Space and Cybersecurity: Challenges and opportunities emerging from national strategy narratives.

Abstract

Modern societies are increasingly dependent on space technology. The number of activities that rely on space infrastructure includes global positioning and communications systems, financial transactions and global trade, public and private scientific research, environmental monitoring and fore- casting, and audio-visual entertainment. Within the security and defence domain, this reliance becomes even more pronounced as satellites enhance command, control, communications and intelligence, surveillance, and recon- naissance (C4ISR), missile defence, or advanced autonomous systems. Furthermore, ongoing advancements in science and technology are opening new frontiers in outer space, promising significant economic potential through ventures like space travel and space mining. Considering the geopolitical implications of the dependence on space technology, the objective of this study is to examine how Western countries and organizations understand space within their strategic thinking. By conducting a comparative analysis of the most recent national security strategies and security and defence space strategies released by a sample of Western countries and organizations, including the United States, the United Kingdom, France, the European Union and NATO, this study aims to discern the narratives employed to depict the space domain and to identify the key trends within it, with a specific focus on the interplay between space and cybersecurity.

This exercise will facilitate the identification of areas where enhanced collaboration among the selected actors is feasible or where competition may define their relationships. Consequently, it will help determine the potential for a coordinated response to collective challenges.

Keywords:
Space security, Space strategy, Cybersecurity

Preprint submitted to Space Policy *February 20th, 2024*
Revised version submitted to Space Policy *May 24th , 2024*

1. Introduction

Space is not a separated realm where events unfolding within it follow a distinct logic and dynamics than those occurring on Earth. In an attempt to disassociate space exploration and utilization from the geopolitical realities, Article I of the Outer Space Treaty claims that the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind. However, the reality is that "space and politics are, and always have been, inseparably interlinked" [1], and, therefore, relations and cooperation among space actors are and have been primarily driven by their self-interests, strategic choices, and geopolitical realities on the Earth [2]. As reduced costs of space launch services have enabled numerous state and non-state actors to acquire advanced technologies [3] and scientific and technological progress is increasingly facilitating new uses of space, space is considered by policy-makers as a strategic domain where states and other actors deploy their power in, gain power from, and may seek to deny such advantages to others [4], making the relationship between space and geopolitics even stronger.

How states and non-states actors comprehend this bi-directional relationship is essential for assessing their strategic understanding of the recent developments unfolding in space and other space-related events. Specifically, it is worth noting the following events across various categories of space activities:

(i) Space exploration: on August 23, 2023, the Indian Space Research Organization's (ISRO) Chandrayaan-3 and its Vikram lunar lander apparently performed a soft landing on the moon near the lunar south pole, becoming the fourth country (after the Soviet Union, United States and China) to perform a soft-landing on the lunar surface and the first to put a spacecraft near the lunar south pole. Nonetheless, Ouyang Ziyuan, the chief scientist of the Chinese Lunar Exploration Program, commonly referred to as the Chang'e program, has raised doubts regarding ISRO's achievement, asserting that the landing did not come close to the lunar south pole region [5]. On August 11, Russia's space agency (Roscosmos) launched the Luna-25 lander mission with the aim of achieving a soft landing on the lunar south pole. However, just nine days later, the spacecraft met an unfortunate end when it crashed into the lunar surface due to an improper thrust manoeuvre during its lunar orbit insertion. In April 2023, the lunar lander Hakuto-R Mission 1, built and operated by the Japanese space company iSpace, crashed into the moon surface due to a computer error.

(ii) ASAT tests: On November 15, 2021, Russia conducted a kinetic anti- satellite test, which resulted in the successful destruction of the Russian satellite Kosmos 1408. This test generated a significant quantity of space debris, posing a threat to the safety of the International Space Station.

(iii) Space and the war of Ukraine: On February 24, 2022, just hours before the unlawful invasion of Ukraine by the Russian army, the satellite communications company Viasat Inc. experienced a cyberattack. This attack had far-reaching consequences, disrupting satellite internet services for tens of thousands of customers in Ukraine, including the Ukrainian armed forces, as well as impacting Europe, where approximately 5,800 wind turbines in Germany were affected. On May 10, 2022, the European Union, together with its international partners, attributed this cyberattack to the Russian Federation [6]. In addition to this, the satellite services provider company Starlink has been supporting the Ukrainian government and military forces during the illegal invasion by Russia [7, 8], providing them with a technological advantage that has allowed Ukraine to resist the pressure of the Russian army for more than a year.

