Space, Cyber and Defence

Navigating interdisciplinary challenges

ESPI

Report:

Title: “ESPI+ Report - Space, Cyber and Defence: Navigating interdisciplinary challenges”

Published: November 2023

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

ESPI is not responsible for any losses, injury or damage caused to any person or property (including under contract, by negligence, product liability or otherwise) whether they may be direct or indirect, special, incidental or consequential, resulting from the information contained in this publication.

ABOUT ESPI+

ESPI+ is a collaborative publication format established by the European Space Policy Institute (ESPI). This new format is designed to unite contributions from various experts in a specific field that is relevant to the Institute's ongoing work. In this context **ESPI acts as the focal point**, directing research questions, identifying synergies between ongoing activities in academia, industry, policymaking and media, facilitating exchange through ESPI-hosted workshops and refining final policy recommendations.

The primary goals of ESPI+ are to simultaneously create comprehensive reports on a given topic by collating expert inputs, respond to topics of particular temporal relevance from a multidisciplinary perspective, and build stronger and more resilient knowledge communities in Europe by:

Leveraging Multidisciplinary Expertise: Space policy and related topics are complex and multifaceted, requiring insights from a diverse range of experts, including scientists, engineers, policymakers, economists, and legal scholars. ESPI+ recognises the need to tap into this wealth of multidisciplinary knowledge to develop comprehensive reports, resulting in more nuanced and informed analysis.

Fostering Knowledge-driven Collaboration: ESPI+ encourages collaboration and knowledge sharing among experts in the field. It provides a platform for experts to work together, exchange ideas, and contribute to a collective body of work, fostering a sense of community and cooperation within the space policy domain.

Enabling Enhanced Clarity and Accessibility: ESPI+ combines expert inputs into a single, coherent report. This format streamlines the information, making it more accessible and easier for readers to understand.

In summary, ESPI+ is a collaborative concept that recognises the complexity of space policy. By uniting experts and harnessing their collective knowledge, it strives to produce reports that are nuanced, provide a broad spectrum of insights, and cultivate a spirit of community and shared endeavour.

Stay tuned for **future opportunities to collaborate** under the ESPI+ Framework.

Table of Contents

INTRODUCTION

Background and rationale

On February 24th, 2022, Russia started its full-scale invasion of Ukraine. More than a year later, the war is still ongoing. Since the attack against KA-SAT, analysed in ESPI's report on "The War in Ukraine from a Space Cybersecurity Perspective", the situation has further deteriorated, both in Ukraine and in the overall space and security fields.

The war continues to demonstrate an extensive use of space solutions by both sides of the conflict. **While the use of space to support military operations on Earth is not a novelty, the extent and magnitude of its use in the Russo-Ukrainian war is unprecedented.** More importantly, Ukraine does not have sovereign space assets and has relied on commercial space systems and services, which directly contributed to its capacity to withstand the Russian invasion. In addition, **the use of commercial space services on a large scale to support both the conduct of operations on the ground as well as the access to connectivity for the civilian population in conflict areas remains unparalleled.** It also reduced the pre-existing space capabilities gap between the two opponents, which led to descriptions of the war as the *"first two-sided space war"*[2] or the *"first commercial space war"*.[3]

Furthermore, **multiple attacks were carried out by both Russia and the IT Army of Ukraine on commercial and state space infrastructures.** On the one hand, Russia targeted Starlink's network on multiple occasions with both electronic and cyberwarfare. It also seems that it attacked Inmarsat's network, which supports critical infrastructures in the United States by exploiting similar vulnerabilities to the ones exploited in the KA-SAT attack. On the other hand, the IT Army of Ukraine attacked the Russian Gonets satellite network, Megafon, and the Statis satellite network.[4] The hacktivist group Anonymous also targeted, in support of

A follow-up to ESPI's Report on "The War in Ukraine from a Space Cybersecurity Perspective"[1]

In October 2022, ESPI published a report, which analysed the Russian cyberattack on ViaSat's KA-SAT satellite network that occurred a few hours before the invasion of Ukraine.

The report analysed that the KA-SAT cyberattack can be considered as a representative case of the state of cybersecurity in the space sector as well as a good illustration of the evolution of the militarisation and weaponisation of both space and cyberspace.

It also underlined that the supply chain and the user segment, which were targeted in the attack, are often crippled with unpatched vulnerabilities.

Additionally, the report explored issues at stake regarding the public attribution of the attack.

Finally, the study provided some political, military, and legal lessons to learn from this attack for the security of the European space infrastructure at large.

[1] Poirier, Clémence. ""ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective", European Space Policy Institute, October 2022. https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf.
[2] Massa, Mark. "Early Lessons from the Russia-Ukraine War as a Space Conflict." Atlantic Council, August 31, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/.
[3] Erwin, Sandra. "On National Security: Drawing Lessons from the First 'Commercial Space War.'" SpaceNews, January 23, 2023. https://spacenews.com/on-national-security-drawing-lessons-from-the-first-commercial-space-war/.
[4] Onefist. "Operation Cataclysm." Team Onefist, November 6, 2022. https://www.onefist.org/post/operation-cataclysm; Onefist. "Operation Pleiades." Team Onefist, November 6, 2022. https://www.onefist.org/post/operation-pleiades; Onefist. "Operation Polaris." Team Onefist, November 6, 2022. https://www.onefist.org/post/operation-polaris.

Ukraine, Russian space-based services with electronic and cyberattacks[5], thereby extending warfare to both the space and cyber domains. Space assets are seen by both parties as a direct enabler of military operations, and therefore as a potential target to disturb and destroy.

The various aforementioned threats and events shed light on the increasing militarisation of outer space and cyberspace. In the past ten years, states have noticed an increase in hostile behaviours, attacks below the threshold of armed conflict, demonstrations of power, and irresponsible uses of outer space. **The current situation is therefore only the corollary of developments that have occurred in the space and cyber domains in the last decade.**

This Report initially takes stock of the overarching security context in which space assets and space actors operate, before taking a deep dive into the technical and governance aspects of the nexus between cybersecurity, space and defence.

Adapting to a changing threat landscape

In this context, European policy-makers should foresee and prepare for the challenges that current developments are uncovering. Past months have already seen an evolution of the European space security framework, most of it having been initiated prior to the war in Ukraine. Yet, the war and the use of space in the conflict only contributed to accelerating these initiatives, as well as further reinforcing the establishment of policy, legal, and programmatic measures.

First, the project to create a **European secure connectivity constellation**, IRIS^2, was formally adopted by EU political authorities in February 2023, following a political agreement reached in 2022. The constellation will be used to strengthen the sovereignty of the EU and its Member States in this domain and support "governmental applications, mainly in the domains of surveillance (e.g., border surveillance), crisis management (e.g., humanitarian aid) and connection and protection of key infrastructures (e.g., secure communications for EU embassies)".[6]

In addition, the **security dimension of existing EU flagship programmes** is expected to increase. For instance, the Full Operational Capability of Galileo's Public Regulated Service should enter into service in 2023.[7] Similarly, EU authorities asserted their willingness to expand Copernicus services to provide an EU Earth Observation governmental service, and a pilot project is expected in the current Space Programme.[8]

At the policy level, the **Strategic Compass**, which provides a shared assessment of the strategic environment, threats and challenges that the EU faces, was released in March 2022. The document called for the publication of an **EU Space Strategy for Security and Defence**, which was released in March 2023. This Strategy formally connects space with civil security and military considerations at the EU level. In particular, the document calls for measures to enhance the resilience and protection of space systems and services in the Union; respond to space threats; enhance the use of EU space capabilities for security and defence; and partner for responsible behaviours in outer space. The cyber dimension is fully integrated into the document and recognised as a key dimension that needs to be addressed to protect European space systems.

[5] "Anonymous Hack Russia's Spy Satellites, Leak Documents from Roscosmos." Technology.org, March 4, 2022. https://www.technology.org/2022/03/04/anonymous-hack-russia-spy-satellites/.

[6] "Iris2: The New EU Secure Satellite Constellation." European Commission. Accessed August 29, 2023. https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en.

[7] Gutierrez, Peter. "Fully Operational Galileo PRS Edges Closer." Inside GNSS, September 15, 2022. https://insidegnss.com/fully-operational-galileo-prs-edges-closer/.

[8] European Commission & High Representative of the Union for Foreign Affairs and Security Policy Joint Communication to the European Parliament and the Council – European Union Strategy for Security and Defence", March 2023

At the regulatory level, the **EU NIS2 Directive on measures for a high common level of cybersecurity across the Union** was adopted in November 2022 and entered into force in January 2023. The Directive recognises space as a "sector of high criticality" and thus outlines stronger cybersecurity measures, reporting obligations, incident response mechanisms, and fines for non-compliance for "*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*".[9] The EU also adopted the **Critical Entity Resilience Directive**, which outlines rules for facing non-cyber and physical threats, which also applies to the space sector.[10]

In addition, the EU is expected to propose an EU Space Law in the coming months, with one of its objectives being to support the resilience of EU space infrastructure. However, it remains to be seen how current threats to space systems will be addressed. The consultation conducted by the European Commission on the EU Space Law explicitly mentions several types of risks, including some related to the resilience of space infrastructure, with the objective of maintaining its physical and digital integrity and functionality. Further measures on this aspect can therefore be expected.

At the national level, Member States have increased their expenditures in space for security and defence in the past year. As an example, the new **French** military programming law for the period 2024-2030 plans to dedicate €6 billion to space, compared to only €4.3 billion in the previous law for the period 2019-2025. In **Germany**, some parts of the €100 billion special fund for defence announced by Chancellor Olaf Scholz in February 2022 will be used to fund space efforts, in particular on early warning or satellite communications. Another example is **Poland**, which bought a full geospatial intelligence system (including two very-high resolution optical satellites, ground segment and associated services such as training) from Airbus in January 2023.[11] At the supranational level, the EU has dedicated around €450 million to military space projects in five years (2019-2023), through the European Defence Fund and its forerunners (the Preparatory Action on Defence Research and the European Defence Industrial Development Programme). In comparison, the United States alone spent approximately $43 billion on military space activities in 2022.[12]

Finally, at the international and intergovernmental level, the **NATO Space Centre of Excellence** was officially established in Toulouse in early 2023. It will provide expertise and experience related to NATO's interests in space. In addition, the United States and Luxembourg signed an agreement to jointly define and manage satellite communications services through the NATO Support and Procurement Agency, with the aim of serving security and defence activities. A new initiative, the Alliance Persistent Surveillance from Space, was also established to make better use of institutional and commercial remote sensing satellites and reinforce the intelligence, surveillance and reconnaissance capabilities of NATO.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555

[10] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

[11] "Airbus to Provide Poland with a Very High Resolution Optical Satellite System." Airbus, January 4, 2023. https://www.airbus.com/en/newsroom/press-releases/2023-01-airbus-to-provide-poland-with-a-very-high-resolution-optical.

[12] Theresa Hitchens, Led by US, global spending on military space jumped to $54B in 2022: Space Foundation, Breaking Defense, 26 July 2023, https://breakingdefense.com/2023/07/led-by-us-global-spending-on-military-space-jumped-to-54b-in-2022-space-foundation/

Navigating the space-cyber-defence nexus

As the environment is changing rapidly, it requires us to reflect upon the frameworks and approaches in which space assets and services are procured, used, protected, and (potentially) attacked. Two elements are worth investigating further:

- The war in Ukraine unveiled overarching trends such as the **decisive role played by private space actors in the conduct of a conflict**. It raises questions regarding the role, capacity, and behaviour of such actors in their support to foreign military operations. It also questions the power balance between these space companies and a state that is or would be reliant on their systems for sovereign missions.
- Given the increasing integration of space and cybersecurity, it appears **crucial to understand whether European states would have the capacity to prevent, protect, and react to an event similar to the KA-SAT cyberattack.** To this end, analysing current national governance structures dedicated to the cybersecurity and cyber defence of the space infrastructure as well as the political, military, and industrial readiness level to cyber threats on space systems is an essential step.

The space-cyber-defence nexus has long been overlooked in the political science literature. While the topic has recently gained traction, many aspects and perspectives remain to be analysed. To reflect on these critical issues, as a follow-up of its 2022 Report on The War in Ukraine from a Space Cybersecurity Perspective, ESPI invited external authors to provide their views in a collective publication, to vary the perspectives and open the perimeter of reflection. The articles were prepared between February and May 2023. In addition to the collection and edition of the articles by ESPI, a workshop was organised with the authors in order to exchange ideas and ensure consistency between the contributions.

Despite this collective work, the words, ideas, arguments, and opinions expressed in the following chapters are the sole responsibility of their authors and only reflect their own point of view. Ideas do not necessarily represent the opinions and positions of the European Space Policy Institute (ESPI) or the authors' affiliated organisations.

Structure of the report

The war in Ukraine has illustrated many of the underlying trends that were ongoing in the space and defence realms. One of the most important is the increasing use of commercial actors for the conduct of military operations, as well as the many questions and concerns that this increased reliance creates. This topic, reflecting on the broader context of today's use of space assets in conflicts, is at the core of the opening contribution to this report.

Furthermore, the conflict crystallised the growing role played by the cyber dimension of space assets, including in the defence field. Therefore, building upon the previous ESPI report, the remaining chapters focus on this particular dimension. The cyber dimension is first tackled from a technical perspective in this report's second contribution, which is followed by three contributions exploring the governance perspective of space, cybersecurity and defence. These governance chapters focus on the analysis of the integration of cyber issues into the military space organisational and policy frameworks of three major European countries, France, Italy and the United Kingdom.

The conclusion of the report highlights the key questions raised in the different contributions, in particular those related to definitions of activities and systems, which will need to be clarified for the future (e.g., what should be considered as an attack against a space system? How can we say whether a satellite is civil, military or dual?). It also identifies challenges that will have to be tackled to better address the cybersecurity dimension of space in military operations.

Name	Description
Béatrice Hainaut	The article provides an operational, legal, and political perspective on the role of commercial actors in Ukraine and the benefits and challenges of using commercial space assets for the conduct of military operations. It investigates the risks created by increased reliance on private actors, in particular for states without national capabilities, but also the consequences that the use of these spacecraft will have on military operations in space.
Nicoló Boschetti, Ioannis Nikas, Dimitrios Serpanos and Gregory Falco	This contribution adopts a technical approach to describe the cyber operations that have been ongoing before and during the conflict in Ukraine and analyse the threats that these developments in the cyber realm create for space systems. The article then explores how such threats could constitute a danger for the security of EU space programmes with the objective of providing key elements for the security of future European architecture.
Paul Wohrer and Xavier Pasco	The article describes the space cybersecurity governance framework in France, clarifying the role of the different institutions actively participating in this field and highlighting the separation between defensive and offensive operations that characterises the French doctrine. The authors then recall that developments in the space sector (e.g., New Space) create additional risks, which are yet not addressed through the development of a dedicated space cybersecurity policy.
Giancarlo La Rocca	This contribution presents the evolutions that have shaped the Italian space policy and governance in recent years, and the ways in which the new organisational structure adopts a more comprehensive approach mixing civil and military organisations and instruments to better integrate and respond to cyber threats against space systems.
Christoph Beischl	This article examines the defence-specific policy objective of the United Kingdom at the intersection of space and cybersecurity. It holds that the UK has not clearly stated any such objective. However, a thorough analysis of selected official documents reveals that the UK has, nonetheless, vaguely established the defence-specific policy objective of "advancing the cybersecurity of UK defence-linked space capabilities and capacities, primarily against (actual and potential) cyber threats posed by adversaries". The article further identifies seven strategic elements serving the pursuit of this objective.

INTERDISCIPLINARY QUESTIONS

The war in Ukraine has further emphasised the critical role of space assets and associated services in conflict. In particular, the use of commercial services to directly support military operations has resulted in new policy considerations, and opened possibilities to develop and implement new operational strategies. The contribution in this opening Chapter provides an overview of operational, legal, political, and strategic questions related to the use of commercial satellites in conflict.

Operational, Legal, Political and Strategic Implications of Using Commercial Satellites in War

Béatrice Hainaut, 'Space Domain' Researcher, Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM)

"The use by the United States and its allies of the elements of civilian, including commercial, infrastructure in outer space for military purposes. It seems like our colleagues do not realize that such actions in fact constitute indirect involvement in military conflicts. Quasi-civilian infrastructure may become a legitimate target for retaliation."[13]

"(…) the Islamic Republic of Iran holds the US Government responsible for such unlawful and irresponsible operation by its SpaceX Corporation. It is not secret that Starlink is not merely a civilian project and has military objective as an element for militarization and integration of an arms race in outer space to threaten national security of states. Therefore, the Islamic Republic of Iran reserves its inherent right to respond in accordance with international law and the Charter of United Nations to any threat posed or wrongful act against its national sovereignty and its territorial integrity, by the conduct and action of constellation companies in Iran's territory."[14]

These two statements were made respectively by Russia and Iran during the sessions of the Open-ended Working Group (OEWG) on Reducing Space Threats[15]. This OEWG took place in a context of rising tensions due to the war in Ukraine, in which satellites are playing a key role.

In November 2021, Russia destroyed one of its satellites in space with a missile. Today this event can be seen as a harbinger of the war in Ukraine and the related "space war". Then, on February 24th, one hour before invading Ukraine, Russia launched a cyberattack on ViaSat's KA-SAT satellite network, which was used by the Ukrainian army. As Ukraine has no indigenous space capability, on February 26th, Mykhailo Fedorov, Ukrainian Vice Prime Minister for Innovations, Development of Education, Science & Technologies, asked Elon Musk, the CEO of SpaceX, to provide Ukraine with Starlink stations[16], which he did two days later. Starlink stations provide connectivity to Ukrainian people and Ukrainian troops. Then, other space services were provided to Ukraine in order to plan and conduct war, such as Earth observation, which aims at locating the progression of Russian troops and targeting them. Space connectivity aims at delivering information between the scattered Ukrainians troops on the battlefield and communicating orders. The vast majority of these satellites are registered in the United States of America (USA)[17], which decided to support Ukraine. In this context, space systems become critical infrastructures and several countries are considering

[13] Statement by the Head of the Russian Delegation K.V. Vorontsov at the second session of the Open-Ended Working Group established pursuant to UNGA resolution 76/231, 12 September 2022, Unofficial-translation-in-English.pdf (unoda.org)

[14] Statement made by the Islamic Republic of Iran, 3rd Meeting, 3rd Session Open-ended Working Group on Reducing Space Threats, 31 January 2023, 01:55-02:10, 3rd Meeting, 3rd Session Open-ended Working Group on Reducing Space Threats | UN Web TV

[15] OEWG was established by resolution 76/231 of the General Assembly of the United Nations (UN), in order to take stock of the existing international legal and other normative frameworks concerning threats arising from State behaviors with respect to outer space; to consider current and future threats by states to space systems, and actions, activities and omissions that could be considered irresponsible; to make recommendations on possible norms, rules and principles of responsible behaviours relating to threats by space-to-space systems, including as appropriate, how they would contribute to the negotiation of legally binding instruments, including on the prevention of an arms race in outer space. Three sessions out of four have taken place so far. Microsoft Word - OEWG OS 2022-01-04 NV e (un-arm.org)

[16] Elon Musk sur Twitter: "@FedorovMykhailo Starlink service is now active in Ukraine. More terminals en route." / Twitter

[17] In accordance with the Convention on Registration of Objects Launched into Outer Space, 1974, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html

commercial space systems, which provide services to belligerents, as legitimate targets. These commercial space systems are particularly vulnerable to electronic and cyber threats, and potentially to kinetic and other non-kinetic threats. For instance, SpaceX leaders report that Starlink is facing regular jamming and hacking.

