to a cyberattack**.[69] It underscores the need to have better security controls along with identified policy and legal frameworks for incident response and clear coordination processes with relevant authorities.

There are endless vulnerabilities on the commercial space infrastructure

The KA-SAT cyberattack shows that many vulnerabilities and entry points can be exploited across the attack surface during a single attack. An attack can be multifaced and target several weak points. In addition, the management and ownership of commercial space services can be complex, with various companies owning and operating the space, ground, and control segments across several countries and jurisdiction**.** Contractual relationships can include numerous IT service providers and various levels of vulnerability and responsibility regarding cybersecurity. **Threat actors can exploit trust relationships and access privileges between space companies and their IT subcontractors to access networks and data. In the KA-SAT case, Russia likely exploited the link between VPN provider Fortinet and Eutelsat's subsidiary Skylogic to access ViaSat's network.** It raises legal questions regarding contractual responsibilities for cybersecurity and minimum requirements required by providers to their subcontractors.

Commercial actors inherit the threat models of their clients

The KA-SAT cyberattack also shows that providing satellite services to domestic or foreign armed forces, security services, or governments can increase the risks of attack. If a space company is providing services to a domestic or foreign government or military, it might become a target. If the customer of a space company becomes a belligerent in an armed conflict or is located in a conflict

[66] ООН. 2022. Выступление главы делегации Российской Федерации К.В.Воронцова на второй сессии Рабочей группы открытого состава, учреждённой резолюцией ГА ООН 76/231.
[67] Bailey, B., 2019. Op cit.
[68] Zarkan, L., 2020. Space domain awareness, governance and security in outer space. AMC Solutions. Webinar.
[69] C4ISR. 2022. How commercial space systems are changing the conflict in Ukraine. [online] Available at: <https://bit.ly/3U5p3C5> [Accessed 30 August 2022].

area, the company may inherit from the threat models of that client and be targeted by cyberattacks.[70] It calls for **a higher level of cybersecurity of commercial space systems, but also for an update of the threat model of a company when a conflict arises, which requires a dedicated cybersecurity budget.** For instance, a week after the Russian invasion of Ukraine, Elon Musk announced that SpaceX was reallocating some of its resources to cyber defence and anti-jamming to face cyber and electronic threats in Ukraine at the expense of other projects such as Starship and Starlink V2, which will face delays.[71]

Segregation between civilian and military customers is essential

The KA-SAT cyberattack shows that servicing commercial and government customers calls for **complete segregation between commercial/civilian customers and government/military ones to reduce the risk of lateral movement and propagation of the attack. The likely lack of segregation on the KA-SAT network may have led to ripple effects on other systems, including critical infrastructure such as German windmills.** According to Gregory Falco from Harvard University, satellites represent *"a single point of failure for various industries"* as they underpin most critical infrastructure (e.g., banking, energy, transport). Targeting one satellite can constitute a destabilizing factor as it may compromise the functioning of many critical industries at the same time, increasing the risks of collateral damage.[72] Yet, the space infrastructure is not always considered as a critical infrastructure, which impacts the cybersecurity measures that the space sector has to implement.

Military systems should not be considered based on their ownership, but on their use

The increasing use of commercial systems for military purposes also brings the need to consider military space assets based on their use rather than the nature of their owners. In Europe, systems are often considered as military assets based on the nature of their owners and commercial systems are limited to non-critical activities. For instance, in France, space capabilities are considered based on three circles: (1) A restrained sovereign circle, which includes national military satellites owned and operated by the military; (2) an enlarged circle, which includes systems developed and operated in cooperation; (3) an extensive circle, which includes applications for which the level of criticality is compatible with the commercial sector. However, in the United States, 80% of military communications rely on commercial satellites. Therefore, space systems are considered as military assets based on their criticality rather than the nature of their owners and operators.[73] Considering the essential role of space in military operations, the pervasive dependence to space-based connectivity and synchronisation in many critical infrastructures, and the priority towards commercialisation in many European space policies, European governments will eventually rely on commercial systems for many critical operations, including military ones. **If a commercial company is servicing domestic or foreign armed forces, its systems should be subject to the same level of cybersecurity and security audits as military satellites owned and operated by armed forces.**