The examples provided highlight the rise of non-Western space powers and private space companies across a spectrum of space activities that were formerly reserved for a limited number of states. This emergence of new actors, as suggested by Baiocchi and Welser [9], points to the "democratization" of space, which adds a layer of complexity in an already fragile space governance. However, the geopolitical implications of the increasing role of commercial companies in space go beyond this, as they are transforming the mere nature of the competition among space powers. In this regard, Moltz [10] argues that the dynamics defining the first space race that took place between the United States and the Soviet Union during the second half of the 20th-century – characterized by rival, state/military-led, and secret "technocracies", a model still followed by China and Russia – are being replaced by a new model of competition. This new model, consisting on a form of organization called "netocracy", is based on "public-private partnerships, distributed architectures, rapid innovation, and the use of multiple commercial and allied partnerships", which is led by the United States.Therefore, according to Moltz, competition in space would encompass not only a different set of actors, but two distinct space power models.

Given the significant geopolitical considerations that these trends have, it is essential to assess how Western countries understand these events and the effects they have in their strategic thinking. Conducting a comparative analysis of strategic documents released by Western countries stands as the most effective way to achieve this outcome. This type of exercise is not an unknown approach within the specialized literature on security studies. In the realm of cybersecurity, for example, it is worth noting the work of Luiif, et. al. [11], which provides a comparative analysis of ten national cybersecurity strategies; and the work of Craig, et. al. [12], which, in the same vein, analyse the national cybersecurity strategies of 83 nation-states in order to conceptualize them using a new typology. Regarding to the space field, there are several recent publications that employ content analysis methodologies to examine national space strategies and related documents. These studies primarily focus on analysing space governance structures, space strategies, and priorities of various members states within the ESA [13, 14, 15]. Notably, one outstanding work in this area is the research conducted by Papadimitriou, et. al. [16]. Their study aims to analyse the security aspects of space policy in Europe, taking into consideration national space strategies, programs and governance at EU, ESA, and national level (including states that are member states of the EU and ESA, such as France, Germany, Italy, and the United Kingdom). Similarly to these publications, the current study aims to offer a distinct approach to the analysis of space within security strategy documents, including also other actors such as the United States and NATO into the analysis. The purpose of conducting a comparative analysis intends to identify shared narratives that could be the ground for further collaboration among the selected states in the space domain.

1.1. Organization of the paper

Section 2 sets out the study's objectives and the methodology employed to achieved them. Additionally, this section provides an explanation about the selected sample, the strategic documents utilized for the study, and their connection to the concepts of grand strategy and strategy. The findings from the comparative analysis of the strategic documents are presented in Sections 3 through 6.

Section 3 offers insights into how the selected actors characterize the strategic environment as a whole based on their national security strategies. More specifically, Section 4 delves into the role of space within the national security strategies. Section 5 highlights the key narratives identified in the defence and security space strategies. Section 6 analyses the specific connection between space and cybersecurity as outlined in the national security strategies and the security and defence space strategies. Finally, Section 7 provides a succinct discussion about the most significant outcomes from the preceding sections as concluding remarks.

2. Objectives and Methodology

2.1. Objectives

This study aims at understanding how Western countries and organizations, such as the European Union and NATO, approach and conceptualise space within their strategic thinking, as well as how they address cybersecurity in the context of space. Specifically, this research seeks to contribute to the assessment of whether the trends and dynamics identified by these actors in the international context apply to the space domain and how these countries and organizations respond to the threats and risks they perceive in this domain, particularly those derived from the cyber domain. This study adds to the broader debate on the space domain, examining its potential as an area for international collaboration or competition, as well as the stance taken by the selected actors in this debate.

To advance these objectives, this study seeks to address the following research questions ("RQ"):

RQ1. How do we understand the strategic environment amongst leading nation states?

RQ2. How is the space domain – understood as "any element relevant for the functioning of space systems and the delivery of space-based services" [33] positioned within the national strategy narratives of Western states and international organizations such as NATO and the EU?

RQ3. How are nation states and bodies like NATO and the European Union addressing cybersecurity in the context of national security narratives and defence and security space strategies?

2.2. Methodology

The data used to address the RQs has been extracted from the most recent national security strategies and defence and security space strategies released by three specific states -the United States, the United Kingdom and France-, and two international organizations, the European Union and NATO.