During the OEWG's discussions, the use of civilian or "quasi-civilian" space systems was mentioned repeatedly. Certainly, this contributes to the escalation of tensions between some states. Russia mentions it in line with the war in Ukraine, while Iran does it in the context of its internal unrest, but both address their complaints to the USA.

As a consequence, it is relevant to think about the operational, legal, political and strategic implications of using commercial satellites in war.

Operational implications

States can no longer conduct a war without the support of space applications. They orient military maneuvers. For that matter, in 2022, Russia accelerated its deployment of military space-based capabilities to support its troops on the ground. In order to try to defeat Russia, Ukraine, as a state without indigenous space capabilities, had no choice but buying space services to commercial actors. We can therefore analyse the operational implications of that use.

In 1991, the United States declared that the Gulf War was the "first space war"[18] in the sense that satellites, especially military, had been used massively in the conduct of the conflict. In 2022, the Russia-Ukraine war is "perhaps the first two-sided space war"[19]. Space is no longer just an environment but has become a domain of operations. Indeed, in 2019, the North Atlantic Treaty Organization (NATO) acknowledged that outer space is a "warfighting domain", alongside the domains of land, sea, air and cyber. The European Union (EU) Strategic Compass of 2022 also considers outer space as an operational domain in which the EU can act[20].

The war in Ukraine has shed light on an old-known fact, the military use of space. It is not the first time that civilian satellites are used in a military conflict. However, what is new is the massive use of commercial, dual-use satellites by an actor, which does not have sovereign capabilities in orbit for the planning and conduct of military operations on the ground. Typically, space-based communications and intelligence, surveillance, reconnaissance (ISR) assets are used effectively. For instance, Earth observation provides information on the maneuver of Russian troops and help to understand the military intentions of the adversary. Infrared and synthetic-aperture radar can "see" at day and at night and whatever the weather conditions (e.g., through clouds). Imagery can be complemented by radiofrequency. It detects electromagnetic signals from radars, for example, in order to target them. Connectivity satellites provide communications between Ukrainian troops. The space assets accelerated the battle pace. To maintain military advantage over the enemy, anticipating and constraining its maneuvers are key. So, Ukraine benefits from the proliferation of commercial space actors providing space services such as radar (ICEYE) and optical imagery (MAXAR, Planet Labs…), radiofrequency (HawkEye 360) and connectivity (Starlink). Finally, these services rely on constellations of satellites, which means that the situational awareness over

[18] Marie-Madeleine de Maack, « La guerre du Golfe ou l'introduction des moyens spatiaux dans l'art de la guerre », in Guerres mondiales et conflits contemporains, Presses Universitaires de France, 2011/4 n°244, p.81-94.
[19] David T. Burbach, Early lessons from the Russia – Ukraine war as space conflict, 30 August 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/
[20] Council of the European Union. 2022. A Strategic Compass for Security and Defence. 7371/22

Ukraine is updated frequently (due to an increased revisit rate). All these space applications are dual-use and constitute space support to operations.

Before the war, Ukraine was already a space user, but it was incentivised to "militarise" its uses to cope with Russian forces. For example, Starlink's satellites are used to guide drones, while other space services contribute to target, adjust artillery fire, make battle damage assessment etc. When Russia conducted a cyberattack against ViaSat's satellite network, it wanted to weaken the Ukrainian army and society. Space resilience came from SpaceX's Starlink constellation. But if commercial space applications became crucial to Ukrainians, alone, they are not sufficient to win a war. Indeed, to act, Ukraine also needs conventional military assistance with diverse type of weaponry provided. Besides, the support of private actors can never been taken for granted as proven by SpaceX's decision to limit the capabilities of Starlink in Ukraine.

As seen, satellites become more and more critical in the conduct of operations. Therefore, they need to be better protected in space, especially in face of a renewed threat environment[21]. Russia considered that commercial systems could be legitimate targets for retaliation, which raises questions on the means and ways in which it can retaliate. Indeed, space has physical characteristics that constrain its use. Destroying a satellite in space by kinetic attack produces a great amount of debris that will last long and prevent the sustainable use of outer space. Some states are technically able to destroy satellites in space. But states with actual ASAT technologies are space dependent too and, therefore, the debris generated by a kinetic attack would negatively affect the attacker. Besides, the service provided by a constellation is resilient against a kinetic attack. Therefore, the operational gain may not be so significant for the attacker. Yet, even if the attacker has satellites, if it has significantly less space assets, it could make the choice of kinetic threats considering that potentially losing its satellites would be less damaging than for its adversaries. Despite this caveat, the most likely form of retaliation is non-kinetic, in particular cyber as seen already against ViaSat's and Starlink satellite network. However, the attacker does not master all the consequences of a cyberattack, as users are many and spread around the world; besides, the attack may be internationally condemned.

Before destroying satellites, the USA joint doctrine for space operations recognises that a range of "space control" negation operations can be conducted to target adversary space systems: deceive, disrupt, deny, degrade, and destroy[22]. It therefore seems unlikely that kinetic destruction (kinetic anti-satellite missile) would be the preferred mode of attack. It will remain rare, confined to targeting non-redundant capabilities of the adversary or to make a show of force like Russia did in November 2021. Conversely, cyberattack and electronic warfare will likely be common in case of tensions as well as espionage in orbit. The operational challenge is to better protect space systems against non-kinetic threats. But if so far SpaceX seems to be able to face the attacks, is it the case for other companies? They will probably need to redirect some extra budget to dedicate it to cybersecurity, or at least more than previously expected.

Legal implications

According to Article III of the Outer Space Treaty (OST), States Parties shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining

[21] For example, in 2022, Russia launched satellites of the Nivelir range capable of inspection missions and maneuvers in low-earth orbit , Soyuz-2.1v launches satellite pair after multi-day delay - NASASpaceFlight.com, 21 October 2021.
[22] Jeremy Grunert, "The US Space Force at 3: Growing Dangers For a Growing Branch", 23 December 2022.

international peace and security and promoting international cooperation and understanding[23]. In outer space, the following international law applies: the UN Charter, the space law treaties, the law of neutrality and the International Humanitarian Law (IHL) or law on armed conflict (LAC) in case of armed conflict. However, some states, such as Russia, Iran, and China, do not recognise the applicability of the IHL in space.

Russia declared the commercial satellites used by Ukrainian troops as legitimate military targets invoking its inherent right of self-defence (Charter of the UN, Chapter VII, Article 51). Iran also invokes this right but without precision on what kind of action it will undertake. Indeed, states may therefore consider options to retaliate in space, but also in other warfighting domains and through diplomatic and political means. While retaliating in a kinetic form would not be a responsible behaviour regarding space sustainability, there are currently no legally binding rules to prevent the use of anti-satellite weapons and the creation of debris. Furthermore, some states do not recognise the applicability of the IHL in outer space. IHL is a set of rules that seeks, for humanitarian reasons, to limit the effects of armed conflict. Their argument is that as there will be no use of force in space, then there is not even the need to wonder whether IHL applies. However, first, when Russia clearly envisions targeting commercial satellites, this is a use of force. Secondly, a significant part of the IHL is, however, recognised as customary law and so enforceable to all states[24]. As mentioned earlier, IHL aims at limiting the effects of armed conflict. If not applied to space, the consequences of attacks would not be circumscribed by the Law. These states are using the Law for strategic purposes in a context of interstate tensions, known as the practice of lawfare.

Therefore, if retaliation in space occurred, Russia would have to take into consideration, in its analysis, the IHL legal requirements, namely the *distinction* and *proportionality*.

About the *distinction* between civilian and military space objects: there are several identification criteria, including a criterion related to the nature and a criterion related to the use of the object. Indeed, *"Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."*[25]

Military satellites recognised as such by their state owners are by nature military objectives. However, civilian satellites used in an armed conflict become military objectives because of their use. But, *"In case of doubt, whether an object which is normally dedicated to civilian purposes,* [...] *is being used to make an effective contribution to military action,* (...) *it shall be presumed not to be so used*"[26].Therefore, in case of doubt, dual-use satellites should not be qualified as military objectives. According to the numerous examples listed above, it can be assessed that commercial satellites used by Ukrainian troops make an effective contribution to military action. However, they are also used for civilians' needs and their destruction, capture or neutralisation can prejudice the population. In that case, the problem of dual-use satellites is up to the applicability of the IHL legal requirements, namely proportionality (and precaution)[27].

[23] United Nations treaties and principles on Outer Space, United Nations Publication, 02-57669 (unoosa.org)
[24] Louis Perez, « L'application du droit des conflits armés à l'espace extra-atmosphérique », Note de Recherche n°69, IRSEM, 31 janvier 2019,
[25] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Part IV, art.52 § 2, IHL Treaties - Additional Protocol (I) to the Geneva Conventions, 1977 (icrc.org)
[26] *Ibid.*, Part IV, art.52 § 3.
[27] Manuel de droit des opérations militaires, Ministère des Armées, 2022, pp. 292, 2204_0002_Manuel_DAJ_C18_CORRIGE.indd (defense.gouv.fr)

Clearly, the satellites used by Ukraine are, by design, civilian. But they became dual-use by necessity. According to SpaceX, Ukraine is using Starlink's services for offensive purposes, an application that the company never intended to support.[28] Ukraine "weaponised" Starlink[29]. As a result, SpaceX took steps to limit Starlink's use in supporting offensive military operations[30]. Generally speaking, even if commercial actors want to provide space services, they remain private companies. They may not agree with all the uses that are made of their services by a belligerent. Can they legally limit the capacity of their systems? In one way or another, they do influence battlefield performance in a tangible way. If they can legitimately fear retaliation from a belligerent, can they ask for protection[31] or indemnification[32] from their state?

About *proportionality*. This principle establishes that some types of attacks are to be considered as indiscriminate. For instance, an attack, which may be expected to cause incidental loss of civilians, damage to civilian objects, or a combination thereof, would be excessive in relation to the concrete and direct military advantage anticipated[33]. According to IHL, this type of attack is not permitted during a conflict.

To what extent is this principle applicable to space? At first, a satellite could be seen as an attractive target. Simply because there is no human being in space (except in the International Space Station). Then, if the target is a fully military satellite and the attack does not create debris in space, the proportionality principle is met. But there are many civilian applications derived from the operation of space systems. The cyberattack against ViaSat's network had consequences not only in Ukraine but also in Europe. So proportionality in space could be defined by the type of missions that the satellite supports on Earth and the extent to which it impacts civilians. Does the attack cause loss of civilians and damage civilian objects in an excessive manner? An assessment would be necessary, even if this is hard to make precisely. Indeed, it could be difficult to assess the ripple effects or "reverberating effects"[34] of this kind of attack against a dual-use space system.

Political and strategic implications

It is possible that an attack against an asset under American liability, whether kinetic or non-kinetic, would provoke an American response. Indeed, the vast majority of commercial satellites used by Ukraine are registered in the USA. Therefore, the country bears international responsibility for them, according to article VI of the OST. According to international law, these attacks could be interpreted as armed aggression. In any case, the decision to retaliate or not, and how to do it, will be a political decision, and not the decision of a private company.

American authorities are not embarrassed by the fact that American commercial satellites are heavily used by Ukrainians troops. However, both Western countries and the USA remain cautious not to fully take part in the conflict. They do not want to be considered as belligerents. It is not the

[28] Jeff Foust, « Shotwell : Ukraine « weaponized » Starlink in war against Russia », Space News, 8 February 2023
[29] *Ibid.*
[30] *Ibid.*
[31] Theresa Hitchens, Commercial remote sensing firms seek government help to plan for, respond to sat attacks, Breaking Defense, 21 March 2022, https://breakingdefense.com/2022/03/commercial-remote-sensing-firms-seek-government-help-to-plan-for-respond-to-sat-attacks/
[32] Sandra Erwin, "US weighing options to compensate commercial companies if satellites are attacked", Space News, 15 September 2022, https://spacenews.com/u-s-weighing-options-to-compensate-commercial-companies-if-satellites-are-attacked/
[33] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, Protocol 1, 8 June 1977, Article 51 – Protection of the civilian population 5 b)
[34] Jessica West, Almudena Azcarate Ortega, "Norms for Outer Space, A Small Step or a Giant Leap for Policymaking ?", March 2022, Space Dossier 7, UNIDIR.

case today[35] and the notion of 'co-belligerent' does not exist in the international law. These states have not declared themselves as neutral[36] either, according to the Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land adopted in The Hague in 1907. They can be considered as non-belligerents even if this term is not defined under international law.

Commercial space actors play a critical role in Ukraine. That creates an unusual situation. Some of these actors are suggesting and/or interfering with national foreign policy positions. This is particularly the case of SpaceX's CEO Elon Musk who, for instance, proposed a "peace plan" for Russia and Ukraine. The involvement of space companies in politics goes beyond the war in Ukraine. Indeed, Elon Musk also published the number of Starlink terminals in Iran despite the ban on them in the country, and he proposed that Taiwan becomes a "special administrative zone of China"[37]. Consequently, some have described him as a "Geopolitical Chaos Agent"[38]. Of course, SpaceX has a unique position because of its – even if temporary – monopoly on connectivity constellations. Indeed, so far, there is no equivalent of Starlink constellation. That may encourage Elon Musk to interfere in the complex global politics. But what is at stake here is the legitimacy of private actors to suggest solutions to global politics and the non-coordination that can occur between private space actors and their public authorities. Finally, the reactions of the states mentioned in these public statements may be uncontrollable for official authorities (for example the Iran's reaction *vis-à-vis* the USA).

Moreover, the initiatives of private actors can have dangerous consequences. In Iran, Starlink users are exposed to a phishing scheme that is organised by Iranian pro-government hackers. They provide malicious links, claiming to provide access to Starlink[39]. In addition, because Starlink terminals are traceable, revealing information on them puts their end-users in danger. Some qualify Musk's action as "irresponsible" although the U.S. government supports it[40]. To what extent does the U.S. government control Elon Musk's actions?

Apart from SpaceX, Elon Musk leads the Tesla and Neuralink companies. These commercial businesses' interests could create, at some point, discrepancy with the political objectives. For example, Musk wants to develop his activities in China and to this end, he is committed to keeping good relations with the Chinese authorities. He wants to expand the Tesla's Shanghai Gigafactory, which is the Tesla's most productive manufacturing hub. In addition, the bulk of Musk's wealth comes from his electric car company. In case of direct or indirect conflict with China, the United States would rely on SpaceX (among other contractors) for connectivity. Beyond SpaceX, the question is to know if the United States will be able to count on private space actors when they need them[41], whatever the economic consequences for the latter.

In order to ensure this access, the U.S. Space Force, amongst other governmental entities, is finding ways to benefit from non-military space services in time of crisis or conflict. This initiative goes

[35] Julia Grignon, La guerre en Ukraine et le droit des conflits armés, Brève stratégique n°35, 28 mars 2022, https://www.irsem.fr/publications-de-l-irsem/breves-strategiques/breve-strategique-n-35-2022-la-guerre-en-ukraine-et-le-droit-des-conflits-armes.html

[36] In the French Law of War Manual of war, a neutral State has to limit its governmental or non-governmental space assistance to the belligerents. Manuel de droit des opérations militaires, Ministère des Armées, 2022, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Manuel%20de%20droit%20des%20op%C3%A9rations%20militaires.pdf

[37] Roula Khalaf, Elon Musk : Aren't Entertained?", Financial Times, October 2022, https://www.ft.com/content/5ef14997-982e-4f03-8548-b5d67202623a

[38] Cade Metz, Adam Satariano, Chang Che, How Elon Musk Became a Geopolitical Chaos Agent, The New York Times, 26 October 2022.

[39] *Ibid.*

[40] Charles Mok, Influencing the Influencer: China and Elon Musk, The Diplomat, 11 october 2022, https://thediplomat.com/2022/10/influencing-the-influencer-china-and-elon-musk/

[41] Sandra Erwin, With Starshield, SpaceX readies for battle, Space News, 19 January 2023.

beyond the current "spontaneous" space support to Ukraine. The objective is to establish a clear framework going through all the complexities (in terms of contracts, financing, indemnification, operational implementation etc.) and create the equivalent of the Civil Reserve Air Fleet (CRAF), named the Commercial Augmentation Space Reserve (CASR)[42].

Still, with the multiplication of commercial space applications in the years to come, it is highly probable that governments will face tricky situations in future conflicts. The blurred line between powerful private actors and state actors could strengthen the fog of war.

Conclusion

The war in Ukraine has shed light on the implications of the massive use of commercial, dual-use satellites for military purposes and in an armed conflict. States are responsible for national activities in outer space, even if they are carried out by non-governmental entities. States can take advantage of this situation against their adversaries or enemies, without being directly involved in the conflict. Nevertheless, this is a tricky situation for the commercial actor that can become a military objective. For dual-use satellites, operational consequences are linked to the fact that a great number of civilians use and depend on these space systems. There are legal implications too. International law applies in space without any doubt. However, its applicability needs further analysis so that the characteristics of the space environment would be taken into account. Finally, the ramping-up of commercial space actors raises the question of possible conflicts of interests. On the one hand, commercial space activities are driven by profit. Space has to be profitable like any other business. On the other hand, war is a highly political phenomenon. Are both activities compatible? It is crucial to take into account these implications and their lessons learned in order to orient future European space choices.

[42] Theresa Hitchens, "Space Force 'framework' for commercial reserve satellite fleet coming in summer", *Breaking Defense*, 21 April 2023, https://breakingdefense.com/2023/04/space-force-framework-for-commercial-reserve-satellite-fleet-coming-in-summer/

TECHNICAL PERSPECTIVES

Having investigated the wider multifaceted questions raised by the current context in Ukraine, the report moves to the analysis of the cyber dimension of this conflict, starting with its technical aspects. The Chapter below describes the different cyberattacks against space systems that have taken place during the conflict and highlights the implications it may have for the protection of the EU Space Programme components.

Towards more robust European space networks after the Ukrainian War experience

Nicolò Boschetti, Ph.D. Student Aerospace Engineering, Cornell University, Sibley School of Mechanical and Aerospace Engineering

Ioannis Nikas, Mechanical Engineering Student, The Johns Hopkins University

Dimitrios Serpanos, Professor, The University of Patras & President, Computer Technology Institute and Press (CTI)

Gregory Falco, Assistant Professor, Cornell University, Sibley School of Mechanical and Aerospace Engineering & Systems Engineering Program

Securing space infrastructure has become increasingly important in recent years as the use of space-based assets for military and civilian purposes has grown. The importance of space in the last years has developed as much as the risk of cyberattacks, as demonstrated by the cyberattack on ViaSat's KA-SAT network in February 2022. This attack, the first of its kind occurring during an armed conflict, highlighted the fragility of the IT architectures and related supply chains that connect military and civilian stakeholders across the European continent.

This article presents an analysis of the cyberwarfare operations in Ukraine since the Russian annexation of Crimea in 2014 and links them to the cybersecurity profile of the European space programmes. Through engineering and intelligence analysis of the Russian cyberwarfare techniques employed in Ukraine and the architecture of a selected European space mission, technical and policy measures that the European Union agencies can enact to strengthen the security of their space-based infrastructure are presented.