3.3.2 Broader cyber lessons to learn from the war in Ukraine

The lack of sovereign space capabilities creates a dependance and strategic autonomy issue

Ukraine is entirely dependent on foreign space assets in this war. At the tactical level, **the use of both commercial and military drones on the battlefield is entirely reliant on Starlink satellites**.[74] Drones

[70] Rückriegel, C., 2022. Security Governance for Ground Segments. CYSEC. Conference.
[71] Foust, J., Berger, B., 2022. SpaceX shifts resources to cybersecurity to address Starlink jamming. [online] SpaceNews. Available at: <https://bit.ly/3RZaVZf> [Accessed 21 August 2022].
[72] Falco., G., 2018. The Vacuum of Space Cybersecurity. 2018 AIAA SPACE and Astronautics Forum and Exposition.
[73] Becht, O. and Trompille, S., 2019.
[74] DW. 2022. Ukraine is using Elon Musk's Starlink for drone strikes. [online] Available at: <https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528> [Accessed 29 August 2022].

play a significant role in the conflict as they are being used for reconnaissance missions to track Russian convoys, send the images as well as GPS coordinates to artillery units in order to carry out strikes. In addition, commercial drones were updated to carry small bombs or anti-tank grenades. A combat unit also developed a network of sensors on the ground that feed data into a live digital map that enable to monitor Russian movements and conduct strikes. This digital map relies on Starlink for connectivity.[75] Troops and commanders were able to maintain contact through Starlink. At the strategic level, the United States is said to have given Ukrainian President Zelensky and Foreign Minister Dmytro Kuleba **Iridium 9575A satellite phones** to ensure protected communications with the U.S. President.[76] Communications with journalists and other decision makers were also conducted using Starlink.[77]

Making a case for the EU secure connectivity initiative	While Europe is not in such a situation of dependence, most European states do not have sovereign satellite communications capabilities, let alone military ones. In case of conflict, their government communications as well as their military operations would be dependent on the quality of their relationships with their allies and their willingness to provide them with satellite capabilities. Moreover, military systems currently developed by European states such as the Future Combat Air System (FCAS) and the Main Ground Combat System (MCGS) will be dependent on satellite communications capabilities to function and are expected to become critical systems in the implementation of multidomain operations. Current European capabilities were already identified as insufficient[78], which may eventually push armed forces to procure commercial SATCOM services, which are more vulnerable to cyberattacks and currently consists of non-European constellations. Therefore, there is a clear need for a European solution that integrates a rationale centered on cybersecurity, digital sovereignty, and strategic autonomy.

The lack of space capabilities also creates a cybersecurity issue in armed conflict

On the other side, the Russian military demonstrated a lower use of encrypted military SATCOM than expected[79] and relied on unsecure communication devices such as unencrypted high frequency radio and mobile phones, which enabled Ukraine to eavesdrop on many Russian communications.[80] In some cases, Russian troops used encrypted satellite phones such as the Era cryptophone, which needs 3G/4G to function. However, in some areas, Russia conducted strikes on 3G/4G towers, destroying their own secure SATCOM capabilities and rendering this phone unusable.[81]

Making a case for the EU secure connectivity initiative	The lack of functioning sovereign encrypted SATCOM capabilities shows that relying on unsecure communications during an armed conflict can directly hamper military operations and expose troop's locations and communications with their commanders as well as their families. It shows how secure satellite communication capabilities play a critical role in armed conflict to guarantee constant connectivity even in case of destruction of the terrestrial digital infrastructure.