Based on the data extracted from these sources, a comparative analysis has been conducted. This exercise has involved the analysis of the threat landscape as characterised in these strategic documents focusing on the specific narratives and language used to describe it. Narratives, or more specifically, "strategic narratives" are understood herein as "future-oriented identity claims that articulate a distinctive position on a specific issue or policy domain, or in general with regard to the place of an actor in world politics" [17].

As stated by Balzacq, Dombrowski and Reich [18] comparing and contrasting the strategic narratives included within the strategic documents adopted by the actors selected in this research will help us: (i) to discover causal relationships between the domestic drivers and the implementation of grand strategies; (ii) to identify areas of convergence and divergence across cases; and (iii) to highlight key empirical aspects of national strategies.

Methodologically, this research is structured around two distinct levels of analysis, ranging from the broad to the specific:

The first level of analysis encompasses a comparative evaluation of the narratives and language utilized in the assessments of the strategic environment as presented in the national security strategies. Furthermore, it scrutinizes whether these documents incorporate references to the space and cyber domains. In cases where such references are present, the analysis delves into how these references are characterized. Consequently, this initial level of analysis offers a general view of the strategic landscape and how it relates to space and cyber considerations.

The second level of analysis focuses on the space domain. In this phase, the comparative analysis is specifically centred on the narratives and language used to discern the primary threats to the space domain as perceived by the targeted actors and their proposals for addressing these threats. Thus, the comparative analysis of the defence and security strategies hinges on an evaluation of the types of threats, threat actors, and the response mechanisms intended to counter these threats. Furthermore, an assessment on how the defence and security space strategies address the cyber domain is included in this level of analysis.

2.2.1. Sources of policy narratives

Following the two different levels of analysis outlined in the methodology described above, the strategic documents from which data has been acquired are, accordingly, divided into two different groups: (i) national security strategies (including the strategic documents released by the European Union and NATO); and (ii) defence and security space strategies. Conceptually speaking, this division responds to two different levels within the strategic thinking: grand strategy and strategy. Importantly, this conceptual division aligns with the methodological framework set forth in this research. Despite the lack of a contemporary and agreed upon definition of these related terms [18, 19, 20, 21], "there is no longer a purely military definition of strategy" [20] or grand strategy. This indicates that there has been a shift from the Classicist tradition of grand strategy that focuses on the employment of military means to achieve national goals, to an International Relations approach that affirms that a state must use all the instruments of national power, military, and non-military, to protect and advance its long-term best interests. Hence, as Hooker suggests [22], grand strategy should be understood simply as "the use of power to secure state". Therefore, defined in this way, the term grand strategy would include those particular strategies intended to secure particular ends [18, 22].The grand strategy of a state is not defined by a single document or policy; rather it encompasses a "collection of plans and policies that comprise the state's deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state's national interest" [23]. In this context, national security strategies emerge as particularly relevant among these plans and policies. Although not synonymous with, national security strategies are closely related to grand strategy [22], since they provide a comprehensive and complete national security document that matches ways, means, and long-term ends. Based on the US legal framework, although it can be extrapolated to other cases, Pavel and Wendt [24] explain what the purposes of a national security strategy are: (i) to outline the President's vision for America's role in the world; (ii) to highlight the President's top national security priorities; (iii) to broadly guide the resource allocation for the national security related departments and agencies; (iv) to articulate to friend and foe alike the strategy and subsidiary national security policies of the United States; (v) to justify the national security departments' and agencies' budgets with the Congress; and (vi) to inform the public debate and garner public support for US national security efforts. It should be acknowledged that national security strategies, as public documents, serve not only to inform the domestic public but also to other international actors, including state and non-state actors [18], about the interests and intentions of the state. Therefore, a national security strategy assumes a pivotal role as an organizing principle, guiding policy formulation and resource allocation within the state, while also acting as a means to signal the state's potential behaviour under specific circumstances.

Table 1. National Security Strategies

Country	Title	Year	Abbreviation
United States	National Security Strategy [25]	2022	USNSS
United Kingdom	Integrated Review Refresh [26]	2023	UKIRR
France	National Strategic Review [27]	2022	FRNSR
European Union	Strategic Compass [28]	2022	EUSC
NATO	Strategic Concept [29]	2022	NATOSC

The second group of sources utilized in this study are defence and security space strategies. Based on a common contemporary definition of strategy, the evaluation of these documents will help us to understand how the actors involved in this study understand this particular domain and maintain a balance between ways, means, and ends; how they identify objectives; and how they match the resources and methods they have at their disposal to the objectives they want to achieve [21] in this particular area.