EU's Space Services Ecosystem

The European Union has several space-related projects aimed at improving environmental management, civil and human security, and communication services. Copernicus, managed by the European Space Agency and EUMETSAT, provides environmental management, climate change mitigation, and civil security across Europe, with standardised and centralised access to its data through solutions like the Data and Information Access Services (DIAS). Galileo is a global satellite navigation system with 30 satellites in orbit and a ground segment consisting of two control centres, playing an essential role in many EU economic sectors. EGNOS, a Satellite-Based Augmentation System (SBAS), provides improved Position, Navigation, and Timing (PNT) services to aviation, maritime, and land-based users in over 30 countries, with precision positioning up to 1.5 meters. The Space Surveillance and Tracking partnership aims to create a platform for identifying and tracking space objects, integrating national expertise and assets into the sensor network and data processing operations. IRIS^2, a new constellation of satellites launching to provide secure connectivity and communication to European stakeholders, will improve the EU GOVSATCOM capability and provide broadband internet to areas with poor connectivity. The European Quantum Communication Infrastructure (EuroQCI) aims to create a security layer in IRIS^2 using quantum physics to protect data in communication infrastructure. The project will achieve secure quantum encryption named QKD, with the Eagle-1 prototype satellite launching in 2024 to test it in LEO. The project builds on the Horizon 2020 OPENQKD project involving European SMEs, research institutions, and national institutes.

Analysis of Cyber Warfare Operations in Ukraine

Ukraine has been a cyber battleground since the political unrest of 2014, which started with the Euromaidan demonstrations and continued with the progressive alignment of Ukrainian eastern regions with Russia, culminating with the Russian annexation of Crimea and then the invasion of February 2022. This led to the deployment of novel cyberwar technologies, methods, and targets that have significantly influenced the development of cybersecurity and had significant effects worldwide.

Ukraine is known as the site of the first cyberattack on a power grid. In December 2015, a sophisticated attack, employing the BlackEnergy trojan and KillDisk malware, infected computational systems used for power distribution, causing outages for approximately a quarter of a million customers for several hours and repair work for several months. The attack focused on industrial control systems, affecting uninterruptible power supply systems (UPSs) and modems in the infrastructure as well. This first campaign which included spear-phishing emails, hijacking systems to remote control or disable them, and file erasure was followed by a second one in December 2016, which exploited another malware, Industroyer, against power grids' industrial control systems.

The ongoing cyberwar in Ukraine is strongly focused on digital infrastructure with spillover effects over other sectors and architectures. Power grids, communication networks, government services, and media organisations constitute permanent targets, as multiple incidents indicate. In January 2022, weeks before the full-scale invasion of Ukraine, servers across the country were attacked, and data were wiped out with a campaign that exploited an SQL elevation-of-privilege vulnerability, a known vulnerability of Microsoft SQL Servers, to insert erasing malware. At the start of the invasion, another infrastructure attack targeted Viasat's KA-SAT network, disrupting its broadband services in Ukraine and in Europe. Ukrtelecom, Ukraine's largest terrestrial broadband provider, was attacked in March 2022, leading to nationwide connectivity disruptions for several hours.

The Ukrainian cyberwar does include all types of cyberattacks, including disruption of services, through Distributed Denial-of-Service (DDoS) attacks as well as through controlling or destroying infrastructure, website defacement, malware distribution – including ransomware –, data exfiltration, social networking attacks, including mis/dis-information spreading and others.

Several well-known malwares have emerged from incidents in the area. In addition to the infamous BlackEnergy and Industroyer, the most damaging malware worldwide, namely NotPetya, also emerged there. NotPetya, the notorious ransomware, was exploited in a massive supply-chain cyberattack in 2017 and crippled Ukraine and several organisations worldwide, becoming "the most destructive and costly cyberattack in history" as the White House announced.[43]

Cyberwarfare targets include infrastructures to a large degree. As Microsoft recently reported, infrastructure attacks have reached 40% of the cyberattacks in Ukraine.[44] Despite the limited number of incidents, up to this point, on satellite services, i.e. the Viasat incident, it is reasonable to expect that the expanding cyberattacks will extend and spread to satellite networks soon.

[43] White House, "Statement from the Press Secretary," 15-2-2018. [Online]. Available: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/. [Accessed 12-2-2023])
[44] (https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

The Space Dimension of Cyberwarfare Operations in Ukraine

ViaSat KA-SAT Attack

The ViaSat KA-SAT cyberattack targeted the ground segment of the KA-SAT satellite telecommunication network during the first hours of the Russian invasion in February 2022. Specifically, the attackers exploited weaknesses in the ground and user segments managed by the EUTELSAT's subsidiary Skylogic.[45] ViaSat acquired the satellite from EUTELSAT in 2020, but the attack happened while the transition process was still not complete, and the ground segment was still in an external company's hands. The attackers used an unpatched VPN to gain access to Skylogic's Gateway Earth Stations and consequently Surfbeam2 end-user modems.[46] ViaSat's statements confirmed that the attackers moved laterally through the trusted management network to target specific geographic cells and their respective modems. The attacker manipulated the modem's management by providing a 'valid' firmware update, installing an ELF binary that deleted data from the modem's flash memory. The attack had cascading effects in Germany and other European states due to either an error in selecting the targeted geographic signal cells or because the selection of cells containing Ukrainian territory overlapped other EU countries.

Industroyer

In 2016, the Industroyer malware caused a power outage in Kyiv, and researchers believe that it was a preliminary test carried out by threat actors for a more significant cyberattack. It was the first malware designed to target a nation's electrical grid and displayed a high level of technical sophistication in industrial control system (ICS) protocols. The Sandworm group, affiliated to Russia's General Staff Main Intelligence Directorate (GRU), was responsible for the attack and gained direct control of switches in electrical substations. In April 2022, the same group deployed the Industroyer2 malware containing IEC-104 commands to disrupt high-voltage electricity. It shared source code with the original Industroyer and was compiled two weeks before the attack. It was planned to be launched via a scheduled task at a specific time, and a second task would have wiped the attacked device and erased all traces of the malware. Researchers also found evidence of a new wiper variant called CaddyWiper, which aimed to slow down the plant's recovery by encrypting ICS consoles and wiping as many devices as possible. In addition, a second wiper targeted Linux/Solaris hosts and wiped all host data after spreading through accessible network devices via SSH. While researchers are still investigating why Industroyer2 failed to complete its mission, they emphasised that the same build of Industroyer2 cannot be used against other electricity plants since it contains hard-coded IP addresses and uses only the IEC 60870-5-104 protocol.[47] That transmission protocol for network access in ICS based on the IEC 60870-5 standard, is currently adopted by programmable logic controllers (PLCs) like Schneider Electric and OMRON ones.[48] An analysis carried out using Shodan.io assessed that, for example, Schneider Electric PLCs are currently used by Skylogic and EUTELSAT; companies cooperating with ESA programmes and European satellite networks. Furthermore, the U.S. government agencies CISA, DOE, the NSA, and the FBI issued a joint Cybersecurity Advisory following the Industroyer2 attack, warning that certain advanced persistent threat (APT) actors have exhibited the capability to gain complete system

[45] Boschetti, Nicolò, Nathaniel G. Gordon, and Gregory Falco. "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack." In ASCEND 2022, p. 4380. 2022.
[46] Ibid.
[47] Tsaraias, Giannis, and Ivan Speziale. "Industroyer vs. Industroyer2: Evolution of the IEC 104 Component". Nozomi Networks White Paper. 2022.
[48] https://blog.scadafence.com/industroyer2-attack [Accessed 15-2-2023]

access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices.[49]

GNSS Spoofing

At the edge between electronic and cyberwarfare, spoofing consists of the ability to capture, alter, and re-transmit a communication signal in a way that misleads the recipient. It is instrumental if applied to GNSS signals since it can dramatically alter the ability of the victim to assess their position.[50] If jamming is eminently an electronic warfare technique that, by saturating a specific band, impedes a receiver from acquiring an RF signal, spoofing actively mimics a GNSS signal leading to incorrect positioning. Russian security forces have mastered this technique in the last years, and the signalisation of this kind of incident has been reported in the entire territory of the Russian Federation, in Crimea and Eastern Ukraine, and Syria starting in 2014.[51] Several vessels in the Black Sea reported to be spoofed hundreds of kilometres away from their real position; for example this clearly happened during Russian President Putin's visits to Crimea in 2016 and 2018.[52]

Both GNSS systems, such as Galileo, and Satellite Based Augmentation Systems (SBAS) like EGNOS, can be targeted by spoofing attacks like the ones witnessed in the Ukrainian war theatre. However, an SBAS system is more difficult to spoof since the signal sent to the users has different encryption and authentication components than a GNSS signal.[53] Consequently, the security of the authentication keys is of extreme importance for the reliability of the system.

Architectural Analysis of a Copernicus Mission

In order to put into context the cyber and electronic weaknesses emphasised by the Ukrainian experience, the architecture of a Copernicus Mission will be described and then related to specific threat vectors.

The peculiarity of the ESA, EU and broader European space ecosystem is the high heterogeneity of the actors and stakeholders involved in its management. Different segments or specific services of each space activity are managed by a wide variety of national space agencies, whose activity is coordinated or simply harmonised by EU Agencies, such as EUSPA, or international organisations, such as EUMETSAT. Although this fragmentation of management and multi-layer hierarchy may assure a good harmonisation and quality from an operational point of view, it risks widening the attack surface area of the ground segment from a security point of view. In fact, among the several layers of the IT architecture of the different institutions, different Internet Service Providers (ISPs) and third-party suppliers are involved. The great variety of IT architectures, technologies, and protocols makes it easier for possible adversaries to penetrate one system and then perform lateral movements or other actions that complicate the work of authorities in identifying and isolating breaches.

[49] Ibid.
[50] Falco, Gregory, and Nicolo Boschetti. "A security risk taxonomy for commercial space missions." In ASCEND 2021, p. 4241. 2021.
[51] C4ADS (Center for Advanced Defense Studies). "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. Technical Report" Center for Advanced Defense Studies, Washington DC. 2019.
[52] Ibid.
[53] Fernández-Hernández, Ignacio, Eric Châtre, Andrea Dalla Chiara, Giacomo Da Broi, Oscar Pozzobon, Javier Fidalgo, Miguel Odriozola et al. "Impact analysis of SBAS authentication." Navigation 65, no. 4 (2018): 517-532.

To highlight possible points of failures in the ecosystem, this article describes, in **Figure 1**, the architecture of the ground operations of the Sentinel-3 spacecraft, part of the Copernicus Programme.[54] Through a block diagram, we show the data flow from the satellite to the end user, also investigating the operations of a fully operational EUSST Consortium in providing Space Situational Awareness services to the Copernicus Programme. In addition to that, the heterogeneity of the entities responsible for the different functions of the mission has been indicated.

As shown in the following table, the ground operations of the Sentinel-3 satellite are organised as follows:[55]

Function	Responsible Entity	Location
Data Acquisition	Kongsberg Satellite Services (KSAT)	Svalbard Islands and Inuvik (Antarctica)
Payload Data Management Centre (PDMC)	ESA Centre for Earth Observation (ESRIN)	Frascati, Italy
OLCI Instrument Data Land Processing and Archiving Centre (PAC)	DLR	Germany
SLSTR and Synergy Instruments Data PAC	ACRIst	France
Flight Operations Segment	European Space Operations Centre (ESOC) and EUMETSAT	-
Orbit Determination Service and SSA	EUSST	-
Mission Performance Centre	ACRIst	France
Data and Information Access Services (DIAS)	Private Operators	-

Table 1: ground operations of the Sentinel-3

As we will describe in the next paragraph, such architecture and governance model have important technical and political benefits, but at the same time widen the attack surface of a space mission. From a cybersecurity point of view, the dispersion of responsibilities and the coexistence of different architectures in what is a System of Systems (SoS) can weaken the security posture.

[54] Donlon, Craig, et al. "The copernicus Sentinel-3 mission and oceanography: overview and current status." EGU General Assembly Conference Abstracts. 2014.

[55] https://www.eumetsat.int/sentinel-3-ground-segment [Accessed 31-01-2023] ; https://sentinels.copernicus.eu/web/sentinel/missions/sentinel-3/ground-segment [Accessed 30-01-2022]; https://www.copernicus.eu/sites/default/files/Copernicus_DIAS_Factsheet_June2018.pdf [accessed 30-01-2022]

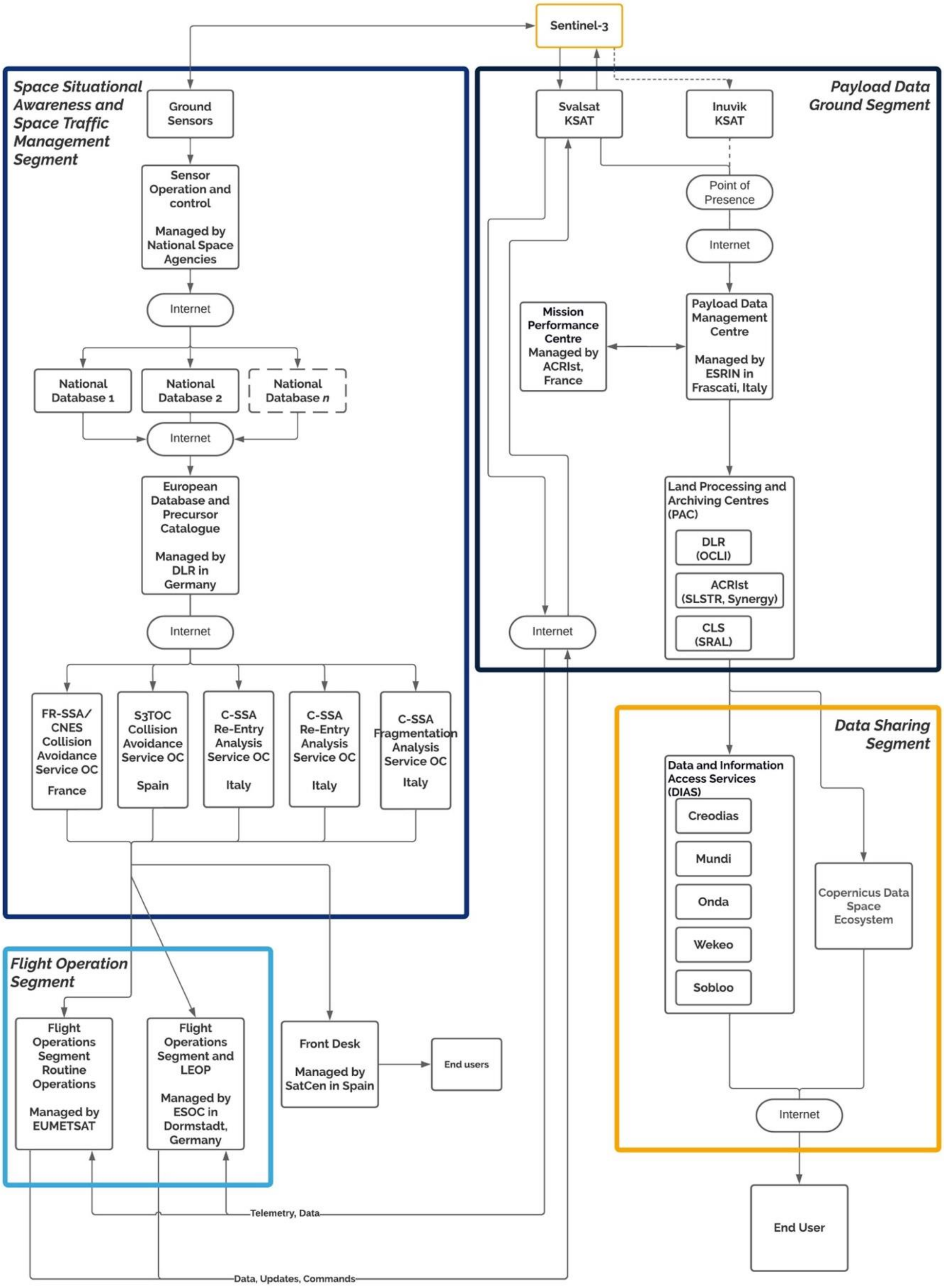
Sentinel-3
Space Situational Awareness and Space Traffic Management Segment
Ground Sensors
Sensor Operation and control
Managed by National Space Agencies
Internet
National Database 1
National Database 2
National Database n
Internet
European Database and Precursor Catalogue
Managed by DLR in Germany
Internet
FR-SSA/ CNES Collision Avoidance Service OC
France
S3TOC Collision Avoidance Service OC
Spain
C-SSA Re-Entry Analysis Service OC
Italy
C-SSA Re-Entry Analysis Service OC
Italy
C-SSA Fragmentation Analysis Service OC
Italy
Payload Data Ground Segment
Svalsat KSAT
Inuvik KSAT
Point of Presence
Internet
Mission Performance Centre
Managed by ACRIst, France
Payload Data Management Centre
Managed by ESRIN in Frascati, Italy
Land Processing and Archiving Centres (PAC)
DLR (OCLI)
ACRIst (SLSTR, Synergy)
CLS (SRAL)
Internet
Data Sharing Segment
Data and Information Access Services (DIAS)
Creodias
Mundi
Onda
Wekeo
Sobloo
Copernicus Data Space Ecosystem
Internet
End User
Flight Operation Segment
Flight Operations Segment Routine Operations
Managed by EUMETSAT
Flight Operations Segment and LEOP
Managed by ESOC in Dormstadt, Germany
Front Desk
Managed by SatCen in Spain
End users
Telemetry, Data
Data, Updates, Commands

Figure 1: Copernicus's architecture

Cyberwarfare from the Ground to Space

The examples of cyberwarfare events in Ukraine in the last years strongly connect with the presented Copernicus architecture. The attacks experienced by Ukraine explicitly aimed at destroying critical infrastructure by disabling entire systems or taking control of terminals to damage almost irreparable portions of the target affected. This has been possible mainly through the spread of wiper malware and ransomware. Attacks have also aimed at data exfiltration and data corruption, both for tactical purposes and propaganda objectives in the context of information manipulation and interference.[56] This is a wake-up call for the European space infrastructure, whose "critical" nature is increasing day by day. The techniques and cyber vulnerabilities described are, in fact, largely applicable to all segments of a space mission.

As in the case of the attack on KA-SAT, gaining access to the ground segment of a satellite network serves the purpose of distributing malware to achieve a permanent denial of service in the user segment. The ability of the Russian Federation to gain minimal control of the satellite, in contrast, could also have been used to physically destroy the asset or disable it, compromising some of its subsystems. Russian hackers gained access to KA-SAT through an infiltration into the ground segment; such action could be carried out through a direct attack on the space segment using ground stations or routing disruption. Infiltrating a ground system or database can also be used to alter and compromise the data stored there. For example, the targeted database could be the one of the EUSST. Altering, deleting, or injecting data in the catalogue of orbiting objects could have catastrophic consequences for active satellites that would be prone to collisions or Rendezvous and Proximity Operations (RPOs), or a possible opponent could "hide" its own spacecraft.[57]

Each node of the architecture presented above is potentially a target of a cyberattack with characteristics in common with those experienced by Ukraine in the last years and months.

An attacker could gain access to the Flight Operation Segment and the Payload Data Ground Segment of a Sentinel spacecraft to hijack control of the satellite with consequences, as mentioned earlier, for the space segment. Likewise, the Payload Data Ground Segment is also a good entry point for the Data Sharing Segment, which is crucial for the exfiltration or injection of data. DDoS attacks on a single segment could lead to a denial of service of Copernicus' mission.