[75] Thomas, A., 2022. Les drones sur le champ de bataille : quelles leçons tirer de leur emploi par les forces ukrainiennes ?. [online] FRS. Available at: <https://bit.ly/3d42VHL> [Accessed 24 August 2022].
[76] American Post. 2022. Iridium 9575A: how is the ultra-secure phone that Zelenski uses to talk to Biden [online] Available at: < https://bit.ly/3B9P1vp> [Accessed 1 September 2022].
[77] POLITICO. 2022. UkraineX: How Elon Musk's space satellites changed the war on the ground. [online] Available at: <https://politi.co/3S0sRCU> [Accessed 28 August 2022].
[78] Le Gleut, R., Conway-Mouret, H., 2020. Le système de combat aérien du futur (SCAF), Rapport d'information. Sénat.
[79] Horton, A. and Harris, S., 2022. Russian troops' tendency to talk on unsecured lines is proving costly. [online] Available at: <https://wapo.st/3U44MN4> [Accessed 30 August 2022].
[80] Cranny-Evans, S. and Withington, T., 2022. Russian Comms in Ukraine: A World of Hertz. [online] RUSI. Available at: <https://bit.ly/3B8U2V3> [Accessed 30 August 2022].
[81] Data Center Dynamics. 2022. Ukraine: Russian military's own encrypted phones impacted after destroying 3G/4G towers, allowing comms to be intercepted. [online] Available at: <https://bit.ly/3S0snwk> [Accessed 4 September 2022].

Rerouting internet traffic strategies make satellites essential in armed conflicts

Russian cyber operations in the war in Ukraine also illustrate the essential role satellites can play when terrestrial systems are under attack. Researcher Louis Pétiniaud demonstrated how Russia was digitally isolating the Ukrainian territories under its control. The Russian military and separatists forced Ukrainian service providers to divert the Ukrainian internet traffic to Russia by modifying agreements with Autonomous Systems (AS) via the Border Gateway Protocol (BGP).[82] An autonomous system (Internet Service Providers, mobile operators, data providers, etc.) is a large network or group of networks with a unified routing policy, which signs agreements with other AS through the BGP to ensure that data can circulate across the world. The BGP defines the routes that the data packets take in cyberspace and can be manipulated to control and block both connectivity and content. It led to the fragmentation of Ukraine's cyberspace and put Ukrainian internet users under Russian internet rules in terms of censorship, control and access to information, as well as privacy.[83] In occupied territories, Starlink enabled to maintain a free access to connectivity.

Making a case for the EU secure connectivity initiative	These cyber operations demonstrate the essential role SATCOM can play in a conflict to restore connectivity when terrestrial systems are under attack. It also shows how satellites can be tools to face the fragmentation of the internet and information warfare, enabling control of content and access to the internet. Whether in peace or war time, it makes a clear case for Europe to have a sovereign solution. It will ensure Europe's capacity to safeguard principles such as freedom of the press, freedom of speech, privacy, etc. by being in control of its digital infrastructure. Most systems currently in development, which could potentially provide connectivity in Europe are private initiatives such as SpaceX's Starlink, Amazon's Kuiper, and OneWeb. As satellites are poised to become a significant component of the digital infrastructure, it may put the control over internet traffic in the hands of a few private actors, who will be able to control content and access to the digital infrastructure. Space cybersecurity should also be seen from the perspective of digital sovereignty.

Overall, lessons from the KA-SAT case and the war in Ukraine illustrate the strategic, security, and military dimensions of SATCOM solutions. These aspects are poised to take a growing place due to the pervasive dependence of the military and society to SATCOM as well as the evolution of the threat landscape. The KA-SAT case also highlights the need to adapt the cybersecurity of SATCOM solutions to new use cases and cyber risks throughout the system lifecycle. The war in Ukraine demonstrates that sovereign and protected SATCOM capabilities are essential to ensure cybersecurity, strategic autonomy, and digital sovereignty.

The rotating Czech Presidency of the Council of the EU unveiled its priorities, which include strengthening Europe's defence capabilities and cybersecurity. It plans to address *"cyber threats and the geopolitical context of new technologies and space"* and plans *"to pay particular attention to the cybersecurity of EU institutions, bodies, and agencies and to the EU space-based secure communication system"*. The main legislative proposal to be discussed during the Czech Presidency will be the regulation on the creation of an EU programme for secure connectivity.[84] Lessons from the KA-SAT case and the war in Ukraine should be considered by the Czech Presidency when discussing this proposal.