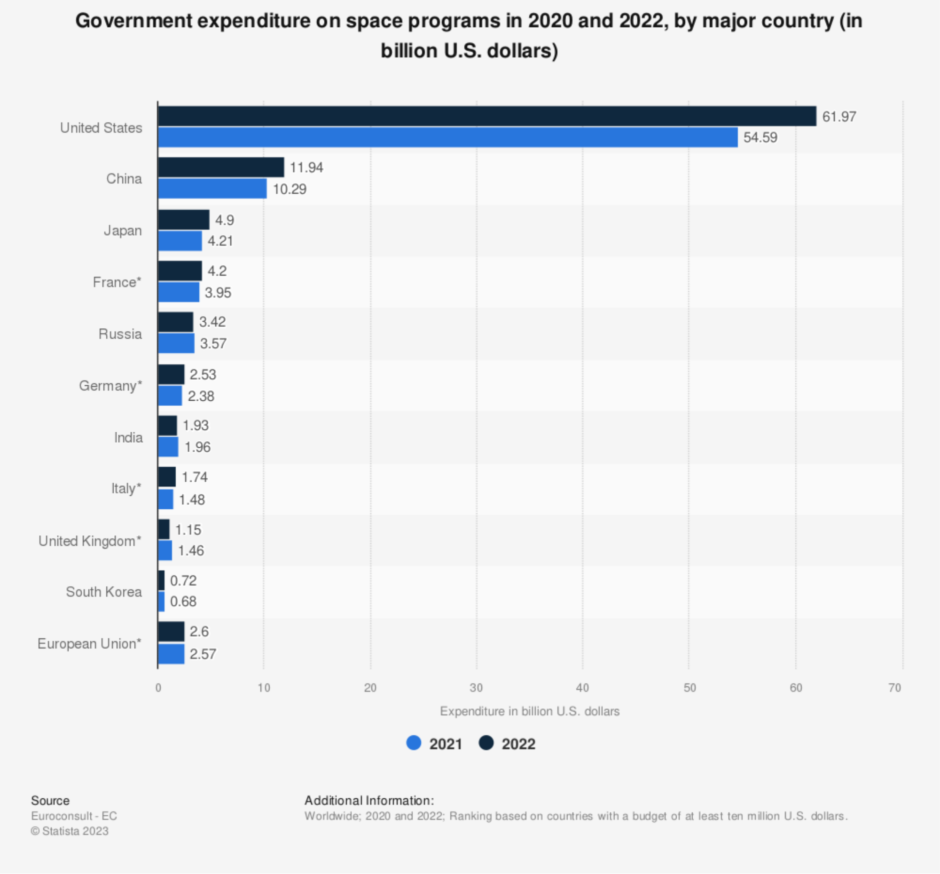
Therefore, an in-depth analysis of national security strategies is conducted in order to collect the necessary data to respond the RQs related to grand strategy such as the assessments of the international environment and the role played by the space and cyber domains in the targeted actors' strategic thinking. Whereas the data acquired from the defence and security space strategies will be employed to respond the RQs specifically related to the space domain, particularly how the actors address cybersecurity within it.

Table 2. Security and Defence Space Strategies

Country	Document	Year	Abbreviation
US	Defence Space Strategy [30]	2020	USDSS
UK	Defence Space Strategy [31]	2022	UKDSS
FR	Space Defence Strategy [32]	2019	FRSDS
EU	Space Strategy for Security and Defence [33]	2022	EUSpSSD
NATO	Space Policy [34]	2021	NATOSP

2.2.2. Sample

To be included in the sample for this study, actors must be Western states or international organizations, each possessing significant space budgets (as per Figure 1). The term “West” is employed not solely in its geographical sense, but also to characterize those countries that uphold liberal democracy as their form of government.


Government expenditure on space programs in 2020 and 2022, by major country (in billion U.S. dollars)

Source
Euroconsult - EC
© Statista 2023

Additional Information:
Worldwide; 2020 and 2022; Ranking based on countries with a budget of at least ten million U.S. dollars.