As previously explained, also several nodes of the Space Situational Awareness managed by the EUSST are a potential entry point for an attacker aiming to deliver wrong alerts to an end user or alter the data contained in the European Database and the Precursor Catalogue managed by DLR.[58]

Most of these nodes use ICS and IT elements similar or identical to the ones targeted by Russia in Ukraine. In addition, the link between many nodes is internet-based, reducing the system's resilience in case of attacks on the communication infrastructure of the continent. For example, in the absence of satellite backup communications, an attack on the seabed optic fibre cables connecting the Svalbard Islands to the main continent would ultimately cut out the Svalsat ground station from the rest of the architecture.[59]

[56] Serpanos, Dimitrios, and Theodoros Komninos. "The cyberwarfare in Ukraine." Computer 55, no. 7 (2022): 88-91.
[57] Pavur, James, and Ivan Martinovic. "On Detecting Deception in Space Situational Awareness." In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, pp. 280-291. 2021.
[58] Faucher, Pascal, Regina Peldszus, and Amélie Gravier. "Operational space surveillance and tracking in Europe." Journal of Space Safety Engineering 7, no. 3 (2020): 420-425.
[59] Boschetti, Nicolò, Nathaniel Gordon, Johan Sigholm, and Gregory Falco. "Commercial Space Risk Framework Assessing the Satellite Ground Station Security Landscape for NATO in the Arctic and High North." In MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), pp. 679-686. IEEE, 2022.

Lastly, the aspect of long-distance connections between different nodes also poses a geographical dispersion threat. When the nodes of a space operation are geographically dispersed, maintaining reliable and resilient communication becomes more complex. It can lead to more significant issues, such as signal interference or other technical problems that can disrupt the mission's success.

Another significant risk of geographical dispersion is the increased complexity of managing and securing each facility. Every node in a space architecture is essential, and any failure can cause severe damage to the entire mission. Therefore, ensuring the security of every node in the chain is crucial against sabotage and industrial espionage. However, cultural differences between the nodes can further complicate this security control.[60] For instance, different nations have different security standards and protocols, making it challenging to ensure that every facility meets the same security standards even when coordinated through supranational agencies.

Moreover, the geographical dispersion of a space architecture on the ground can also increase external dependencies, making the architecture vulnerable in the long term. For instance, countries often encourage foreign investment in their economy by creating favourable conditions for foreign companies to open factories or production facilities. However, these conditions can change over time, depending on that country's economic or political performance, dramatically impacting the supply chain's resilience. Thus, this variable must be considered when analysing the security of the European space sector in the long term.

Key Elements for the Future Security of European Space Infrastructure

The analysis of cyberwarfare techniques adopted in Ukraine illustrates that some key aspects must be considered to enhance the security and resilience of European space assets.

Firstly, a more robust control framework for their cybersecurity levels must be enacted in such a complex hierarchy of management entities and suppliers. The Regulation (EU) 2021/696 established the EUSPA's Security Accreditation Board which also operates on cybersecurity. The individual Member States shall provide this body with details of their security measures which are subsequently approved. The security of Galileo is managed separately by EUSPA's Galileo Security Monitoring Centre. None of these bodies operates exclusively on cybersecurity, and the feasibility, in this framework, of analysing in depth the risks arising from the growing integration, at the national and EU levels, with private operators should be investigated.

Furthermore, the security techniques and protocols should be frequently checked and updated, as well as the technical equipment of the different third-party suppliers of services. As previously described, stakeholders in the European private space sector are using ICS components with recognised vulnerabilities that could open the door to attackers.

Mainly focusing on the PNT sector, but with cascading effects on all the others, the spotlight on updates and the supply chain aims at a more robust and diversified GNSS security ecosystem. Efficient management and updating of encryption and authentication methods must be a priority for EUSPA, especially considering the increasing number of spoofing incidents on GNSS signals in Ukraine, the Black Sea, the Baltic Sea, and Norway.

Thirdly, the European space activities governance model should be reformed and simplified. Simplification does not necessarily mean a reduced number of stakeholders involved but could

[60] Falco, Gregory, and Nicolo Boschetti. "A security risk taxonomy for commercial space missions." In ASCEND 2021, p. 4241. 2021.

entail, for example, unified management of the third-party supply chain. This is crucial for the prevention and response to an attack. The dispersed geographic locations of the organisations, coupled with heterogeneous stakeholders, further complicate coordination efforts during an attack.

Lastly, assuming that IRIS^2 and the European Quantum Communication Infrastructure development will follow rigorous cybersecurity protocols, they should become a crucial component of inter-agency and inter-infrastructure communications to overcome risks related to the heterogeneity of Internet Service Providers (ISPs) and legacy IT infrastructure whose fragility has been highlighted by the Ukrainian conflict.

GOVERNANCE

Beyond technical aspects, a lack of proper governance can also contribute to the development of cyber vulnerabilities in space systems, including those employed for military operations. In this context, the integration of cyber issues into the organisational and policy frameworks governing military space activities appears crucial. The following Chapters analyse the integration of cybersecurity requirements in military space activities in France, Italy and the United Kingdom.

THE FRENCH APPROACH TO SPACE CYBERSECURITY

Paul Wohrer, Researcher, Foundation for Strategic Research[61]

Xavier Pasco, Director, Foundation for Strategic Research

Cybersecurity has become one of the most pressing issues for space security. The 2019 French Space Defence Strategy identifies cyber threats as the most common type of attack on space systems, with a high destructive potential, while attribution remains difficult and politically risky. The current dynamics of space developments favour a greater use of software-defined payloads and digitalised ground segments, increasing the potential for cyberattacks. This article will provide a synthesis of the French approach to cyber defence, which is not specific to space activities. It then examines the French cyber infrastructure, which includes a number of institutions responsible for ensuring the security of space systems. The paper concludes with an overview of the ongoing changes in the space domain and its implications for the future of the French approach to space security.

The growing cyber threat in space

Cyber threats now exist in all sectors. Space used to be characterised by its relative isolation from such threats. Accessing space systems used to be very difficult from a hardware, software, and networking perspective. Previously, ground stations were not connected to the internet. Satellites launched before 2020 were generally equipped with outdated technologies[62]. Some of them have little or no protection of their telecontrol channel, while they also used bespoke components.

On the one hand, this makes them less vulnerable to backdoors and malware than traditional components. The software suite of "old space" systems generally consists of many hardware and passive components (diodes, resistors), non-reprogrammable integrated circuits and non-rewritable memories containing flight and emergency software. This increases the overall reliability of the system. On the other hand, it also makes it impossible to issue patches to correct vulnerabilities, a common practice in the software industry. Additionally, unprotected telecommunication links, overexposing such systems to malevolent actions, have remained a key security issue.

The space supply chain also used to be highly specialised and closed, as most space companies were defence companies. Combined with the very limited number of satellites produced, which provided little financial incentive for hackers to develop specific malware, this explains why satellites were once considered beyond the reach of most cyber threats. This “security by obscurity” also helps to understand the current state of cybersecurity for space systems, sometimes described as "dismal"[63].

It is however important to distinguish between satellites and space systems. While common sense dictates that cyberattacks on space systems would target satellites, such instances are rare. In fact, satellites are only one part of a space system, which also includes the ground segment and the user segment, both of which are located on the surface of the earth. The ground segment includes all the infrastructure used to control satellites, such as telecontrol and telemetry (TC/TM) signals

[61] Since June 2023, the author has been Research Fellow on Space at the French Institute for International Relations (Ifri)
[62] Airbus presentation, 2023
[63] Secure World Foundation, 2022, “Global Counterspace Capabilities, an open source assessment”, p. 13-07

and teleports for data transmission and reception. The user segment consists of thousands, sometimes tens of thousands, of user terminals that allow customers to use the services provided by the satellite[64].

Recent cyberattacks against space systems include the 2022 Russian attack against the Viasat network[65]. The target of this attack were modems for internet access to citizens and equipment in the energy sector. The attack used a wiper malware called "AcidRain", designed to erase data on board routers and modems. This rendered them unusable and potentially destroyed them. The attack was part of a wider aggression against Ukraine in February 2022, but it had a knock-on effect on European infrastructure, affecting tens of thousands of customers across the continent. It was attributed to Russia by the European Union and Five Eyes governments[66]. Another recent attack on the space infrastructure was attributed to Fancy Bear, a group of Russian hackers also known as APT28. While details of the attack are scarce, researchers at the Cybersecurity and Infrastructure Security Agency (CISA) indicated that the attack was carried out on the ground segment of a satellite operator providing services to U.S. critical infrastructure[67].

A common feature of these attacks is their focus on the terrestrial part of space systems: the Viasat attack targeted the user segment, while the Fancy Bear attack targeted the ground segment. In both cases, the satellite segment of the space system was unaffected.

These types of attacks are much more common than direct actions against satellites for several reasons. Firstly, physical access to satellites after launch is impossible. The only reasonable way to attack a satellite in orbit is to combine a cyberattack with a sophisticated electronic attack. This would however require a combination of skills that may limit most hackers' capacity to act in an efficient way. On the other hand, since satellites are controlled from ground stations, attacking these can be more effective than targeting satellites themselves. Targeting the ground station may be considered easier and cheaper for the attacker and grant them control of the satellite if successful. Such events have officially never happened[68], and ground stations use ever more elaborated protection techniques (such as sophisticated firewalls, VPNs, etc.) that may render such attacks more complex than generally perceived. Attacks on the user segment are the least complex, given that satellite terminals such as modems and routers are generally more accessible and less protected than satellite ground stations.

[64] The Aerospace Corporation, 2022, « Protecting Space Systems from Cyber Attack", https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368

[65] Laetitia Cesari Zarkan, 2023, "Commercial Space Operators on the Digital Battlefield", Centre for International Governance Innovation, https://www.cigionline.org/articles/commercial-space-operators-on-the-digital-battlefield/?utm_source=twitter&utm_medium=social&utm_campaign=cybersecurity-outer-space-series

[66] Cyberpeace Institute, 2022, "Case Study: Viasat", Cyberconflict website, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

[67] Christian Vasquez, 2022, "CISA researchers: Russia's Fancy Bear infiltrated US satellite network", Cyberscoop, https://cyberscoop.com/apt28-fancy-bear-satellite/#:~:text=Researchers%20at%20the%20Cybersecurity%20and,the%20rapidly%20expanding%20space%20economy

[68] Attacks in the past may have resulted in taking control of satellites, but no command was sent to the satellite. For a more detailed account of past events, see Secure World Foundation, op. cit., p. 13-04

The French cyber defence architecture

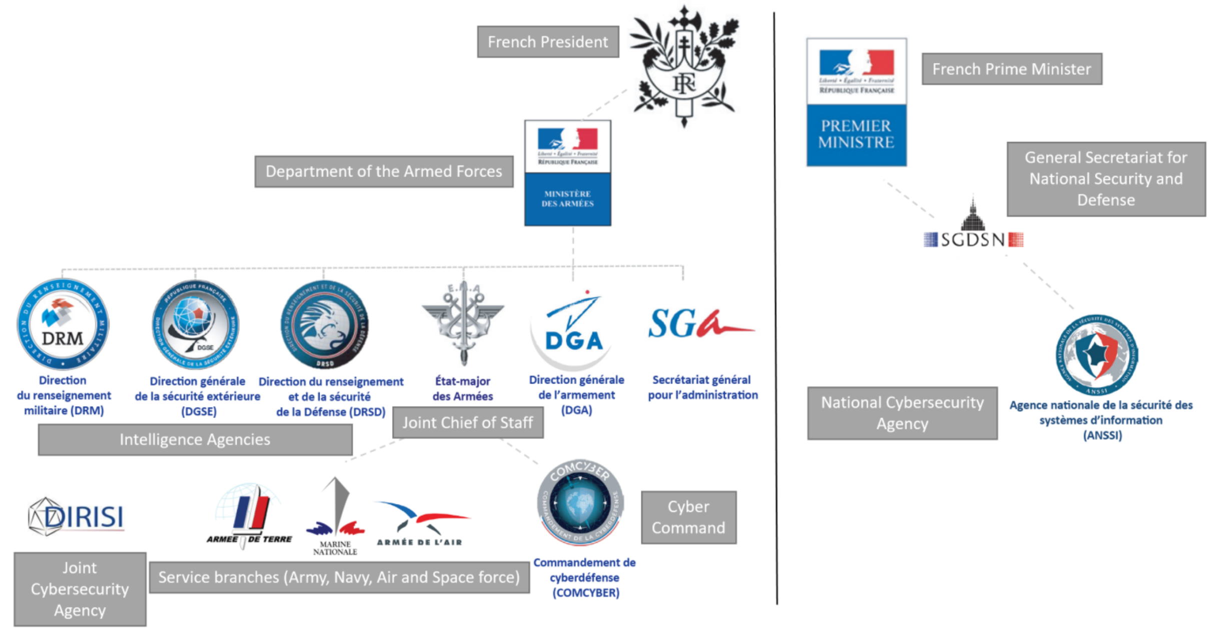
French President
Department of the Armed Forces
MINISTÈRE DES ARMÉES
French Prime Minister
PREMIER MINISTRE
General Secretariat for National Security and Defense
SGDSN
DRM
Direction du renseignement militaire (DRM)
Direction générale de la sécurité extérieure (DGSE)
Direction du renseignement et de la sécurité de la Défense (DRSD)
État-major des Armées
DGA
Direction générale de l'armement (DGA)
SGA
Secrétariat général pour l'administration
Intelligence Agencies
Joint Chief of Staff
National Cybersecurity Agency
Agence nationale de la sécurité des systèmes d'information (ANSSI)
DIRISI
Joint Cybersecurity Agency
ARMEE DE TERRE
MARINE NATIONALE
ARMÉE DE L'AIR
Service branches (Army, Navy, Air and Space force)
COMCYBER
Commandement de cyberdéfense (COMCYBER)
Cyber Command

Figure 2. Simplified organizational chart of French cyber defence architecture[69]

The French cyber defence doctrine allows for different types of operations in the cyber domain. While some elements remain classified, French institutions are officially able to conduct defensive cyberwarfare operations, offensive cyberwarfare operations and cyberwarfare for influence purposes[70]. France recognises the application of international law in both space and cyberspace. In the case of cyberattacks, any attack that causes significant damage can be considered an armed aggression[71]. Armed aggression would lead France to exercise its right of self-defence in both cases.

The French model differs from the British and American models, where all defensive and offensive cyber operations are carried out by intelligence agencies (National Security Agency in the United States, Government Communications Headquarters in the United Kingdom)[72]. France has a system of strict separation between defensive actions (protection and network security) and offensive actions (intelligence and offensive operations)[73], which are conducted by different entities. This approach relies mainly on four institutions, both civilian and military. They form the "first circle" of French cyber defence.

The French National Cybersecurity Agency (ANSSI) is the main civilian agency in charge of cybersecurity in France. It reports to the Secretariat-General for National Defence and Security (SGDSN), which in turn reports directly to the Prime Minister. Its missions include cyber protection and defensive computer warfare. It is tasked with protecting the State's institutions, the so-called

[69] This organizational chart is based on Martial Le Guédard, 2020, « Gestion de crise et chaînes cyber : synthèse de l'organisation européenne et française liée à la sécurité numérique », INHESJ

[70] Ministère des armées, 2023, « La cyberdéfense au ministère des armées », https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees

[71] « Significant damages » are never defined. This discourages adversaries to launch attacks, since they do not know when they would cross the threshold to trigger a response.

[72] SGDSN, 2018, "Revue Stratégique de cyberdéfense" p.45, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

[73] Aude Géry, 2020, "La stratégie française de cyberdéfense", Brennus 4.0, p.2, https://www.penseemiliterre.fr/ressources/30147/14/la_strategie_francaise_de_cyberdefense.pdf

"Vitally Important Operators" and those providing essential services, which includes space among other domains[74]. ANSSI is the cornerstone of French cyber defence and, since its creation in 2013, has coordinated France's strategy in this field. It has a regulatory role: it sets cybersecurity standards for Vitally Important Operators and ensures the certification and qualification of their information systems. It is empowered to impose certain measures on these operators if a major crisis occurs. The coordination of ANSSI actions requires the contribution of the Ministries of Home Affairs, of Justice, and of Europe and External Relations, making the system entirely inter-ministerial. ANSSI also advises the government, informing it of potential threats to guide French policy[75]. In space, ANSSI has publicised its involvement in securing the European Union's Galileo GNSS programme. Specifically, it contributed (together with other European agencies) to the validation of security equipment, audited critical infrastructure and secured the programme's information systems[76].

Defending the information systems of the Ministry of the Armed Forces is the responsibility of the French Cyber Command (COMCYBER). ANSSI has delegated this responsibility to COMCYBER because of the specific nature of the armed forces' information systems. COMCYBER can carry out cyber operations including defensive computer warfare. Furthermore, COMCYBER may conduct offensive computer warfare, but only within the framework of military operations[77]. By combining defensive and offensive capabilities, COMCYBER is an exception to the general philosophy of the French system, but only in a very specific and limited field. COMCYBER was created based on two considerations: the need to place cyber defence under the responsibility of the French Joint Chiefs of Staff (CEMA) and the need to integrate cyberspace into all military operations. COMCYBER has publicly declared its interest in space cybersecurity and has started efforts of coordination with the newly created French Space Command to study this issue[78].

The Joint Directorate of Infrastructure Networks and Information Systems (DIRISI) is a joint agency responsible for the security of telecommunication networks and information systems within the Ministry of the Armed Forces. In particular, it is responsible for ensuring the security of the Syracuse military satellite communication systems. A specific cyber centre is also operated by each branch of the armed forces (navy, army and air and space force). In addition, a dedicated agency, the Defence Intelligence and Security Directorate (DRSD), is responsible for specific cyber counterintelligence operations within the Ministry of the Armed Forces[79].

Other agencies involved in French cyber defence are the Directorate General for External Security (DGSE) and the Directorate General for Internal Security (DGSI), both of which are intelligence agencies in charge of external and internal security respectively[80]. The French police, gendarmerie, customs and judiciary are also involved in conducting cyber-related investigations and can conduct operations whenever hackers from the civil society are identified[81].

[74] Vitally Important Operators are companies or institutions participating in activities considered vital for French sovereignty, French economy, Defence or Security. These activities are difficult to substitute or replace. They include operators in various sectors such as food, water and energy distribution, energy, transport, electronic communications and space. There are fewer than 350 Vitally Important Operators in France, and their list is classified for security reasons. For more information, see SGDSN, 2016, "la sécurité des activités d'importance vitale": http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

[75] Commission de la défense nationale et des forces armées, 2018, "Rapport d'information sur la cyberdéfense " , Assemblée Nationale, p.41

[76] ANSSI, 2017, "Avec le programme Galileo, l'ANSSI agit aussi dans l'espace", https://www.ssi.gouv.fr/actualite/avec-le-programme-galileo-lanssi-agit-aussi-dans-lespace/

[77] Ministère des Armées, « Le commandement de la cyberdéfense », https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber

[78] Riskintel Media Youtube channel, 2022, « La cyberguerre des étoiles »

[79] Commission de la défense nationale et des forces armées, op.cit, p. 45

[80] Their role in space cybersecurity is unclear.

[81] Commission de la défense nationale et des forces armées, op.cit, p. 39

The aforementioned organisations are the main cyber defence institutions of France[82]. Also fundamental to space cybersecurity is the role of CNES, the French space agency. CNES applies the most stringent cybersecurity measures to ensure the integrity, authentication and security of space system data, as it manages space launches and satellite operations, both for civilian purposes and for the French armed forces. CNES also conducts research on space cybersecurity. Since 2016, CNES has created a collaborative group aimed at better understanding cyber threats to the space sector and identifying appropriate responses: the Comet-CYB[83]. The main mission of COMET groups is to organise communities to foster expertise, innovative ideas, and interdisciplinary sharing. The cyber community focuses on cybersecurity for space missions. Its role aims at formalising and reducing the complexity and heterogeneity of organisational and technical approaches in information systems (IS), analysing and understanding threats to facilitate their detection and reaction, making operational and enterprise information systems more reliable and secure, improving protection mechanisms and procedures. They also aim at understanding the state of the art for research actions in Information Systems Security, promoting the integration of security in space missions and analysing the constraints and opportunities of the regulations in cybersecurity.