[82] Pétiniaud, L., 2022. Ukraine : comment la Russie isole numériquement les territoires qu'elle contrôle ?. [online] France Culture. Available at: <https://bit.ly/3QGbiXo> [Accessed 28 August 2022].
[83] Douzet, F., et al. 2020.
[84] Czech Presidency of the EU. 2022. Programme of the Czech Presidency of the Council of the European Union. [online] Available at: <https://bit.ly/3QIJjGG> [Accessed 29 August 2022].

The KA-SAT case: diverging views on the application of international law to cyberspace

The KA-SAT cyberattack affected users in Ukraine, France, Germany, Hungary, Greece, Italy, and Poland. It raises questions regarding the consequences of a cyberattack conducted as part of an armed conflict but generating ripple effects on space services in non-belligerent countries. Looking at the views of affected countries on the applicability of international law to cyberspace can provide insights on the perception and potential reaction of these countries to an attack on their space systems. In the past few years, many States have released official documents outlining their views on the application of international law to cyberspace. Most of them agree on the applicability of international law to cyberspace, but the ways and extent in which it applies vary greatly from one country to another. Among controversial aspects, the application of sovereignty to cyberspace remains contentious. States have adopted two approaches:

The approach of sovereignty as a principle: *"sovereignty is a principle of international law from which certain prohibitive rules flow but does not itself constitute such a rule."*

The approach of sovereignty as a rule: *"sovereignty is a primary rule of international law, which requires States to respect the sovereignty of another States, which is also applicable to State conduct in cyberspace."*

Within the sovereignty as a rule approach, two doctrines have been adopted by States:

- **The 'de minimis' approach:** a breach of sovereignty in cyberspace is based on a minimum threshold of effects generated by the attack, usually effects similar to a kinetic attack.
- **The penetration of systems approach:** a breach of sovereignty is based on the penetration of any system located within the territory of a State, regardless of the effects generated.[85]

This distinction is important as supporters of the sovereignty as a rule approach would likely consider that a cyberattack on a system (e.g., a satellite internet modem) located on their territory would consist of a violation of their sovereignty and that the attacker violated international law. However, supporters of the sovereignty as a principle approach would likely consider that as sovereignty is not a rule that has to be respected in cyberspace, the attacker did not violate the sovereignty of the victim State and therefore did not breach international law, unless other rules (e.g., duty of non-intervention, prohibition of the use of force, etc.) were violated.

Among the seven States affected by the KA-SAT cyberattack, only three (France, Germany, Italy) have released an official document outlining their vision on the application of international law to cyberspace. Among them, diverging views can be identified. For instance, France adopted the sovereignty as a rule approach and the doctrine on the penetration of systems, therefore, it may theoretically consider the KA-SAT cyberattack as a breach of its sovereignty; whereas Germany also considers sovereignty as a rule but seems to consider that a minimum threshold should be reached for an attack to be considered as a breach of sovereignty, but without defining such threshold. As the KA-SAT cyberattack was only temporary, Germany may likely not consider it as a breach of sovereignty. **While these views remain more political than legal, the KA-SAT case shows that there is a need for more dialogue on the application of international law in cyberspace.[86] All European countries should release their own views on the matter, outline their views on sovereignty, highlight which doctrine they consider as the most relevant, define a threshold in case they consider the 'de minimis' approach[87], and state whether it also applies to the space infrastructure, both on Earth and in outer space.**

[85] Roguski. P. 2020. Application of International Law to Cyber Operations: A Comparative Analysis of States' Views. Policy Brief. The Hague Program for Cyber Norms.
[86] Interview of Duncan Hollis, conducted by ESPI in August 2022; Interview of Francois Delerue, conducted by ESPI in September 2022.
[87] Roguski. P. 2020. Op cit.