Figure 1: Government expenditure on space programs in 2020 and 2022, by major country (in billion U.S. dollars).

The actors selected in the sample represent the existing diversity within this group of countries. The United States is the hegemonic power of the West but is not a European country. France and the United Kingdom are part of Europe, but just France is a member state of the European Union. The inclusion of the EU and NATO obeys to the increasingly relevance that these two international organizations have in the international context, particularly in the defence and security field.

Regarding the space domain, the actors included in the sample have the highest budgets in the world devoted to space. Unlike the European Union, which has its own space programme, NATO does not possess space capabilities of its own, and is not aiming to develop these capabilities nor to become an autonomous space actor [34]. Despite this fact, NATO is part of the sample given the increasingly relevance that the defence and security realm has today, especially in the space domain. As the United States, the United Kingdom and France are members of NATO, evaluating the strategic documents released by this organization will provide important insights.

Finally, assessing the cyber domain from the security space perspective released by the selected actors also justifies the selection of the sample as all of them have recently published strategies related to cyber security (the US in 2023 [35, 36]; the UK in 2022 [37]; France in 2018 [38]; the EU in 2020 [39]; and NATO in 2023 [40]). It is therefore the case that all the actors included in the sample have published security strategy related to both the space and cyber domains.

3. Characterising the strategic environment

The main idea that underpins the assessments of the international environment provided by the actors involved in this research is that the international system, the open rules-based international order that was born after the Cold War and is characterised by the pivotal role of international organizations, multilateralism, and the interdependence between states and non-states actors, is evolving, leading to a deterioration of the international system itself, whose main principles are being contested by powerful competitors such as China and Russia, and their respective positions within it.

This evolution is explained mainly by two trends: the existence of a competition among the powers constituting the international system; and an increasing emergence of transnational challenges (climate change, food insecurity, diseases, and terrorism, among others) that must be collectively addressed. It is noteworthy that these two trends are not independent, but they reinforce each other. In this regard, the United States explicitly warns to the necessity to "understand how a more competitive world affects cooperation and how the need for cooperation affects competition" [25].

Although described with different adjectives ("strategic" by France, NATO, and the European Union; "systemic" by the United Kingdom; and "geopolitical" by the United States), all the actors coincide in pointing out not only that a growing competition among states is currently undergoing, but also the negative impact that this competition has on the nature of the international order. The relevance of this competition in the international environment is of immense magnitude as it is portrayed as "the most pressing strategic challenge" [25] or as "the most immediate and substantial threat to UK interests and will require an increasingly proportion of national security resources" [26]. Therefore, open conflict, even war, is a real possibility for which actors intend to be prepared. France is particularly clear in this respect as it includes as one of its strategic objectives to prepare a war economy plan in order to adapt its economy and industrial base to different geopolitical contexts [27].

3.1.Authoritarian versus democratic states: China and Russia

This strategic, systemic, or geopolitical competition encompasses states that challenge the international order, named authoritarian states, and those who share its basic principles and tenets, or democratic states, category to which all the actors involved in this research belong to.

The use of the concept authoritarian states or autocracies is broadly employed by all the selected actors to refer to the opposing group, with the exception of the European Union. Instead, the European Union uses the expression "the return of power politics" to describe those countries that "act in terms of historical rights [other actors, like the US and France, use the term revisionist] and zones of influence, rather than adhering to internationally agreed rules and principles and uniting to promote international peace and security" [28]. Moreover, the European Union acknowledges the existence of a "competition of governance systems accompanied by real battle of narratives" [28]. Therefore, it can be affirmed that, according to the documents reviewed, different systems of governance behaviour, not ideology, are the main elements that differentiate both groups.

Although, as said, this differentiation between autocracies and democracies is widely used, not all the actors consider these categories as a close dichotomy that can describe all the participants in the international system. Supporting this point of view, it can be found the case of the United States, who explicitly states that the undergoing competition is between democracies and autocracies [25]. A different approach is held by the United Kingdom, as it openly affirms that although "a growing convergence of authoritarian states are challenging the basic conditions of an open, stable and peaceful international order" [26], "today's international system cannot be simply reduced to 'democracy versus autocracy' or divided into binary, Cold War style blocs" [26]. These two different approaches also entail a different perception on who are the participants involved in this competition. Whereas the United States considers major powers as the main characters of this competition, other actors like United Kingdom and France underline the importance of "regional actors" in it [27], acknowledging the growing importance to the international affairs of "middle-ground powers" [26], i.e. Iran and North Korea [26].