As shown above, the French cybersecurity architecture does not display any significant dedicated organisational apparatus to deal with space-directed cyber threats. The choice has been to address such threats as for any other sector. The French approach towards space cybersecurity could be summarised as such: space cyber is just cyber. Then a question arises: how long can this approach remain effective in the face of a rapidly changing space world, especially with the current New Space environment?

The changing space landscape and the stakes of future cybersecurity

The French Space Defence Strategy has described the rise of cyber threats in the space domain: "Cyberattacks on the software parts of the different segments of space capability are among the most likely threats, though they require precise knowledge of the target's technical parameters. Difficult to attribute, they may have reversible or irreversible effects including, at the most serious end of the scale, loss of control of payloads or even the platform itself, reducing it to junk"[84].

Cyber threats to space systems are therefore serious. However, the space domain is not exceptional in this respect. General Thierry Blanc, deputy commander of the French Space Command, explained that while satellites tend to attract attention, the user segment of space systems is often much less secure than the space segment, making it an easier target for cyberattacks[85]. Although cyberattacks on satellites have the potential to seriously disrupt military and civilian operations, they have continued to prove rather speculative for the most part until today. In 2021, a French team, Solarwine, was a finalist in the Hack-a-sat challenge organised by the U.S. Air Force. Only one member of the team was a space specialist, reinforcing the point that cybersecurity does not differ

[82] For a more complete map of cybersecurity institutions, please see Martial le Guédard, 2020, "Gestion de crise et chaînes cyber: synthèse de l'organisation européenne et française liée à la sécurité numérique": https://www.ihemi.fr/sites/default/files/inline-files/Gestion%20de%20crise%20et%20cha%C3%AEnes%20cyber%20-%20INHESJ%20-%20juillet%202020%20-%20Martial%20Le%20Gu%C3%A9dard%20-%20MAJ15juil%281%29.pdf
[83] Comet-CYB website, 2023, Centre National d'Etudes Spatiales, https://www.comet-cnes.fr/cyb
[84] French Ministry of the Armed Forces, 2019, "Space Defense Strategy", p.23
[85] Riskintel Media, "La cyberguerre des étoiles", Youtube interview, https://www.youtube.com/watch?v=_MhRgWUebiw

between space and non-space systems[86], somewhat highlighting the main characteristics of the French cyber defence organisation as already noted.

According to General Michel Friedling, former head of the French Space Command, the French space security architecture consists of three concentric circles. These include a "sovereign core" of sovereign satellites and space systems, an "extended core" involving partnerships with foreign actors, and "complementary capabilities" of commercial service providers. Cyber threats are likely to have very different impacts on these three circles, and cyber and space institutions will have to work together to ensure a higher level of security. The first two circles are considered crucial to ensure the success of military operations. Because of their military nature, the sovereign and extended core space capabilities are generally considered to be highly secure. Their command and control centres are managed by public institutions and their data links are highly encrypted. It seems very unlikely that a cyberattack on these capabilities would be successful.

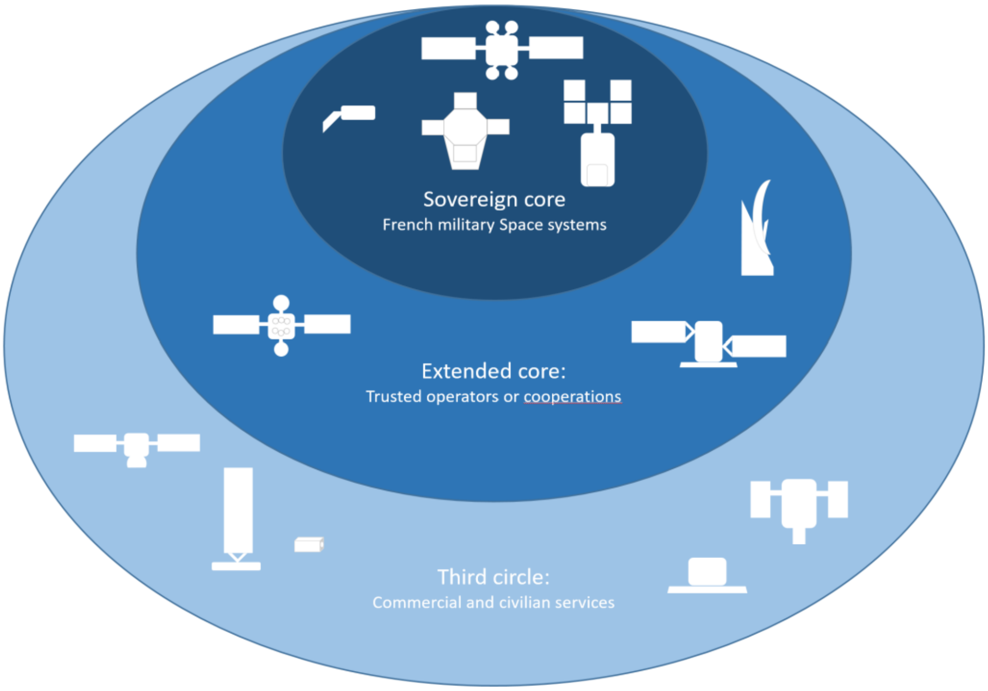
Sovereign core
French military Space systems
Extended core:
Trusted operators or cooperations
Third circle:
Commercial and civilian services

Figure 3. Chart of the three circles of space sovereignty, as envisioned by General Michel Friedling, former head of French Space Command

However, in order to conduct effective military operations, the French armed forces are increasingly relying on partnerships with commercial providers. As the economic models of commercial space providers evolve, they are becoming more exposed to increasingly sophisticated cyberattacks.

Using more software and less hardware to accomplish the same task is the general approach for New Space systems. Open-source software, such as the LINUX operating system, are now widely used by New Space companies[87]. As software is responsible for more critical tasks, there is a greater attack surface and increased vulnerability. Software security testing, vendor reliability, and frequent software patching would allow for better security. However, New Space actors are generally not in a position to spend as much on security as traditional space actors.

[86] Aris Ada, 2022, "Cysat2021 Solarwine interview: the Hack-a-sat competition", Youtube: https://www.youtube.com/watch?v=hiK82ZQDW7s

[87] Leppinen, Hannu, 2017 "Current use of linux in spacecraft flight software" IEEE Aerospace and Electronic Systems Magazine. 32. 4-13. 10.1109/MAES.2017.160182.

Also, these systems often use commercial off-the-shelf (COTS) components[88]. Their integrated circuits (so-called FPGAs) are usually reprogrammable, even in flight. They require frequent updates, which can be vehicles for computer viruses or new vulnerabilities, even if these updates are usually carried out by the manufacturers themselves that actually limit those risks. Mass production of satellite components is often required as these companies aim to deploy constellations of hundreds or thousands of satellites in low Earth orbit. With many different suppliers and an increasing number of developers, the New Space ecosystem is generally more open than traditional defence suppliers[89]. These trends increase the risk of supply chain attacks from both a component and software perspective. In addition, the security of the supply chain is under increasing pressure. This is due to the fact that satellites are nowadays more often produced in constellations, which entails the use of more and more components that may be exposed to malicious attacks. As the number of standardised satellites increases, they also become more tempting targets for a potential attacker, since the investment needed to design an attack can be scaled on more targets[90]. This is particularly important since cyberattacks appear to be the only practical way to damage interconnected systems such as satellite constellations.

The development of connectivity also means that ground stations or command and control centres are no longer completely isolated from the Internet. While fully part of a space system, attacks on ground segments are however not fundamentally different for space and non-space infrastructure and require the same cybersecurity measures.

For now, France's approach to space security appears adequate. It treats cybersecurity as an all-encompassing and transversal mission for all domains, including space, and does not distinguish between space and non-space cybersecurity. The use of less secure New Space services is, for the time being, confined to the third circle of sovereignty, meaning their use would not be crucial in times of crisis. However, the increasing value of these systems for military actors, as demonstrated by the war in Ukraine, may raise new challenges to ensure the safety and resilience of space services. The current French architecture may remain relevant in the future, however cybersecurity should be enhanced through better information and oversight as new space systems evolve and cyber threats become more sophisticated. The French government plans to improve French cybersecurity by dedicating more than €1 billion to accelerate efforts in by 2030. Given the importance of space services to the armed forces and society as a whole, it would be advisable to dedicate a part of this effort to improve space cyber security. This effort could provide information on the specificities of the space sector with regards to cyber threats, including for instance the growing threat of combined electronic warfare and cyberattacks against satellites.

For France, as for any other major space power, the use of commercial space has become a necessity. However, the cyber vulnerabilities of this sector are clearly evident. To prevent such risks, the regular use of these capabilities will require a sufficiently robust upstream adaptation including, but not limited to, New Space companies. This is one of the paradoxes of today's inescapable convergence of hitherto protected space technologies and an information world that poses new dangers.

[88] Mathieu Bailly, 2021, "Newspace: les enjeux liés à la sécurité des données", CYSEC presentation, https://www.comet-cnes.fr/sites/default/files/ressources/COMET%20cyber_Mathieu%20Bailly_Newspace.pdf

[89] For example, the Falcon 9 launcher's internal systems

[90] This fact was pointed out by Therry Blanc during a public discussion between French Cyber and French Space Commands. Riskintel Media, op.cit.

THE ITALIAN APPROACH FACING THE EVOLVING CYBER THREAT TO SPACE SYSTEMS

Giancarlo La Rocca, Resident Fellow Defence and Security, Istituto Affari Internazionali (IAI)[91]

The relevance of the space-cyber nexus in Italy

In recent years, Italy boosted its attention and efforts devoted to space, updating the policy and governance framework and adapting the institutional structures to the recognition of space as an operational domain. The same has happened with the cyber dimension, together with increasing awareness on the interdependence between the two domains. The National Recovery and Resilience Plan (NRRP) devotes large investments to both sectors, €2 billion for space and no less than €630 million to cyber.

The Russian invasion of Ukraine notably revealed the proximity between the space and cyber threats, ringing alarm bells on the protection of space systems from orbit to the ground. Indeed, according to the Minister in charge of space affairs Adolfo Urso, the ongoing conflict in Ukraine has demonstrated how the space and cyber domains are interconnected.[92] Besides, the firm support to Kyiv has brought a general increase in the number of cyberattacks against Rome and put the cyber governance in turmoil with the resignation of the Head of the Agency for National Cybersecurity (ACN).[93] Moreover, in the annual report to the Parliament, the national intelligence addressed the cyber threat mentioning also the specific vulnerabilities of the aerospace value chain.[94] The constant sharpening of the cyber threat is also widening the area where the two domains are connected, expanding the overall surfaces and entry points to conduct attacks on space systems. For instance, the development of easily accessible Electronic Warfare (EW) instruments adds another layer of complexity, in particular when the three dimensions of space, cyber and EW converge in the emergence of new threats, a situation that could be potentially exploited to hit space systems.[95]

Italy is the third largest investor in ESA and the second state in Europe for the number of assets in space. This number is projected to increase as the national space programme envisions a forthcoming small constellation for Earth observation in low Earth orbit together with a fleet of 20 minisatellites with diverse scopes and applications.[96] Moreover, the Italian space value chain is extensively involved in the whole European industry, and a pillar of the EU Space Programme's manufacturing power, especially since the integration of national champions with French players in the Space Alliance. Italian presence is also tangible in the wider Middle East and North Africa as well as North America markets. As a result, analysing the Italian approach to space and cybersecurity is relevant for Rome's national interests.

[91] Since 1st May 2023, the author has been a Researcher in the Directorate for International Affairs of the Italian Space Agency

[92] Credi, Ottavia, Giancarlo La Rocca, and Alessandro Marrone. "Il dominio spaziale e la minaccia cyber." In Documenti IAI (March 2023). Istituto Affari Internazionali.

[93] Interview, February 2023

[94] Relazione al Parlamento 2022 - Sistema di informazione per la sicurezza della Repubblica (sicurezzanazionale.gov.it)

[95] Credi, Ottavia, Giancarlo La Rocca, and Alessandro Marrone. "Il dominio spaziale e la minaccia cyber." In Documenti IAI (March 2023). Istituto Affari Internazionali. (To be published)

[96] "IRIDE: Firmati i Contratti." Agenzia Spaziale Italiana. December 5, 2022. https://www.asi.it/2022/12/iride-firmati-i-contratti/; "Smalsat Revolution: le 20 Missioni di Alcor, il Cavaliere dello Spazio." Spaceconomy 360. https://www.spaceconomy360.it/missioni-spaziali/smalsat-revolution-le-20-missioni-di-alcor-il-cavaliere-dello-spazio/

The 2022 Italian Chief of Defence Strategic Concept recognises the breaking point marked by the Russian invasion of Ukraine, a "harsh realisation of the danger of the so-called hybrid war […] bringing together the classical domains (land, air, naval) with the cyber and space domains and the cognitive environment as a whole".[97] It also acknowledges that the increasing competition in space and cyberspace sharply broadens the threats to national security. As a consequence, the Italian Defence community should be part of the industrial initiatives and technological revolution, with a specific focus on space and cyber, where military equipment needs a "profound upgrade" due to the role of these domains as "fundamental enablers for all operations". The upgrade is also dependent upon human capital, which needs to be specifically trained and attracted to defence institutions. This is partially reflected in a recent call for armed forces officials to enter the space and cyber domains within the Army and Navy commands [98], or in initiatives for cooperation with universities. [99]

The attention devoted to the interconnected nature of space and cyber resonates within the overall goals of the 2022 Concept, focused on seeking the best synergies between the National Cybersecurity Agency (ACN), the Inter-ministerial Committee for Space Policy and Aerospace Research (COMINT), the Office for Space and Aerospace Policy of the Presidency of the Council of Ministers, and the Civil Protection Department.

Yet, how are the two domains governed? What degree of cross-awareness and fertilisation exists between the sectors? How does the cyber threat fit within the Italian space approach and shape it at European level? Is the ongoing conflict in Ukraine affecting the overall approach? This paper aims to outline the Italian framework and overall approaches to space and the cyber threat, through open-source documents and tailored interviews with experts and officials. The paper first provides a landscape of the policy elements and considers the involved actors, in particular presenting the civil and defence approaches and the transformation that occurred in recent years. Then, it discusses the posture towards the cyber threat in the space domain and the national posture as expressed at European level.

Governance and policy of the space-cyber nexus

Over the last five years, Italy has endeavoured to reform and update its posture in space and cyber, transforming the governance of each sector to adopt a top-down approach, a development coherent with EU and NATO initiatives and declarations.

[97] Italy. Stato Maggiore della Difesa. "Chief of Defence Strategic Concept 2022." https://www.difesa.it/SMD_/CaSMD/Concettro_strategico_del_Capo_di_SMD/Documents/CS_22/Chief_of_Defence_Strategic_Concept_2022_.pdf.

[98] "Concorsi Ufficiali Forze Armate Cyber e Spazio." Ministero della Difesa. https://www.difesa.it/SMD_/Concorsi_Ufficiali_Forze_Armate_Cyber_e_Spazio/Pagine/default.aspx.

[99] Ministero della Difesa. January 19, 2023. Cyber Security: COR e Università Federico II insieme per i frequentatori dell'Accademia Aeronautica https://www.difesa.it/SMD_/Eventi/Pagine/Cyber_Security_COR_e_Federico_II_insieme_per_Accademia_Aeronautica.aspx

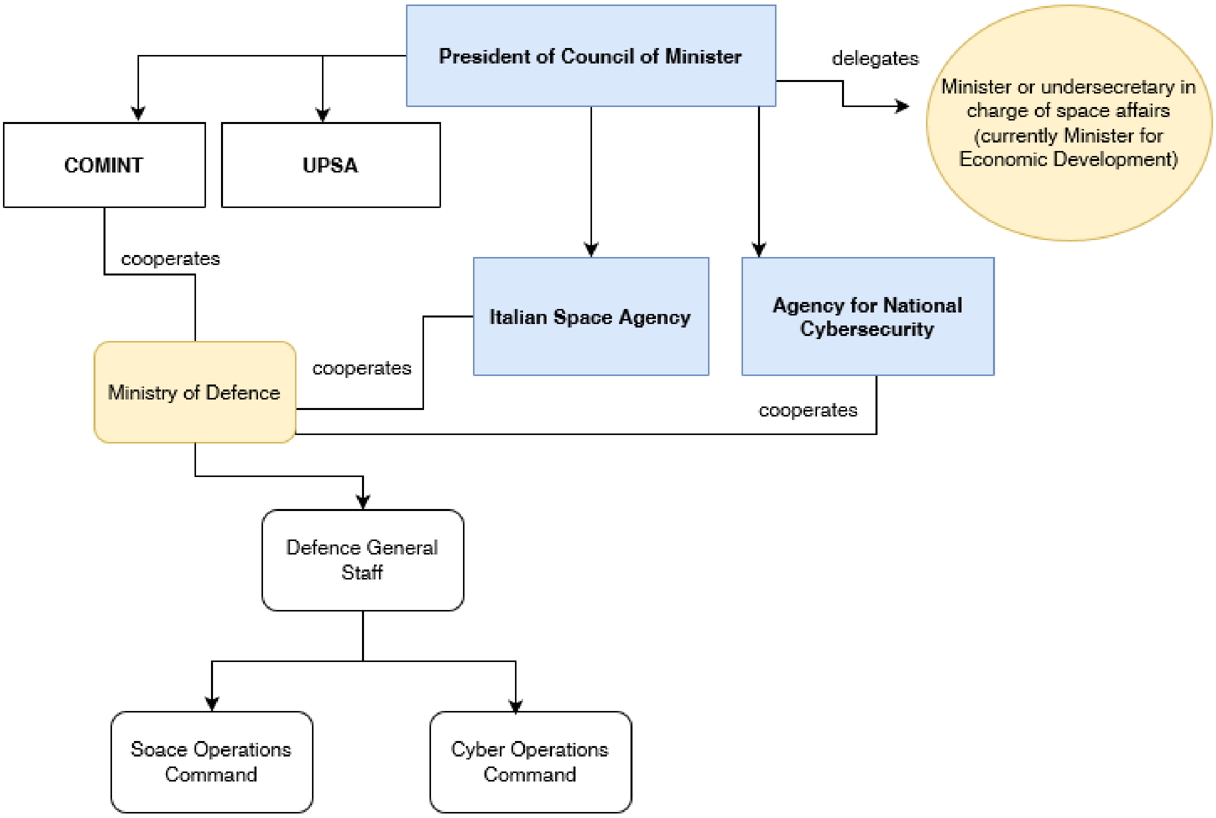
President of Council of Minister
delegates
Minister or undersecretary in charge of space affairs (currently Minister for Economic Development)
COMINT
UPSA
cooperates
Italian Space Agency
Agency for National Cybersecurity
Ministry of Defence
cooperates
cooperates
Defence General Staff
Soace Operations Command
Cyber Operations Command

Figure 4: Governance of space cybersecurity

Space: civil and defence approaches

The primary foundation of the new Italian space governance is the Law n. 7 from 2018, which represents a concrete advancement towards the development of a closer institutional focus on space and the establishment of a systemic approach.[100] This legislation put the space governance at the highest political level within the government, as the Prime Minister assumes the "key management, general political responsibility, and policy coordination" for space. It also creates the COMINT, headed by the Prime Minister or the highest political authority delegated to space affairs by decree. This Inter-ministerial Committee is chaired by the Military Advisor of the Prime Minister and is the body entitled to discuss space affairs with approximately 12 Ministries. It approves strategic documents for the sector, implemented by the Italian Space Agency (ASI).[101]

Through this Law, the governance of the sector has been transformed to promote a whole-of-government approach and to enhance the institutional awareness on the benefits and applications of space. The role of the Italian Space Agency (ASI) was also reformed to bring it closer to the Prime Minister's portfolio of responsibilities and thus give more strategic relevance to the activities once only supervised by the Ministry for Education. A second law was implemented to establish a "Coordination Structure" within the Military Advisor's office to support the COMINT and the implementation of policies at the inter-ministerial level. Yet, the practical application of the Law is contingent upon the political will of the governing parties and might be affected by majority changes. To avoid this unstable outcome, the Draghi government upgraded this political

[100] Italy. "Legge 11 gennaio 2018, n. 7: Misure per il coordinamento della politica spaziale e aerospaziale e disposizioni concernenti l'organizzazione e il funzionamento dell'Agenzia spaziale italiana." Gazzetta Ufficiale, February 10, 2018. https://www.gazzettaufficiale.it/eli/id/2018/2/10/18G00025/sg.
[101] Ibidem

configuration instituting the above-mentioned Office for Space and Aerospace Policy (UPSA), a department for space affairs at the Presidency of the Council of Ministers.