4 PAVING THE WAY FORWARD: PROTECTING THE EUROPEAN SPACE INFRASTRUCTURE

Based on the lessons learnt from the KA-SAT cyberattack and acknowledging the current state of affairs in the cybersecurity of the space sector, some policy and legal reflections for the cybersecurity of the European space infrastructure can be outlined.

Updating a scattered legal and policy framework

At the European level, the cybersecurity of space systems is rather overlooked in EU policies and regulations. There is currently no legislative framework dedicated to the cybersecurity of commercial space systems or to the cybersecurity obligations of space companies providing space services on European soil. It must be noted that **the EU Space Programme Regulation** addresses cybersecurity, but it only applies to the EU flagship programmes such as Copernicus, Galileo, EGNOS, EUSST, and GOVSATCOM. Therefore, the cybersecurity measures of the EU Space Programme Regulation would not have applied to ViaSat in the KA-SAT case.

In addition, the **2016 EU Network and Information Systems (NIS) Directive** outlines the security and safety measures, including cyber ones, that operator or critical infrastructure and essential services have to follow as well as reporting obligations to authorities. However, this Directive only applies to the following sectors: energy, transport, banking, financial markets, health, water, and digital infrastructures. The NIS Directive does not include the space infrastructure or SATCOM operators as part of the digital infrastructure. As a result, **the NIS Directive does not directly apply to the space sector**, although many of these essential services rely on satellites to function. As it is an EU Directive, it has to be translated into the national legislations of Member States. Member States may consider space as essential and therefore subject space operators to this Directive, but it is not compulsory.[88]

In light of these gaps and the evolving threat landscape, the European Commission proposed to adopt a **NIS2 Directive on measures for a high common level of cybersecurity across the Union** in December 2020, repealing the 2016 NIS Directive. The draft text, which is yet to be adopted in the fall of 2022, distinguishes between essential and important entities. Space is expected to be integrated as an essential entity. More precisely, the Directive will apply to *"operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972"*. While it is not encompassing all space actors, it will outline stricter cybersecurity measures, reporting obligations, incident response mechanisms, and fines for non-compliance for space operators.[89] **This Directive is a positive initiative to enhance the cybersecurity of the European space infrastructure, enabling to reduce the cyber risks, which were exploited in the KA-SAT case.**

To complement the NIS2 Directive, the Commission proposed to adopt a **Directive on Critical Entity Resilience (CER Directive)** to repeal the European Critical Infrastructure (ECI) Directive. The CER Directive outlines rules to face non-cyber and physical threats and will apply to the essential entities of the NIS2 Directive, including space.

The space sector will have to be accompanied to implement the NIS2 and ECI Directives. When Member States will translate these directives into their national legislations, the cybersecurity measures and obligations will also have to be adapted to the nature of space operations. At the same

[88] Mendonca, H., et al., 2020. Security-Compliant Cyber Measures for Satellite Systems. IAC Cyberspace Edition. IAF
[89] European Commission. 2020. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

time, there should not be unnecessary burdens on satellites used for science, education, and technology. This will be a challenge as there is often a lack of cooperation between the cybersecurity, computer science, space engineering, astrophysics, and space policy communities to better understand cyber threats on space systems, which led to a lack of research on space cybersecurity. There is also a sort of **digital conundrum**: on the one hand, the digitisation of space systems makes them more vulnerable to traditional cyber threats, which prompts to adopt traditional cybersecurity measures; on the other hand, the unique nature of space systems often renders traditional cybersecurity inadequate.[90]

However, some existing initiatives can be used as an inspiration to assist Member States in translating the NIS2 Directive into their national frameworks and in ensuring implementation in the space sector and more generally improve space cybersecurity:

Figure 2: Initiatives to improve space cybersecurity

More generally, the EU has been actively adopting policies and policy tools regarding cybersecurity. However, there is currently no policy entirely dedicated to the cybersecurity of space systems. While it may not be essential to develop such a policy, there are other policy frameworks, which should better recognize cyber risks. Among the policies, which are yet to be adopted, an **EU space strategy for**

[90] Pavur. J., Martinovic., I., 2022. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. Journal of Cybersecurity. Oxford University Press.

security and defence is expected to be drafted in the coming months. The war in Ukraine and the KA-SAT case illustrate that cyberattacks against space systems can directly provide a strategic advantage to an adversary in an armed conflict and should therefore be comprehensively acknowledged in such public policies.