In any case, what all the assessments of the international environment agree on is to identify Russia and China as the most prominent authoritarian states, although with important differences. As a result of Russia' actions in Georgia in 2008, the occupation of Crimea in 2014, and the illegal invasion of Ukraine in 2022, Russia is portrayed as a national, regional, and global threat. In this regard, the United Kingdom states that "the most pressing national security and foreign policy priority in the short-to-medium term is to address the threat posed by Russia to European Security" [26]. In the same vein, NATO affirms that Russia is "the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic" [29]. Meanwhile, the United States amplifies the risk posed by Russia signalling it as "an immediate threat to the free and open international system" [25]. Instead of describing Russia as a threat, the European Union refers to it as an aggressor who has violated international law and undermined European and global security and stability [28]. Equally, France does not use the term threat and it focuses on how Russia has moved from a more indirect approach towards conflict to engage in direct military confrontation [27].

The assessments on China vary in substance and language as China seems to represent a much more complex challenge than Russia. In this regard, it is noteworthy how the United States defines China as "the only competitor with both the intent to shape the international order and, increasingly, the economic, diplomatic, military and technological power to advance that objective" [25]. The relevant position in the international order and hence the complexity of the challenge posed by China is also reflected in the assessment that the European Union and the United Kingdom provide. The European Union affirms that China is a "partner for cooperation, an economic competitor, and a systemic rival" [28], while the United Kingdom portrays China as a national security threat, but also as an actor to engage with when necessary [26]. NATO adopts a more assertive position towards China as it reckons that the "PRC [People´s Republic of China] stated ambitions and coercive policies challenge our interests, security and values" [29]. France considers China a revisionist state whose main goal is to supplant "the United States as the world's leading power" and the Western influence [27]. For this purpose, France states, China is spreading its influence throughout the world using all the tools it has at its disposal: propaganda, military strength and espionage, economic and technological predation, and an assertive diplomacy.

Only two actors, the United Kingdom and France, warns about the consequences of further collaboration between China and Russia on their desire to challenge the international order. The United Kingdom sees this phenomenon as an "intensification of systemic competition" and does not encapsulate it in the deepening partnership between China and Russia, but also between Russia and other authoritarian states such as Iran [26]. France asserts that the shared objective of China and Russia to challenge the "Western influence, particularly in the context of the war in Ukraine, is giving rise to some kind of occasional cooperation" and warns that "the political, strategic and technological implications for global governance could be enormous" [27].

3.2. Competitive behaviour: use of hybrid strategies and technology

In addition to identifying and delineating the primary characteristics of authoritarian states, all national security strategies centre special attention on the behaviour of these states or, more precisely, the methods employed by these states (and, as underscored by the EU, non-state actors as well [28]) to advance their objectives within the ongoing strategic competition. Given the potential impact on actors' security and stability, it is important to note that these methods are categorized as "threats" on their own merit, not only because the potential malicious use that authoritarian states can make with them. Two terms are used to describe these methods: "hybrid strategies, tactics and campaigns" and "threats below the threshold of armed conflict". The

European Union, NATO, and France refers to hybrid strategies, tactics and campaigns, although France is the only actor who defines this concept. According to the FRNSR:

> France's main strategic competitors use hybrid strategies, deliberately ambiguous combinations of direct and indirect, military and non-military, legal and illegal, and often difficult-to-attribute means of action [27].

Therefore, encompassed by this concept, or closely interlinked with it, is an extensive and varied range of actions, including: malicious activities in cyberspace and space, disinformation campaigns, economic coercion, the instrumentalization of irregular migration, critical infrastructure disturbances, or the misuse of law to achieve political, economic, and military objectives (also referred as "lawfare" by the EU [28]). Furthermore, actors also agree on affirming that hybrid strategies aim to discredit democratic systems, targeting elections, processes, and institutions, or reduce their economic and national defence potential.

Although there are references to the terms "hybrid threat" and "hybrid conflict" in the UKIRR, the United Kingdom, as well as the United States, employ the term "threats below the threshold of armed conflict" to refer to the dynamic competition that is playing out across overlapping the "strategic arena over the military, economic, and political balance of power, rules and norms, and institutional architectures" [26]. The main challenge of this type of activities is, as Klein argues, that they may "complicate the invocation of mutual defence agreements, collective action by an alliance or coalition, or application of the inherent right of self-defence under either the standing or supplemental rules of engagement" [41].