The institutional change stemming from the Law generated significant results in the form of two strategic documents. The first of these are the 2019 "Guidelines on space and aerospace", a government-level publication that centres on space and delineates strategic priorities and the overall security dimension associated with the sector.[102] The high-level document already points to the cyber threat among the intentional ones, which calls for "acquiring an adequate intrinsic resilience".[103] The Guidelines are expected to be updated by the end of 2023, focusing specifically on a set of strategic addresses from the government, due to the changed context compared to only five years ago.[104]

The second outcome of the governance reform is the "National Security Strategy for Space", which concentrates on the protection of space systems and intentional or unintentional threats to bolster the entire sector and its defence capabilities.[105] Interestingly, the commercialisation of space is seen as a factor potentially increasing the concerns about sustainability, safety and security requirements as well as property rights. In this context, the National Security Strategy outlines five objectives with the safety and security of space assets at the core:

a) "to ensure the security of space infrastructures [...], regarded as enablers of the national infrastructure as a whole;
b) to safeguard national security, including through space, by ensuring access to and use of national security capabilities in any given situation;
c) to strengthen and protect the institutional, industrial and scientific sectors, also with a view to protecting national classified information;
d) to promote a space governance capable of ensuring sustainable, safe and secure space operations at international level;
e) to ensure that the development of private initiatives in the space sector (upstream and downstream) is consistent with the country's overriding interests."[106]

The purpose driving the Strategy is clearly to strengthen the resilience of all national assets, public and private, protecting systems against intentional threats, hereby factually including cyber. The robustness of systems and of the national security architecture is considered to be at the core of the strategy together with prevention, deterrence and defence measures. Finally, a critical line of action concerns the protection and supervision of the development of industrial and scientific activities and protection of classified information. This has to do with the absence of a national space law, the development of which is being discussed at present and could be beneficial also to regulate, systematise, and organise the sector. Such an upgrade could also be instrumental to highlight the cyber nexus from a normative approach.[107]

The absence of a comprehensive and holistic space legal framework results in an ambiguous delineation of the roles and responsibilities of defence entities pertaining to activities carried out in the space domain. To some extent, the gap has been filled by the Draghi government Decree n. 50

[102] Italy. Prime Minister's Office. "Government Guidelines on Space and Aerospace." March 25, 2019. https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/DEL_20190325_aerospazio-EN.pdf.
[103] Ibidem
[104] Interview February 2023.
[105] Italy. Prime Minister's Office. "National Security Strategy for Space." July 18, 2019. https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/NationalSecurityStrategySpace.pdf.
[106] Ibid.
[107] La Rocca, Giancarlo, and Alessandro Marrone. "Italy and Space, a Strong Position to Enhance." In The Expanding Nexus between Space and Defence, edited by Alessandro Marrone and Michele Nones, 65. Roma, 22|01.

of 2022, which reforms the military law by introducing space and cyber within the areas of intervention of the military apparatus.[108] This reform thus calls for permanent availability of command-and-control structures to defend the space and cyber domains.

Notably, this piece of legislation comes within a decree on urgent measures spawned from the Ukrainian crisis. It reinforces an idea already put forward in the Multiannual Programmatic Document (DPP) of the Ministry of Defence for the triennium 2021-2023 where space and cyber are singled out as "strategic and cross-cutting enabling domains" with a joint nature.[109] As a matter of fact, both the space and cyber domains are put under the Italian Joint Operations Headquarters (COVI), part of the Defence General Staff (thus not one single military branch), constituted in 2021 as an evolution of the previous inter-army command towards multi-domain operations. Specifically, both the space and cyber operations commands are dependent on COVI.

Coherent with NATO's approach after the 2019 London declaration on space, the Italian defence governance evolved as well, adapting to the reality of the new operational domain. Alongside the implementation of the new overall political governance, a significant restructuring has taken place within the Ministry of Defence. The Italian Defence General Staff first established the General Space Office (UGS) in November 2019, responsible for policy planning, space programmes and international cooperation. Subsequently, in June 2020, the Space Operations Command (COS) was established to develop space operations while continuing to provide space services to the other traditional domains. Therefore, the appointment of COS under the COVI's control is meant to properly account for the conceptualisation of multi-domain operations across land, sea, air, space, and cyberspace.

The establishment of COS is also quite a natural evolution of the military's need to operate its assets effectively and autonomously in the space domain. Notably, UGS and COS have been reflecting on an MoD space strategy, outlined below. Italy, like other NATO countries, recognises space as the high ground where confrontation can increase to achieve competitive advantages. This further calls for updating and upgrading the operational capabilities to protect national assets and ensure freedom of access and manoeuvre in orbit.[110] This represents a significant change, as space is no longer viewed solely as an enabler for defence operations on Earth, but rather as an operational domain in its own right, closely linked to the other domains.

A dedicated Defence Space Strategy has been approved in 2022, without public release. The landmark document interestingly contains strategic actions of implementation, starting from a doctrinal development of space operations intended to define rules of engagement and include the pervasiveness of the cyber domain. At the same time, other domains will have to integrate space into each specific doctrinal approach, to develop support capabilities to space operations conducted by COS, combine the space dimensions into each service and mature the know-how to operate in degraded environments. Indeed, space is considered as an enabler of all the other domains, including cyber, essential as a generator of services ensured by space systems.

Finally, the National Military Policy Directive of 2022 by the defence minister calls for the investment of more resources in the two new domains, especially due to the pace of technological innovation, but also because of the pervasiveness of these environments and the effects of operations for

[108] Italy. Decreto-legge 17 maggio 2022, n. 50. "Misure urgenti in materia di politiche energetiche nazionali, produttività delle imprese e attrazione degli investimenti, nonché in materia di politiche sociali e di crisi ucraina." Gazzetta Ufficiale, May 17, 2022. https://www.gazzettaufficiale.it/eli/id/2022/05/17/22G00070/sg.

[109] Ministero della Difesa. "Documento Programmatico Pluriennale della Difesa per il Triennio 2021-2023." 2021.

[110] La Rocca, Giancarlo, and Alessandro Marrone. "Italy and Space, a Strong Position to Enhance." In The Expanding Nexus between Space and Defence, edited by Alessandro Marrone and Michele Nones, 65. Roma, 22|01.

which attribution is difficult.[111] Moreover, the document envisions that space and cyber could take over the traditional domains in defining military competition. When it comes to the concrete emergence of the threat, military satellites are considered more resilient, designed, and manufactured with strict requirements and taking into account the necessity to be ahead of technological innovation and meet the pace of modernisation of threats. Moreover, these satellites are part of a closed network, which reduces the overall surface vulnerable to threats.

Cyber: civil and defence approaches

The Network Operations Command (COR), a joint command under COVI dealing with cyberwarfare, spreads its area of competence over the protection of military satellites.[112] Therefore the paragraph below introduces the civil and defence approaches to cyber at the national level highlighting the nexus with space. A formalisation of the national approach on cyber preceded space, starting already in 2013 in line with a faster formalisation of a cyber posture at the European and Transatlantic level. The responsibility for cybersecurity and resilience in Italy falls under the horizon of the National Agency for Cybersecurity (ACN). The ACN has been instituted in 2021 with the Decree-Law No. 82 of 14 June 2021, as the successor of the Security and Intelligence Department (DIS) formerly responsible for the cyber competence. Moreover, the President of the Council of Ministers holds the high management and the general responsibility of national cybersecurity policies and reports annually to the Parliament on the basis of a progress review document prepared by the ACN.[113] Interestingly, a Prime Minister Decree of 2020 includes space services and activities within the national perimeter of cyber security, giving thus specific recognition of the critical nature of space infrastructure for the national security.[114]

The governance landscape is complemented by an Inter-ministerial Committee for Cybersecurity (CIC), a Cyber Security Unit which involves the Intelligence community and several Ministers, and also by a specific unit at the Ministry of Foreign Affairs and International Cooperation (MAECI), operational since 2013 and focusing on the political and diplomatic actions related to the cyber domain. In May 2022, the ACN released a National Cybersecurity Strategy for 2022-2026 and an associated implementation plan. Already in 2013, however, and in 2017 with the "National Strategic Framework for Cyberspace Security" and the "Italian Cybersecurity Action Plan", the need for active defence in the domain was clear, with the objective to increase the costs of cyberattacks and make them more difficult and expensive to conduct.

From this, it ensued the relevance of a proper military approach and the establishment of COR in 2020, transformed from the several commands that were existing within the Defence community, unifying the competences and the authority to counter cyberattacks against Defence structures as well as attacks of national relevance. The Command then complements the national cyber architecture and represents the primary institution for cooperation at NATO level as well as for the EU cyber-defence initiatives. For instance, the Italian COR Computer Emergency Response Teams (CERT) participated in the EU MilCERT Interoperability Conference (MIC) of EDA, scoring the third overall mark and winning the award for information sharing, thus taking stock of the clear added-value demonstrated by other countries of a strong civil-military cooperation. Last but not least, the COR is the entity responsible for technological development within the military realm and for enhancing and cultivating the human capital and competence.

[111] Ministero della Difesa. "Direttiva Politica Nazionale Militare 2022."
[112] Interview, February 2023
[113] Marrone, Alessandro, Ester Sabatino, and Ottavia Credi. "Italy and Cyber Defence." Documenti IAI 21|12 (September 2021).
[114] Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131.

For what concerns technology, the recent ACN implementation plan contains a measure on developing national and European technology with particular regard to innovative and sensitive components, including space, with involvement of the ACN but also of the Ministry of Defence and the competent authority on space affairs.[115] Furthermore, as is already the case for space, the Italian industry is also a leading innovator in the cyber sector. Leonardo is the leading company for security services provided to the public administration and Defence authorities in Italy and is the prime contractor for the protection of the infrastructure of the NATO Communication and Information Agency and for the Cyber security operations centre of the European Space Agency.[116] Leonardo is also developing a proper Cyber Range within the Joint Telecommunications Academy of the Italian armed forces, based in Chiavari, which is essential to simulate complex scenarios that are not permitted or acceptable in the real world.[117]

A national perspective on cyber threat and the way ahead

Overall, Rome has initiated a streamlining of the governance of the space and cyber sectors, which is advantageous for a greater institutional focus on these domains and achieving a deeper space and cyber nexus. Both COS and COR provide services to Defence community and are responsible for asset protection. The general understanding of professionals and insiders confirms that the cyber threats to space systems are the same as the ones faced by terrestrial infrastructure.

First, space systems can be targeted in their ground infrastructure. These can be intrinsically vulnerable because of software and hardware components. Moreover, the supply chain is considered an increasingly emerging vulnerable point, especially for COTS or mass market products, which will require more attention in the short to medium term due to the growing space economy and presence of start-ups. These companies may be less inclined to take all the necessary measures to update security patches, thus increasing the vulnerabilities. Civil, education, and experimental satellites must indeed be cyber-secured to prevent hostile takeover of telemetry and control of assets leading also to potential co-orbital threats. Finally, in the digital cyber domain, the physical space and distances are irrelevant.

For what concerns the space systems as a whole, a typical vulnerability could be its connection to open networks. While malwares and backdoors can be found also in closed ones, open networks undeniably widen the possibility of access to systems and the overall attack surface.[118] Moreover, space systems traditionally have a peculiar difference with other potential targets of cyberattacks, i.e., the long design and production cycles, an opposite trend compared to the quick and unstable cyber threat.[119] This emphasises a trade-off between cheaper COTS products and longer production cycles facing the cyber threat, leading to considerations on the acknowledgement of the involved risks and the necessity of a serious debate on security-by-design at the European level.

This outlook confirms the need for the Defence community to ensure the safety and security of the space domain. Non-state actors or hacktivists, protected by states, are also exploiting the threat, which is clearly cheaper and more accessible than other space threats potentially leading to a surge in attacks. The EU Space Strategy for Security and Defence (EUSSSD) takes quite a proactive role

[115] Agenzia per la Cybersicurezza Nazionale. Piano di Implementazione. Strategia Nazionale di Cybersicurezza 2022-2026. https://www.acn.gov.it/ACN_Implementazione.pdf

[116] "Wired" L'alta formazione della Cyber & Security Academy contro gli attacchi informatici. https://www.wired.it/branded/article/sentinelle-digitali-cyber-and-security-academy-leonardo/

[117] Ministero della Difesa. Poligono Cyber. https://www.difesa.it/SMD_/EntiMI/STELMILIT/Pagine/UNAVOX.aspx

[118] Interview, February 2023

[119] Credi, Ottavia, Giancarlo La Rocca, and Alessandro Marrone. "Il dominio spaziale e la minaccia cyber." In Documenti IAI (March 2023). Istituto Affari Internazionali. (To be published)

in defining policies and processes, within a clear security architecture, to address cyberattacks while keeping a balanced approach in the overall spectrum of kinetic and non-kinetic threats. In fact, before Ukraine, direct-ascent kinetic ASAT technologies materialised as the most destructive and serious threat to satellites. Yet after Ukraine, cyber is more and more seen as the most likely threat to space systems. The Strategy is successful in providing a definition of the space domain, which notionally also includes cyber and the electromagnetic spectrum, as well as in presenting a complete space threat landscape.

From the Italian perspective, these developments at the EU level could be positive to break down silos between communities of different stakeholders (operators, institutional and commercial actors, cyber and space actors, etc.) and ensure a holistic approach to space security. As paramount initiatives, information sharing platforms must be established and common standards improved. Moreover, most national experts maintain that penetration tests, red teaming, crisis management exercises and simulations must be conducted at European level also to enable offensive training and achieve a sort of digital twin where factually analysing the cyber vulnerabilities and finding appropriate countermeasures. In this perspective, Rome supports the security core task at the basis of the foundation of EUSPA, driving also the new agency to acquire more competences and responsibilities in the field. This is viewed as a positive transition from a more purely commercial and economic approach to space to recognise the weight and relevance of security and defence aspects and implications for the whole sector. At the same time, some experts emphasise how relevant it would be to exploit the relations with NATO on this front, if necessary by building the appropriate mechanisms at the interorganisational level directly within EUSPA.

The war in Ukraine emphasised the nature of space assets as essential *centres of gravity* – as defined within the Italian Space Defence strategy – and critical infrastructures for states. The attack against KA-SAT is considered by interviewed officials as meant to disable first and foremost the Ukrainian air defences, with spill overs on all the end-user's modems and interdependencies with private networks and systems, such as energy providers. Therefore, an attempt to map the dependences of public and private sectors from space systems is warmly welcomed from the national perspective, in order to fully understand the value – only fated to grow in the future – as well as the weaknesses of this relation.

Italy has been a target of cyberattacks, more so compared to the past, and the support to Ukraine certainly is considered the primary cause of this new trend.[120] This brought the threat even more under the eye of the military, where there is a growing awareness also of the increasing relevance of cloud and digital integration in the sector. Finally, the increased attention towards cyber – in the news recently also because of the approval of the NIS2 Directive[121] – should be capitalised in a support for an EU-wide solution similar to the White House SPD-5, Section 4, for instance for what concerns the creation of a supranational stakeholders' initiative to gather developers, owners and operators to consult and define best practices and solutions. This is now implemented in the EU SSSD which proposes the creation of an EU Space ISAC gathering commercial and public entities.

Last but not least, the Italian Space Agency conducts several activities relevant to the space-cyber nexus. During this year, ASI has signed an agreement with the intelligence Department of Information for Security aiming at the development, within the European navigation programme Galileo, of the necessary capabilities to enable the use of the PRS service. The partnership has the objective to enhance and protect national capabilities in the field of security, as envisioned also by

[120] "Il Sole 24 Ore" (2023, February 22). Cyber terrorismo, attacco russo contro siti italiani dopo la visita di Meloni a Kiev. https://www.ilsole24ore.com/art/attacchi-cyber-italia-russia-reazione-visita-premier-kiev-AEP2mlrC

[121] Network and Information Security 2 (NIS2) Directive on measures for a high common level of cybersecurity across the Union.

the National Space Security Strategy of 2019.[122] ASI also entered in agreement with the national State Police to anticipate and counter cybercrimes targeting the networks and information systems that support the institutional functions of the Agency and are of particular relevance for the country.[123] The initiative reinforces the role of the Italian Space Agency within the national cyber security perimeter through its information systems and network infrastructure. Furthermore, within the "Three-year activity plan", the Agency focuses on cybersecurity related activities as well as on quantum ones, especially on Quantum Key Distribution which is considered a strategic area of interest given also a positive national track record, on this segment. This could potentially change the approach to the cyber threat to space systems.[124] [125]

[122] https://www.asi.it/2023/03/segnali-dal-cielo-piu-sicuri/

[123] ASI | Agenzia Spaziale Italiana

[124] "Piano Triennale delle Attività 2022-2024", Agenzia Spaziale Italiana, 2022. ASI | Agenzia Spaziale Italiana

[125] La Rocca, Giancarlo, and Alessandro Marrone. "Italy and Space, a Strong Position to Enhance." In The Expanding Nexus between Space and Defence, edited by Alessandro Marrone and Michele Nones, 65. Roma, 22|01.

THE INTERSECTION OF SPACE AND CYBERSECURITY IN UK DEFENCE POLICY - POLICY OBJECTIVE AND STRATEGIC APPROACH

Christoph Beischl, Associate Deputy Director, London Institute of Space Policy and Law (ISPL)

Over the past few years an increasing number of governments, militaries, academics and others has come to pay considerable attention to space and cyber, including on defence matters. The current Ukraine War in particular has put a spotlight on the defence issue of cyberattacks against space assets. As shown further below, the United Kingdom (UK) is no exception in this context.

Against this background, this article aims to advance the research on and general understanding of space and cybersecurity in UK Defence Policy. It especially asks whether the UK presently pursues any defence-specific policy objective and related basic strategic approach at the intersection of space and cybersecurity.

The short answer is that no such policy objective and strategy have been clearly stated. Nonetheless, the content of its various official documents allows extrapolating that the UK has, alongside its various declared objectives, vaguely established such a defence-specific policy objective. Its publicly promoted strategic approaches also encompass elements that serve the pursuit of this objective.