New security stakes for EU flagship programmes

The KA-SAT case demonstrates the importance of better protecting space systems against cyber threats. Cybersecurity and sovereignty objectives have already been identified by the European Commission in its proposition for an EU secure connectivity initiative, which are particularly relevant in the context of an evolving threat landscape. Among other things, the European Commission plans to integrate the EU secure connectivity initiative into the EuroQCI initiative and develop Quantum Key Distribution (QKD).[91]

This future programme is expected to have both commercial and security objectives, which raises challenges for the European Commission to develop a system that will be both competitive and secured. In other words, the initiative will have to be secure enough for government communications, but also competitive and efficient enough for commercial applications. **The challenge for the EC will be to craft an innovative approach to ensure the capacity of the EU secure connectivity initiative to provide secure connectivity at competitive costs.** Strong cybersecurity can sometimes have negative impacts on the efficiency, latency, and quality of SATCOM solutions. It may push economic sectors, which are looking to benefit from space connectivity in new verticals such as automotive, energy, health, IoT, smart cities, etc. to opt for SATCOM offerings that are faster and cheaper.

Nevertheless, it is important to highlight that the number of cyberattacks across sectors has skyrocketed in the past few years. Attempts to target space actors and space infrastructures have increased in both complexity and severity. The KA-SAT case showed that a lack of cybersecurity can lead to widespread and uncontrolled ripple effects due to the interconnectedness and links between systems. Cyberattacks can lead to devastating financial losses and even bankruptcy, disturbances in operations, data and intellectual property loss, as well as reputational harm, etc. As a result, **it is very likely that the cost of cybersecurity compared to the cost of cyberattacks will increasingly shrink in the eyes of users and customers.**

Europe, as a responsible actor in space and cyberspace, may therefore put cybersecurity at the heart of its secure connectivity initiative in order to gain a comparative advantage and increase industrial competitiveness. In a strategic and critical sector such as space, reliability and operational continuity are essential. The growing awareness of customers with regards to new cyber risks and threats will probably become a major competitive factor. **A European solution featuring a high level of (cyber)security could become an opportunity cost.** As the space sector is increasingly being commoditized, **cybersecurity is a differentiation and competitive factor to better exploit.**

[91] ESPI. 2022. Yearbook 2021. Space Policies, Issues, and Trends. European Space Policy Institute

Developing an integrated approach to space cybersecurity

The extension of the attack surface and the evolution of the threat landscape call for a holistic approach to cybersecurity. Space cybersecurity should not solely rely on one countermeasure but rather on a broad set of measures such as but not limited to:

Zero Trust	Space cybersecurity should rely on Zero Trust Architectural frameworks, which is a perimeter-less cybersecurity model based, among other things, on the principle "Never Trust, Always Verify", in which devices should not be trusted by default.[92]
DevSecOps	Space cybersecurity should include DevSecOps (Development, Security, and Operations), which is an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.[93]
Encryption	Space cybersecurity should rely on encryption such as end-to-end encryption and independent encryption. Also, the development of quantum computing is posing a major cyber threat as it will likely be able to decrypt today's encryption keys, therefore Quantum Key Distribution (QKD) will become essential to protect space systems.[94]
Hardening	Space cybersecurity should rely on hardening, which include wrapping electronic components with isolating materials to better protect them from jamming, spoofing, or laser interference. On the software layer, hardening can also entail a drastic reduction of the number of software installed on the computers of satellite operators as well as restricted access to reduce potential vulnerabilities.
Redundancy	Space cybersecurity should rely on redundancy, which is the capacity to immediately compensate for the loss or unavailability of some functionality or component in case of a cyberattack. It can include the duplication of identical components or component of the same nature on a satellite.[95]
Substitution	Space cybersecurity should rely on substitution, which is the capacity to replace a non-functioning system by a system of a different nature but providing similar capabilities.[96] It can include the use of aircraft, drones, or HAPS for imagery, the use of both LEO and GEO communications satellites, the interoperability between terrestrial and space infrastructure, the interoperability between allied systems (e.g., Galileo and the GPS), as well as responsive launches to rapidly replace a satellite. Substitution can also include the use of fully software-defined satellites, whose missions can be entirely reprogrammed remotely to make up for the loss of another system in case of an attack.
D3SOE capacity	Space cybersecurity, in particular for military operators, should also rely on the capacity of the armed forces to operate in a Denied, Degraded, and Disrupted Space Operational Environment (D3SOE). It includes the capacity to conduct military operations without relying on space systems should they become unavailable by retaining the know-how of the pre-electronic era.