Beyond their effects, national security strategies focus on the existing relationship between hybrid strategies and technology and how technology is transforming conflict. It is broadly acknowledged that the extensive use and effectiveness of the hybrid strategies and tactics is allowed and enhanced by the appearance of emerging and disruptive technologies. In fact, NATO affirms that these technologies are "altering the character of conflict" [29], while the European Union and the United States acknowledge that technology is transforming the nature of warfare and shaping military affairs [25, 28]. Nevertheless, the strategic importance of technology is not solely utilitarian, as it is also considered as an "arena" of global competition [25, 26, 29]. This is because all actors consider that achieving technological advantage and autonomy has become a strategic objective for competitors as well as for allies, affecting not just foreign policy, but essential domestic policies leading to develop and protect a more resilient, innovative, and competitive defence technological and industrial base.

This explains why technological and scientific innovation is regarded as a strategic objective, existing also a common understanding on what emerging and disruptive technologies are deemed crucial and, as a result, deserves increased investments. Among them, the following technologies are identified as critical by the selected actors: Artificial Intelligence and quantum computing [25, 26, 27, 28]; bio-technology (including bio-manufacturing and engineering biology), nano- technology, microelectronics and semiconductors [25, 26, 28]; and advanced telecommunications [25, 26].

4. Space and national security

The assessment of space within the national security strategies begins by acknowledging that space is an increasingly congested and contested domain [28], “subject to renewed competition” [27]. This assessment is grounded in the notion that competitors possess the enabling technology to impede actors’ unfettered access to space and undermine their space assets. In this regard, NATO says:

> Strategic competitors and potential adversaries are investing in technologies that could restrict our access and freedom to operate in space, degrade our space capabilities, target our civilian and military infrastructure, impair our defence and harm our security [29].

In addition to having the necessary technology, these assessments also acknowledge that competitors have already conducted malicious activities in the space domain [29], targeting allies and partners with “a broad set of tools and testing [their] resilience with the aim to diminish [their] security and actively undermine their secure access to space domain” [28]. Therefore, the selected actors uphold that space is an essential field where competitors are conducting hybrid strategies and tactics. It is noteworthy that when addressing the space domain, national security strategies refer to strategic competitors and potential adversaries in general. Only NATO and the Europan Union emphasize China’s role in space [28, 29]. Certainly, the United Kingdom refers to Russia’s direct ascent anti-satellite missile test that took place in November 2021 [26], but as an example of irresponsible behaviour is space.

As noted by NATO, competitors’ space technology could potentially not only restrict free access to space, but also compromise selected actor’s space capabilities, jeopardizing their critical infrastructure. In this context, France openly designates the development of space communications capabilities to detect, assess, and counter hybrid threats aimed at its critical infrastructure as a strategic objective [27]. This stems from the recognition that space capabilities are viewed as “strategic enablers”, that is, capabilities necessary to conduct a full range of missions and operations [28]. Hence, all national security strategies underline the importance of addressing the vulnerabilities of space systems and enhancing the resilience of space infrastructure.

Another important narrative about space in national security strategies is the close relationship between space and the rules-based international order they depict. NATO considers aggressive actions within space as a way “to subvert the rules-based international order” [29] and France affirms that “freedom of access to common spaces [including the space domain] is now threatened by challenges to the rules-based international order” [27]. This approach underscores the great importance attributed to international law for regulating activities in space, in a way that a threat to the international order is perceived as a threat to the freedom of access to the space itself. In this regard, the United Kingdom warns:

> Traditional multilateral approaches and defending the post-Cold War rules-based international system are no longer sufficient on their own. The UK will prioritise shaping activity across the strategic arenas where developments will be most consequential for our core national interests and international order [including the space] [26].

From this statement it can be induced that the ultimate strategic goal would not be the defence of the current international order as such, but to adapt it where necessary. Therefore, to influence the future norms and rules governing activities in common domains, including the space, is a highly important objective to pursue by all the selected actors. For the United Kingdom, "shaping the international environment" is one of the four pillars sustaining the strategic framework introduced by the UKIRR [26]. For the United States, "shaping the rules of the road" of closely linked areas to space such as technology, cyberspace, and trade and economics is understood as a "global priority" [25]. The European Union stresses its will to, in line with the United Nations, "work on the development of norms, rules and principles of responsible behaviour in outer space" [28]. And NATO also defends the applicability of international law to the promotion of responsible behaviour in space and cyberspace [29].