In particular, the following official documents allow for this extrapolation: the Government's recently released *Integrated Review Refresh* (IR2023),[126] an update to its *Integrated Review of Security, Defence, Development and Foreign Policy* of 2021;[127] the *Defence Space Strategy* (DSS), released by the UK Ministry of Defence (MoD) in 2022;[128] the *National Cyber Strategy 2022* (NCS), first published by Government in 2021;[129] the Government's *National Space Strategy* (NSS) of 2021;[130] the MoD's *Defence in a Competitive Age* (DCA) report published in 2021;[131] the Government's *Defence and*

[126] 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', Presented to Parliament by the Prime Minister by Command of His Majesty (HM Government, March 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145586/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf. This document also explains on page 6 that '[t]he 2021 Integrated Review, Global Britain in a Competitive Age (IR2021), set the UK's overarching national security and international strategy, bringing together defence, security, resilience, diplomacy, development and trade, as well as elements of economic, and science and technology (S&T) policy. It is supported by a series of published sub-strategies, including the 2021 Defence Command Paper, the Defence and Security Industrial Strategy, the National Artificial Intelligence Strategy, the National Cyber Strategy, the National Space Strategy, the Strategy for International Development, the UK Export Strategy, the British Energy Security Strategy, the Net Zero Strategy, the Arctic Policy Framework and the UK Government Resilience Framework.'

[127] 'Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy', Presented to Parliament by the Prime Minister by Command of Her Majesty (HM Government, March 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

[128] 'Defence Space Strategy: Operationalising the Space Domain' (Ministry of Defence, February 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051456/20220120-UK_Defence_Space_Strategy_Feb_22.pdf.

[129] 'National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK' (HM Government, December 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

[130] 'National Space Strategy' (HM Government, September 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1034313/national-space-strategy.pdf.

[131] 'Defence in a competitive age', Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty (Ministry of Defence, March 2021),

Security Industrial Strategy (DSIS) of 2021;[132] and the MoD's *Joint Concept Note 1/20 Multi-Domain Integration* (JCN 1/20) of 2020.[133]

Defence-relevance of space and cyber *per se*

Overall, a general look at the aforementioned documents makes clear that the UK is aware of the relevance of space and cyber for the country's defence per se.

For example, DSS states that the UK knows five operational domains, namely air, cyber, land, maritime and space. Space is considered a key enabler for its military operations, especially by providing military support functions such as global command and control, surveillance, intelligence, missile warning, and delivery of precision weapons.[134] For the UK the space domain "includes the satellites in space, supporting ground infrastructure, and the information layer connecting ground and space."[135] In DCA the UK similarly determines that access and use of space are "fundamental to military operations. Loss of, or disruption to, the space domain could severely impact our ability to undertake most Defence tasks, and have a catastrophic effect on civilian, commercial and economic activity." Furthermore, the growing reliance on space has translated into a growing vulnerability that adversaries might want to exploit to hamper UK military operation capabilities.[136]

Besides that, DCA also reads that "[f]or Defence, the cyberspace threat surface is broad with information networks, weapon systems and platforms relying on cyberspace capabilities. Cyberspace threats will emanate from state, state-sponsored and criminal groups with personnel and capabilities moving seamlessly between them. As with other domains, cyberspace activity is often leveraged as part of a wider, coordinated and integrated attack. Cyberspace espionage can and will be used as part of wider influence and propaganda campaigns, as well as in support of wider hostile activity up to and including conventional warfare."[137]

JCN 1/20 then indicates that research focusing on the connection of space and cyber from a defence perspective will find an interested audience in the UK defence community. After all, the document concludes that "[t]he space and the cyber and electromagnetic domains underpin MDI [(Multi-Domain Integration)] with its emphasis on systems and networks and links to information activities; they are critical enablers and effecters, yet they are the least understood domains in UK Defence."[138]

Policy objective

Ultimately, a deeper dive into information and indications in the aforementioned documents allows extrapolating that the UK has vaguely established the following defence-specific policy objective

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf.

[132] 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty (HM Government, March 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971983/Defence_and_Security_Industrial_Strategy_-_FINAL.pdf.

[133] 'Joint Concept Note 1/20 Multi-Domain Integration' (Ministry of Defence, November 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950789/20201112-JCN_1_20_MDI.PDF.

[134] 'Defence Space Strategy: Operationalising the Space Domain', 6.

[135] 'Defence Space Strategy: Operationalising the Space Domain', 9.

[136] 'Defence in a competitive age', 45.

[137] 'Defence in a competitive age', 10.

[138] 'Joint Concept Note 1/20 Multi-Domain Integration', 18.

at the intersection of space and cybersecurity: *advancing the cybersecurity*[139] *of UK defence-linked space capabilities and capacities, primarily against (actual and potential) cyber threats*[140] *posed by adversaries*.

After all, IR2023 states that the space and cyber forces of the UK "must be sufficiently capable, resilient, deployable and adaptive to deter potential adversaries from engaging in conflict, and to win a conflict if deterrence fails."[141] The document further highlights "cyber security and resilience across the UK's businesses, people, critical national infrastructure and public services" as a priority area.[142] Notably, the UK considers space a part of its critical national infrastructure.[143] JCN 1/20 holds that "activities in space, especially destructive actions, are almost certainly of strategic significance and involve high stakes in terms of deterrence", adding that "[t]he cyber and electromagnetic domain is ubiquitous and pervades all other domains".[144] NCS also puts forward in one paragraph that cyber capabilities will play a stronger role in future conflicts. In the same paragraph it indicates that with more activity in the space domain, the related cyber risks[145] will increase.[146] DCA states in one section addressing anti-satellite weapons that the UK's "potential adversaries are aware of how reliant space is on cyberspace. These technologies are growing in capability, type and number and now present a full spectrum of threats that modern space and space-enabled operations will need to counter." The section concludes with the appeal that "[w]e must be vigilant; understand the threats we face and be prepared to continue to adapt."[147] Moreover, DSS determines cyber threats as one counterspace category with the potential to disrupt, deceive or deny UK space military capabilities.[148] DSS further conveys that the UK expects cyber-based counterspace activities to have likely mostly a temporary impact.[149] It shall be noted here that, by way of quoting an assessment by the Centre for Strategic and International Studies, China is called out as one actor with "widely used electronic and cyber-based counterspace capabilities."[150]

As a short excursion, there are information and indications in UK documents that allow inferring that the UK also pursues the policy objective of developing UK offensive cyber capabilities.[151] Apparently, the National Cyber Force (NCF), which involves MoD and other entities, "provides capabilities that will be used to deceive, degrade, deny, disrupt, or destroy targets in and through cyberspace in pursuit of our national security objectives."[152] While direct references to the

[139] According to NCS, cybersecurity covers for the UK broadly '[t]he protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.' See: 'National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK', 126.
[140] According to NCS, the UK generally determines cyber threats as 'anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.' See: 'National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK', 126.
[141] 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 34.
[142] 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 50. The first four words of this citation are originally in bold.
[143] 'National Space Strategy', 10.
[144] 'Joint Concept Note 1/20 Multi-Domain Integration', 18.
[145] According to NCS, the UK understands cyber risks as '[t]he potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm'. See: 'National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK', 126.
[146] 'National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK', 30.
[147] 'Defence in a competitive age', 10.
[148] 'Defence Space Strategy: Operationalising the Space Domain', 10–11.
[149] 'Defence Space Strategy: Operationalising the Space Domain', 10.
[150] As cited in: 'Defence Space Strategy: Operationalising the Space Domain', 12.
[151] 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', 21.
[152] 'Defence in a competitive age', 44; Adding to that, it reads in a recent NCF publication (originally in bold): 'In practical terms the NCF develops and uses cyber capabilities to carry out operations including disrupting adversary ability to make use of cyberspace and digital technology, influencing adversaries away from doing harm, and exposing hostile activity and wrongdoing.' See: 'The National Cyber Force: Responsible Cyber Power in Practice' (National Cyber Force, March 2023),

development of dedicated UK cyber-based counterspace capabilities are absent, their development seems not excluded. Future research focusing on offensive UK cyber capabilities regarding space might want to give this more attention.

Basic strategic approach

Naturally, in absence of a clearly formulated defence-specific policy objective at the intersection of space and cybersecurity, there is no related official basic strategic approach to be found. However, the strategic approaches outlined in aforementioned documents encompass elements that, while not explicitly directed at it, arguably serve the pursuit of the extrapolated policy objective. In particular, this article wants to point out the following seven strategic elements in service of the policy objective of advancing the cybersecurity of UK defence-linked space capabilities and capacities, primarily against (actual and potential) cyber threats posed by adversaries:

Multi-Domain Integration (MDI).[153] First, the UK works actively towards integrating the five operational domains of air, cyber, land, maritime and space with each other under the MDI concept.[154] This is no surprising step considering the recognised reliance of the various domains' information networks, weapon systems and platforms on cyber capabilities, and multi-domain relevance of space for military support functions. UK Strategic Command, NCF, UK Space Command and the UK Space Operations Centre (SpOC) seem to take on important roles in this regard.[155]

Cross-government understanding of risks. Second, and surely contributing to above integration attempt, the UK wants to advance cross-government understanding of cyber and space risks, including services and supply chains, so as to address them appropriately within its overall strategic approach.[156]

Resilience-building. Third, the UK wants to work towards increased resilience of the UK space, terrestrial and cyber infrastructure.[157] It is not clear what this entails in detail but the *Cyber Resilience Strategy for Defence* will undoubtedly come into play.[158] At the very least the investment into technological development, industry involvement, training of relevant staff, and collaboration with allies, as mentioned further below, will provide some contributions on that front.

Defence engagement with commercial actors. Fourth, the UK seeks to advance its engagement with commercial actors regarding its various defence and security activities.[159] Concerning space, DSIS states that MoD in its space projects plans "to embrace the growing UK space innovation environment and support the wider UK Space Sector growth aspirations through targeted projects

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf.

[153] To fully understand the MDI concept from the UK perspective, see: 'Joint Concept Note 1/20 Multi-Domain Integration'. Page 3 of the document describes MDI, among others, as 'the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare.'

[154] 'Defence Space Strategy: Operationalising the Space Domain', 6; see also: 'Defence in a competitive age', 39.

[155] 'Defence in a competitive age', 44–46.

[156] 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 50; 'Defence Space Strategy: Operationalising the Space Domain', 11.

[157] 'Defence Space Strategy: Operationalising the Space Domain', 19; supported by information and indications in: 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 34, 50.

[158] 'Cyber Resilience Strategy for Defence. Building a cyber resilient Defence' (Ministry of Defence, 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1073315/20220425-Cyber_Resilience_Strategy_for_Defence.pdf.

[159] 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', 6–10.

that can exploit novel technologies and provide capability to the user faster than traditional procurement methods." What is more, the UK follows in the path of many other states looking to benefit from dual-use in advancing its defence capabilities. In particular, DSIS reads that "[d]ual-use will be considered at all stages to ensure maximum cross-government benefit is derived, both in capability and value for money."[160] Also, in the context of industrial testing and evaluation capabilities, the UK wants to retain a strong domestic capability, while engaging internationally where appropriate. It is noted that the UK "intend[s] to develop future [… testing and evaluation] capability for Novel Weapons, Artificial Intelligence, synthetic/digital systems and space-based systems."[161] The *Cyber Security Toolkit* (CST) published by UK Space Agency (UKSA) in 2020[162] can serve as an important baseline for defence-commercial exchanges at the intersection of space and cybersecurity. According to NSS, CST aims to provide cybersecurity-specific guidance for commercial space systems.[163] It acknowledges that "there is a present and increasingly significant threat to vulnerable space assets; their strategic nature makes them a specific target for a wide range of cyberattacks that could manipulate or disrupt essential services and potentially destroy or weaponise them, demonstrating a clear requirement for an enhanced and robust cyber security regime."[164] It mentions, among others, defence-relevant actors such as states and terrorists as potential hostile actors. Potential cyberattack types listed are "Installation or execution of unauthorised/malicious software", "Physical loss, theft or damage of an IT [(Information Technology)] asset", "User impersonisation", "Suspicious privilege admendment", "Suspicious use of legitimate privileges", "Eavesdropping on a communication channel", "Service Spoofing", "Service Jamming", "Denial of Service", and "Phishing".[165]

Engagement with international allies. Fifth, the UK wants to foster its engagement with international allies as appropriate.[166] When it comes to space and cyber, the United States of America, France and Germany receive special mentioning in DCA.[167] Moreover, according to the same document, the UK considers engagement through the North Atlantic Treaty Organization (NATO) as important to tackle cybersecurity of space capabilities. DCA reads that, "[f]rom both a political and military standpoint, NATO must respond to trends such as […] the importance of space and cyberspace as operational and warfighting domains." The organisation must address "the need to deter and constrain hybrid attacks on the Alliance and its members, such as cyberattacks, assassinations, disruption to space based systems, disinformation and attempts to erode our technological base through espionage."[168] Interestingly, broader cooperation with EU institutions receives little attention. That is a shortcoming as reporting of cybersecurity incidents, as promoted in CST,[169] can help mitigate impacts among allies.

Skill improvement. Sixth, the UK is aware that "[c]apability in the future will be less defined by numbers of people and platforms than by information-centric technologies, automation and a culture of innovation and experimentation."[170] Tackling threats in the space and cyber domains, including the cyber threat to space capabilities requires a workforce with the necessary skill sets. Thus, the UK wants to foster relevant training and education. This includes cyber-related learning

[160] 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', 100.
[161] 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', 87.
[162] 'Cyber Security Toolkit' (UKSA, May 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885869/Space_cyber_toolkit_final_v4.pdf.
[163] 'National Space Strategy', 26.
[164] 'Cyber Security Toolkit', 2.
[165] 'Cyber Security Toolkit', 4.
[166] 'Defence Space Strategy: Operationalising the Space Domain', 12–13, 19–20.
[167] 'Defence in a competitive age', 28–30.
[168] 'Defence in a competitive age', 27–28.
[169] 'Cyber Security Toolkit', 17–18.
[170] 'Defence in a competitive age', 39.

from academia, industry and allies, as well as the setup of a Space Academy.[171] The UK further considers employing "the Unified Career Management approach, as pioneered with the cyber workforce", towards the space domain. Adding to the aforementioned engagement with the commercial sector, this approach involves "develop[ing] novel and innovative partnerships with the commercial sector", having "commercial staff embedded within the [...] SpOC Commercial Integration Cell" and advancing the partnership "with the UKSA to fully integrate them into the UK SpOC."[172] Moreover, the UK wants to integrate space into exercises and war games conducted for, among others, the cyber domain.[173]

International norms and responsible behaviour. Seventh, in all the above the UK wants to abide by current international norms, promote responsible behaviour, and support related cross-government and international efforts.[174] This includes establishing "an international environment of behaviours and operating norms that deters adversaries and lessens their appetite for engaging in deliberate disruption or denial of essential space services."[175] IR2023 adds that the UK wants "to shape rules and norms of behaviour in cyberspace", involving the "unblock[ing of] the international debate on the application of rules, norms and principles in cyberspace and move it towards a consensus on effective constraints on destructive and destabilising activity by state and non-state actors."[176]

Conclusion

As its central finding, this article holds that the UK has within official documents vaguely established the defence-specific policy objective of *advancing the cybersecurity of UK defence-linked space capabilities and capacities, primarily against (actual and potential) cyber threats posed by adversaries*.

The article further concludes that the following seven elements in the strategic approaches outlined in the UK's current official documents serve the pursuit of this policy objective:

- Multi-Domain Integration of the five operational domains of air, cyber, land, maritime and space;
- Advancement of cross-government understanding of cyber and space risks;
- Improvement of resilience of the UK space, terrestrial and cyber infrastructure;
- Advancement of defence-commercial engagement;
- Engagement with international allies as appropriate;
- Increase of relevant skills among the workforce;
- Promotion of reasonable international norms and responsible behaviour.

The article's main recommendation to the UK is to develop and publish a document clearly stating the UK policy objectives and related strategic approach at the intersection of space and cybersecurity, as well as other aspects concerning the space-cyber connection. It would allow for a better understanding of the needs of the UK regarding these topics, ultimately benefiting UK Defence in the long-run. Until then, much more research is required to discern such objectives and strategy.

[171] 'Defence in a competitive age', 35, 45–46; see further: 'Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors.', 60–62, 82–83; 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 50.
[172] 'Defence Space Strategy: Operationalising the Space Domain', 27.
[173] 'Defence Space Strategy: Operationalising the Space Domain', 26.
[174] 'Defence Space Strategy: Operationalising the Space Domain', 20.
[175] 'Defence in a competitive age', 45.
[176] 'Integrated Review Refresh 2023. Responding to a more contested and volatile world', 28.

Conclusion

This ESPI collective report took stock of the different evolutions and highlights revealed by the war in Ukraine or impacting it and used this event as a starting point to raise broader questions that will affect future conflicts. The authors not only provided an analysis of the interaction between space and cyberspace in the context of the war in Ukraine, but they also conducted detailed examination of the specificities related to national policy perspectives and elaborated on the consequences of the commercialisation and digitisation of the space sector on military space activities. While doing so, the **report also uncovered numerous unresolved issues and questions that shed light on the complexity of the space-cyber-defence nexus**, which should be further investigated.

Defining, conducting, attributing, and responding to an attack on a space system

The nature of satellites: military, commercial, or dual?

The space cybersecurity governance at the European and intergovernmental level

Is cybersecurity in space the same as cybersecurity on Earth?

Skills development, cyber ranges, space exercises, and wargaming

Is Ukraine one cyberattack away from losing the war?

Heterogeneous national approaches to space cybersecurity

Defining, conducting, attributing, and responding to an attack on a space system

The war in Ukraine and recent developments in the military space environment raise questions regarding the definition of an attack on a space system, as well as the ability and legal character of attacking a spacecraft and responding to such threats. Objects navigating in space are not as flexible as their counterparts on Earth; this makes space a specific domain and has an impact on the options to respond to a threat or attack. Overall, conceptual, operational, and legal aspects can be debated:

- **Definition:** defining what constitutes an attack in space is a difficult exercise and triggers controversy. There is currently no universally accepted definition of an attack on a space system. Whenever a country starts developing and conducting military activities in space, doctrinal developments addressing the establishment of a threshold of aggression are necessary. Indeed, for a state to protect its spacecraft, it needs to determine when an "unfriendly" behaviour will be interpreted as an armed attack on its space capabilities. The issue becomes even more complex when addressing non-kinetic attacks, which rarely generate physical damage. Some states believe that cyberattacks should generate the same damage as kinetic attacks to be labelled as armed attacks while others consider that an intrusion on their system is sufficient to be regarded as such. However, the definition and qualification of an armed attack remain highly political and circumstantial.
- **Attack**: it seems important to question the legal character of any attack that would be carried out in outer space. In other words, which factors and motivations could justify such an action? In addition, there are still uncertainties around the specific corpus of law that should be leveraged when conducting an attack in space. While, in line with Article III of the 1967 Outer Space Treaty, most countries and scholars recognise the applicability of international law to outer space, including international humanitarian law, some countries such as China and Russia remain reluctant to acknowledge this latter point.

- **Attribution**: attribution is a concept that is at the core of any strategy to protect a nation's space assets, including deterrence strategies. However, attribution is a task whose complexity varies with the type of attack considered. While kinetic attacks may be easier to attribute with appropriate space situational awareness and early warning capabilities, identifying an aggressor in case of non-kinetic attacks can prove much more difficult as the attack cannot be easily detected by third parties. In case of co-orbital kinetic attacks, it may also be difficult to demonstrate the intention to harm a potential adversary as the attacker can plead for a technical issue. In the case of cyberattacks, attribution implies to trace back the data packets and routes that the attacker used to enter a network as well as patterns (e.g., in the code or in the types of vulnerabilities exploited) that may enable to identify it. Attribution of cyberattacks often involves specific capabilities and potentially hacking back, which is usually considered as the sole domain of governments.
- **Retaliation:** In the event of an attack, the question of retaliation can also be raised. When an action is clearly identified as an attack, is retaliation systematically allowed? If not, how severe does it need to be to allow for retaliation and what form can the latter take? The UN Charter as well as provisions of international humanitarian law (in particular the distinction and proportionality criteria) can be useful to support the decision to retaliate, but not all major space powers recognise the applicability of IHL to space. In case of cyberattacks, the applicability of IHL to cyberspace and the way in which it applies is also not consensual among states. Finally, another question is related to the nature of the actors who could retaliate or act in space. While institutional actors and operators of military satellites are compelled by the doctrine of their state, commercial operators that are providing services to military actors may be attacked and tempted to retaliate in some sort. This is particularly striking with cyber threats on space systems where commercial space companies may decide to start offensive cyber activities to attribute or retaliate against an attacker, without the authorisation or approval of their state; this raises questions about the legal character of such actions as well as the consequences for strategic stability in both space and cyberspace.