Table 2: Examples of cybersecurity measures to face space cyber threats

[92] NIST. 2020. Zero Trust Architecture. [online] Available at: <https://bit.ly/3qzvsrE> [Accessed 28 August 2022].
[93] RedHat. 2018. What is DevSecOps?. [online] Available at: <https://red.ht/2NpD7aP> [Accessed 28 August 2022].
[94] ESPI. 2022. Yearbook 2021. [online] Available at: https://www.espi.or.at/yearbooks/ [Accessed 28 August 2022].
[95] Georgescu. A., et al., 2019. Critical Space Infrastructures. Risk, Resilience and Complexity. Springer.
[96] Ibid

ACKNOWLEDGMENT

The author would like to express their gratitude to the experts who agreed to be interviewed for this report under Chatham House Rules and provided their highly appreciated opinions and perspectives.

- Duncan Hollis, Professor, Temple University Law School
- Francois Delerue, Assistant Professor, IE University Law School

I am furthermore grateful to the ESPI experts, who reviewed the draft report, providing invaluable feedback and comments.

- Marco Aliberti, Resident Fellow, European Space Policy Institute (ESPI)
- Lina Pohl, Resident Fellow, DLR/European Space Policy Institute (ESPI)
- Mathieu Bataille, Resident Fellow, European Space Policy Institute (ESPI)

AUTHOR

Clémence Poirier is a Resident Fellow seconded by CNES (the French Space Agency) at the European Space Policy Institute (ESPI) in Vienna, Austria. She is also a member of the Space Generation Advisory Council's Space and Cybersecurity Project Group. She holds a master's degree in International Relations, International Security, and Defence and a bachelor's degree in Foreign Applied Languages from University Jean Moulin Lyon 3, France.

ABOUT ESPI

Policy & Strategy

Economy & Business

Security & Defence

International & Legal

ESPI is the European think-tank for space. The Institute is a not-for-profit organization based in Vienna, World capital of space diplomacy, providing decision-makers with an informed view on mid to long-term issues relevant to Europe's space activities since 2003.

ESPI is governed by a General Assembly of member organisations and supported by an Advisory Council of independent high-level experts.

ESPI fulfils its objectives through various multi-disciplinary research activities leading to the publication of books, reports, papers, articles, executive briefs, proceedings and position papers, and to the organisation of conferences and events including the annual ESPI Autumn Conference.

Who we are	What we do
Independent think-tank specialised in space policy	Research and analysis on major space policy issues
Multinational team with interdisciplinary expertise	Monitoring of global space trends and policy developments
Part of a network of European and international partners	Organization of thematic conferences and workshops

Download our reports, check out our events and subscribe to our newsletter online

www.espi.or.at

Schwarzenbergplatz 6 | A-1030 Vienna, Austria | (Entrance: Zaunergasse 1)
Phone +43 1 718 11 18 - 0 | E-Mail: office@espi.or.at

Schwarzenbergplatz 6, 1030 Vienna
(Entrance: Zaunergasse 1)

+43 1 718 11 18 - 0
office@espi.or.at

www.espi.or.at