The nature of satellites: military, commercial, or dual?

The characterisation of a satellite as a military, dual, or civilian asset seems to become more complex and blurrier. The emergence of commercial actors and their role in providing services to both civilian customers and armed forces or belligerents in an armed conflict raise **new questions on the validity of this characterisation.** Should it be based on the *use* of the satellite or on its *ownership*? Focusing on the actual missions supported by the satellite at a specific point in time could also prove relevant to clarify the concept of "dual-use", which remains highly debated.[177]

However, such debate needs to be held, as the growing role played by dual-use satellites in the conduct of military operations has some consequences. First, **the situation renews the discussion on whether such satellites are a legitimate target or not.** Some states, such as Russia and Iran, have expressed that commercial satellites employed against their interests (e.g., by supporting adversaries' military operations or internal uprisings) should be considered as such targets

[177] In this context, new research is proposing to differentiate dual-use and dual-purpose spacecraft. The former refers to the "present function of an object", which can be both military and civilian, simultaneously or not. The latter rather insists on its "potential future application", meaning that, although the object is not built to harm other spacecraft, it could potentially be repurposed to do so due to its characteristics or capabilities. This category focuses rather on in-space threats and therefore does not apply to the current Ukrainian context. For more information, see Ortega, Almudena; Azcárate. "Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems." June 5, 2023. https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems. One author in this report also distinguishes between "actual" and "potential" dual-use, the former being for satellites that still have dual-use applications while the latter applies to those that used to have such applications.

according to the UN Charter and the right to self-defence. More generally, the fact that a spacecraft can serve both civilian and military interests highlights the **importance of the time factor.** In this context, a satellite, even commercial or civil, could become a legitimate target as long as it serves military applications but would lose this label as soon as it reverts back to purely civilian missions. Of course, this may be complicated by the fact that civilian and military needs can be met at the same time by a single satellite.

While the definition of a satellite as civil, military or dual may seem like a purely semantic question, it impacts its security requirements. Indeed, as civil/commercial spacecraft are increasingly used for military purposes, it also becomes questionable whether such systems should be as protected as military ones.

Is Ukraine one cyberattack away from losing the war?

Considering the criticality of Starlink to support both access to connectivity for the population as well as the entire Command and Control (C2) of Ukrainian operations, one could raise the question: *"Is Ukraine one cyberattack away from losing the war?".* While Starlink is usually depicted as the backbone of Ukraine's military and civilian communications, the issue is likely more complex as terrestrial infrastructure remains used for military communications and space systems are often employed as a back-up solution when terrestrial systems are unavailable.[178] Ukrainian soldiers also seem to know how to operate in a degraded and contested environment, and space systems are only one enabler among others of military operations on the ground. Therefore, Ukraine might be able to resist without satellite communication capabilities, albeit likely for a short period of time.

However, **this question raises broader interrogations on the security and resilience of large constellations such as Starlink.** How difficult is it to entirely disrupt the functioning of a large constellation? Are large constellations providing better resilience than a single military communication satellite in GEO? One could argue that constellations are more resilient as many of its individual space systems would have to be disabled to prevent any connection. Unlike individual GEO communications satellites, the high number of assets in constellations provides redundancy to the service. However, it could also be argued that large constellations' small satellites are all identical and therefore one unpatched vulnerability found in one system would enable attacking all the satellites of the constellation, making it a single point of failure.

In addition, space start-ups and emerging companies make more often use of commercial off-the-shelf (COTS) components to build their spacecraft, which can easily be bought by malicious actors to look for vulnerabilities. Finally, they also often overlook cybersecurity due to cost and a lack of awareness and are usually more communicative than traditional defence and space actors as they share much information about their systems, employees, facilities, and supply chain, which may give a malicious actor some critical information to launch an attack.[179]

Is cybersecurity in space the same as cybersecurity on Earth?

A debate among experts and scholars is now extending to satellite operators and industrial stakeholders as space cybersecurity best practices, standards, and rules are being implemented

[178] "Cysat 2023: Live from Kyiv with General Oleksandr Potii." YouTube, May 22, 2023. https://www.youtube.com/watch?v=CFCwOoVii7A.
[179] James Pavur, Space for the IoT, Webinar, Space Generation Advisory Council, 2020

and discussed: is cybersecurity in space the same as implementing cybersecurity on traditional computers on Earth?

One could argue that space systems are now digital objects operating with software components and IP protocols and are therefore **subject to the same cyber threats as traditional computers** on Earth. This situation implies that implementing the same cybersecurity solutions would be enough to ensure the integrity of space systems (considered as ground, control, user and space segment altogether).

However, **when it comes to the space segment, some arguments are made to explain that the situation is rather different due to its far distance from Earth and the natural hostility of the orbital environment.** For instance, when the FBI and CISA advised satellite operators to implement independent encryption, James Pavur from the University of Oxford noted that *"security practices used by terrestrial internet customers, such as end-to-end VPN encryption, were not designed for compatibility with the traffic optimizations used in satellite broadband services... Satellite signals travel immense distances and are subjected to significant packet loss and latency as a result... the use of VPNs and customer-implemented end-to-end encryption results in significant performance reductions."*[180] Gregory Falco also noted that applying encryption requires using significant processing power and bandwidth, which is limited onboard the spacecraft, leading operators to prioritise critical functions. He further highlighted that the risks of applying traditional IT security to space assets can result in significant gaps in cybersecurity due to a lack of understanding of the satellite and its specific components,[181] which *"lack terrestrial equivalents"*.[182] James Pavur takes the example of star trackers, which are not present on terrestrial systems, and therefore do not benefit from the general body of knowledge on cybersecurity.

Limited research exists on the vulnerability and resilience of these components to cyber threats and the literature on the applicability of traditional cybersecurity measures to such systems is almost inexistent. In addition, the difference also lies in the perceptions of threat actors. For instance, when the Ukrainian OneFist hacker group hacked the Russian Statis satellite network in November 2022, it acknowledged that it was its first cyber operation on a satellite network and that the environment was unique for them.[183]

As a result, it appears that the supply chain, the ground segment, control segment, and the user segment are all facing traditional cybersecurity issues for which traditional cybersecurity solutions can be adapted and implemented. However, when it comes to the space segment, cybersecurity seems very different in forms and challenges.

Skills development, cyber ranges, space exercises, and wargaming

Further developing skills in military space and space cybersecurity is also a topic that increasingly needs to be tackled. **These domains are relatively new and their expansion for military operations will require an appropriately educated workforce**, especially in light of the wave of retirements that the European space sector will face in the coming years. Public authorities should take appropriate measures in their educational systems to make sure that the skills that are needed by military space and cybersecurity actors are available on the job market. Interdisciplinary research

[180] Targett, Ed. "US Agencies Urge 'Independent Encryption' for Satellite Communications." The Stack, May 24, 2023. https://www.thestack.technology/satellite-communications-encryption-cisa-satcom-cybersecurity/
[181] Falco, Gregory. "The Vacuum of Space Cyber Security." 2018 AIAA SPACE and Astronautics Forum and Exposition, 2018.
[182] Pavur, James, and Ivan Martinovic. "Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 years of Spaceflight." Journal of Cybersecurity 8, no. 1 (2022). https://doi.org/10.1093/cybsec/tyac008.
[183] One Fist. "Operation Polaris." Team Onefist, November 6, 2022. https://www.onefist.org/post/operation-polaris.

on space cybersecurity is still lacking, in particular to better understand cyber threats against the space segment, ensure that industry develops the right cybersecurity and cyber defence capabilities and eventually enable operators to implement appropriate processes and incident response.

Beyond the educational phase, **continuous training is also important.** Therefore, another requirement is to provide more opportunities for training and red teaming in order to make sure that the armed forces will be operational in case tensions in space give way to actual conflict. Such exercises allow testing systems in (quasi-)real conditions as well as the reactions of operators, and thus better prepare to face a potential threat. In this context, the French exercise AsterX as well as the EU Space Threat Response Architecture, whose latest editions were both conducted in March 2023, are generally seen as best practices to replicate or build upon.

The space cybersecurity governance at the European and intergovernmental level

The governance of space cybersecurity as well as international and intersectoral cooperation in the field of space cybersecurity is also an issue to better investigate. **Cybersecurity in the space sector remains under-regulated and cybersecurity obligations to obtain launch permits or operate a spacecraft are mostly inexistent in Europe.** Despite a scattered and limited regulatory framework, most actors have gradually acknowledged the cyber threat and taken dedicated measures.

At the European level, **both ESA and the EU recently acknowledged the importance of space cybersecurity.** ESA adopted a space cybersecurity strategy for its own systems. It also acknowledges the importance of the threat and the criticality of developing dedicated capabilities and skills with the establishment of the European Space Security and Education Centre (ESA ESEC), a centre of excellence for cybersecurity services[184], and the recent creation of the Cyber-Security Operations Centre (C-SOC) to provide cyber-monitoring and management capabilities to its Member States.[185]

Through Regulation 2021/696, the European Commission, with the support of EUSPA, is responsible for ensuring a *"high degree of security with regard to the protection of the infrastructure, both ground and space, and of the provision of services, particularly against … cyberattack, including interference with data streams"*.[186] However, Regulation 2021/696 is only applicable to the EU Space Programme and does not include national or commercial space systems. Therefore, in 2022, the EU adopted the NIS2 Directive, which compels *"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"* to apply strict cybersecurity measures.[187]

In addition, the establishment of an EU SPACE Information Sharing and Analysis Centre (ISAC) by the end of 2023, as announced in the EU Space Strategy for Security and Defence, will help sharing

[184] "ESA ESEC." ESA. Accessed August 29, 2023. https://www.esa.int/About_Us/Corporate_news/ESA_ESEC.
[185] "New Cyber-Security Centre Will Safeguard ESA Assets and Missions." ESA. Accessed August 29, 2023. https://www.esa.int/Space_Safety/New_cyber-security_centre_will_safeguard_ESA_assets_and_missions2.
[186] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU. https://eur-lex.europa.eu/eli/reg/2021/696/oj
[187] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

information, raising awareness, and providing best practices to enhance the resilience of the European space ecosystem, including related to cyber threats.

At the international level, **cyber threats on space systems were recently discussed at the United Nations Open-Ended Working Group (UN OEWG) on Reducing Space Threats**, in particular in light of the KA-SAT cyberattack. However, space cybersecurity was never at the agenda of either the previous UN OEWG on "the security and use of ICTs" or the UN Group of Governmental Experts (GGE) on "Advancing responsible State behaviour in cyberspace in the context of international security". In addition, **the space and cybersecurity communities in these UN *fora* rarely interact to debate, let alone adopt consistent guidelines, norms, and other best practices on space cybersecurity.** Therefore, the topic is rather new for the international policy community. Similarly, within NATO, it remains to be seen how the NATO Space Centre and NATO Space Centre of Excellence will coordinate and cooperate with the NATO's Cyber Security Centre and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) to conduct consistent, adapted, and timely research, training, and exercises, and establish standards on space cybersecurity.

Heterogeneous national approaches to space cybersecurity

This collaborative report provided ground for a compared analysis of the public policy framework and governance of space cybersecurity in three selected European countries: France, Italy, and the United Kingdom. **These states have recently and gradually recognised cyber threats on space systems and updated their policy and governance framework accordingly.** Convergences and divergences are visible across these three countries:

State	Dedicated space cyber security strategy	Cyber threats on space systems recognised in space policy	Cyber threats on space systems recognised in cyber policy	Entity responsible for space cyber security	Cyber security obligations in national space law	Cyber offensive action authorised
FRA	X	✓	X	Multiple	X	✓
ITA	X	✓	X	Multiple	X	X
UK	X	✓	✓	Multiple	✓	X

Table 2: Comparative analysis of national approaches to space cybersecurity

The comparative analysis illustrates that these three countries do not have a dedicated space cybersecurity strategy, policy, or legislation unlike the United States with the Space Policy Directive-5. **It also raises the question of the usefulness of adopting such strategies in Europe.** In addition, all three countries only recently recognised and acknowledged cyber threats in their national space policies. France's Space Defence Strategy of 2019 acknowledges cyber threats, in particular on the software layer, and aims to protect and harden systems against cyber and electronic attacks.[188] Similarly, Italy's National Security Strategy for Space underlines that the purpose of the document is to ensure the resilience of the space infrastructure against unintentional

[188] French Ministry of the Armed Forces, "Space Defence Strategy", 2019. https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2020/08/france_-_space_defence_strategy_2019.pdf

and intentional threats, including cyber and electronic ones.[189] Comparably, the UK's Defence Space Strategy recognises cyber threats against space assets and aims to develop protection against such threats.[190] However, the cyber policies of France and Italy do not seem to explicitly address cyber threats on space systems, although they may consider satellites as part of cyberspace (e.g., French Cyber Offensive Doctrine).

Differences between these countries can also be spotted. For instance, the Italian reorganisation of 2019 led to a clearer governance of space, defence, and cyber issues compared to France, where activities related to cyber defence are scattered between different organisations and responsibilities for space cybersecurity, in particular, are not easily identifiable. In a different perspective, both France and the United Kingdom put a strong emphasis on the multi-domain dimension, then trying to integrate space and cyber with other warfighting domains (i.e., land, sea and air), while this cross-cutting approach is less present in Italy. Finally, Italy has no legal framework for offensive cyber capabilities that would authorise Italian authorities to conduct such operations. However, in France, specific organisations (e.g., COMCYBER) are allowed carrying offensive cyber operations, while policies of the United Kingdom indicate that the country may consider such operations.

This report has addressed several dimensions of the space-cyber-defence nexus. It has shown that the growing involvement of commercial space actors in armed conflicts raises new questions that need to be embraced and leveraged by policy action. With regard to cyber, it demonstrated that, although this threat is increasingly considered by states, the elements to focus on and the ways to address it vary between countries. In this context, measures taken at the intergovernmental or supranational level could encourage better convergence between the approaches selected, which would contribute to strengthening the protection of European space systems. Nevertheless, additional analyses and comparative studies among all EU and ESA Member States would provide value in better understanding the space-cyber-defence nexus as well as, as an extension, the evolution of national approaches regarding kinetic and non-kinetic threats against space systems. ESPI will certainly remain actively involved on the matter and continue to explore these links in future research projects, under its growing "Security & Defence" research line presented in the Institute's **ESPI 2040** Policy Vision.

[189] Presidency of the Council of Minister, "National security strategy for space", July 2019. https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/NationalSecurityStrategySpace.pdf

[190] UK Ministry of Defence, "Defence Space Strategy: Operationalising the Space Domain", February 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051456/20220120-UK_Defence_Space_Strategy_Feb_22.pdf

Editors

Mathieu Bataille is a Research Fellow and Lead on Security and Defence at the European Space Policy Institute, whose research activities mostly focus on the use of space systems for the conduct of security and defence operations on Earth, as well as the protection of spacecraft in orbit. He worked previously at the Studies Department of the French Air Force. He holds a master's degree in Political Science and International Relations from Sciences Po Paris.

Clémence Poirier is a Research Fellow at the European Space Policy Institute (ESPI) in Vienna, Austria. She has expertise on space cybersecurity issues as she conducted policy research on cyber threats on space systems as part of the war in Ukraine, the perception of cyber threats on satellites in French policies, and the applicability of data protection laws to satellite images. She previously carried out research on space cybersecurity for Flinders University in Adelaide, Australia. She is an active member of SGAC's Space and Cybersecurity Project Group. She holds a Master's degree in International Relations, International Security, and Defense from University Jean Moulin Lyon 3, France.

Authors

Béatrice Hainaut is a Research Fellow at the Institute for Strategic Research (IRSEM) in Paris. She has expertise on outer space issues as she has held multiple space-related positions in the French Air and Space Force for more than ten years. She holds a PhD in Political Science, International Relations from University Pantheon-Assas Paris 2, France, which deals with Space Security

Nicolò Boschetti is pursuing a Ph.D. in Aerospace Engineering at Cornell University. His research interests include space and satellite ground systems security. Boschetti holds a BA in International Sciences from the University of Bologna, a MA in Politics and Economics in Eurasia from the Moscow State Institute of International Relations, and an MS in Systems Engineering from Johns Hopkins University.

Ioannis Nikas is an undergraduate student at Johns Hopkins University in Baltimore, Maryland, United States. His research interests include autonomous space systems, assured autonomy, and space security policy.

Dimitrios Serpanos is President of the Computer Technology Institute and Press (CTI) and Professor at the University of Patras, Greece. He is the Chair of the Scientific Council of the INSIDE Industrial Association. Dimitrios holds a PhD from Princeton University and his research interests include embedded and cyber-physical systems, and cybersecurity.

Gregory Falco is an Assistant Professor at Cornell University in the Sibley School of Mechanical and Aerospace Engineering and the Systems Engineering Program. He earned his Ph.D. at MIT, where he conducted cybersecurity research funded by NASA's Jet Propulsion Laboratory. He also worked as an Assistant Professor at Johns Hopkins University and completed postdoctoral research at Stanford University and MIT CSAIL.

Xavier Pasco has been director of FRS (Foundation for Strategic Research) since October 2016. For more than 30 years, he has coordinated research on space, high technology and security programmes at FRS. He has been the author of numerous reports on civil and military space activities carried out on behalf of national and European public bodies. A member of multiple ministerial and inter-ministerial working groups, he has also been an expert at the European Economic and Social Council and has been elected member of the International Academy of Astronautics.

Paul Wohrer is a Researcher specialising in space issues at the French Institute of International Relations (Ifri). His research focuses on geopolitical and strategic issues, as well as technological and industrial developments in the space sector. From 2017 to 2023, he worked at the Foundation for Strategic Research (FRS) as a Research Fellow on space issues. Paul Wohrer is a graduate of Sciences Po Bordeaux and the International Space University in Strasbourg.

Giancarlo La Rocca is a Researcher at the International Affairs Directorate of the Italian Space Agency (ASI) since May 2023. Previously, from 2021 to 2023, he worked as a Junior Researcher at the Istituto Affari Internazionali and, in 2019-2020, he served as a Research Fellow at the European Space Policy Institute in Vienna. In 2019 he joined as an intern the Member States Relations and Partnerships Office at the European Space Agency and worked as research assistant of two international publications. With a master's degree in International Studies from Roma Tre University and a post-graduate master in Space Policies and Institutions from SIOI, Giancarlo has signed and contributed to various articles and publications on space and managed research projects collaborating with Italian, European, and international partners.

Christoph Beischl is the Associate Deputy Director of the London Institute of Space Policy and Law (ISPL). He is a member of the International Institute of Space Law (IISL) and the German 'SichTRaum' space research network, as well as a Physics Academic Visitor at Imperial College London. He holds a PhD from the Institute of Advanced Legal Studies (IALS), University of London, having examined the potential for establishing an Asian Space Agency. His current research focuses on UK and East Asian Space Policy and Law; Institutionalised Space Cooperation; Space Terminology; and Responsible Behaviour in Space, from Space Safety to Space Security, including as it relates to cybersecurity, AI and privacy.

ESPI

European Space
Policy Institute

office@espi.or.at

www.espi.or.at