It is noteworthy that strengthening the rules-based international order is not just a mere formal goal outlined in these strategic documents, but several actions have been taken by the selected actors in this regard. Already in 2014, the EU proposed a Draft International Code of Conduct for Outer Space Activities, a non-legally binding, voluntary international instrument aimed at building norms of responsible behaviour in space activities [42]. More recently, in 2020 and 2021, the United Kingdom sponsored two significant resolutions within the United Nations on reducing space threats through norms, rules and principles of responsible behaviour by which the General Assembly (UNGA) encourages Member States "to study potential threats and security risks to space systems (…), characterize actions and activities that could be considered responsible, irresponsible or threatening (…), and share their ideas on the further development and implementation of norms, rules and principles of responsible behaviours and on the reduction of the risks of misunderstanding and miscalculations with respect to outer space" [43]; and convenes an open-ended working group to make recommendations on norms, rules and principles of responsible behaviours relating to threats by states to space systems [44]. In October 2022, France co-sponsored a resolution calling on all States "to commit not to conduct destructive direct-ascent anti-satellites missile tests" (DA-ASAT tests), which was adopted in the United Nations General Assembly by a very large majority [45] (155 countries voted in favour, including the UK, the US, France, and the EU; 9 against, including China and Russia; and 9 abstentions, including India and Pakistan). It is interesting to point out that this resolution was adopted following an unilateral moratorium on DA-ASAT tests pledged by the United States in April, 2022 [46]. Finally, in addition to the technology aspect and the challenges to the norms and rules governing the space, national security strategies also highlight the strong security and defence implications of competition in space [28]. These security and defence implications, which are an expression of the strategic relevance of space, are interlinked to the technology aspects of the competition in this domain, as technology provides new means to undermine secure access to space. As noted before, the United States recognizes that “emerging technologies transform warfare and pose novel threats to the US” and, consequently, the United States “is investing in a range of advance technologies including applications in cyber and space domains” [25]. Within the Pillar 2 of the United Kingdom strategic framework named “deter, defend and compete across all domains”, the United Kingdom highlights the importance of space forces as part of its approach to deterrence and defence [26]. The European Union openly addresses the issue of Defence in Space asserting the need to develop cutting edge capabilities “to improve its access to space and protect its space based assets”, including technologies related to Space Based Earth Observation (EO), Space Situational Awareness (SSA) and space based communication and navigation services [28], as well as a security and defence space strategy (which was released on March 2023, a year after the publication of the EUSC). Finally, the strategic relevance of space and its security and defence implications are reflected by the fact that NATO has concluded that any “hostile operations to, from, or within space could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty” [29].In order to be able to compete in this domain, all actors admit that international cooperation among allies and partners will be key in order to confront potential adversaries and rivals and, therefore, should be strengthen.

5. Defence and space security

5.1.The defence and security space strategies are built on the space environment assessment provided by the national security strategies. As noted, technology is understood as the main driver of the space environment transformation. Technology advances, mainly led by the private sector, have lowered production costs, and increased what can be done in space, resulting in a growing dependence on space assets and the emergence of new state and non-state space actors. Consequently, as space has become more critical, space assets could become a high priority target to potential adversaries and malicious actors [34], which could lead to potential disruptions, denials, and degradation of both access to and utilization of space.Threats in space

As the European Union puts it "space threats are intentionally hostile activities through counterspace capabilities" [33]. There is a common understanding on what these capabilities are and how they can affect space systems. First, counterspace capabilities can affect the entire structure of space systems, i.e. the space segment; the ground segment; and the data links between them. It is noteworthy that beyond space systems, the European Union warns that counterspace capabilities can also target "the space sector as a whole, including the underlying supply chains" [33]. Second, depending on what the target is, counterspace capabilities can disrupt, degrade, deceive, deny, or destroy space systems; or can be used to inspect, manipulate, eavesdrop, or intercept data. These effects can be reversible or irreversible. Third, depending on their form, counterspace capabilities can be: (i) kinetic: if the capability produces a destructive physical effect in the space asset (i.e. directs ascent anti-satellite missile, on orbit anti-satellite system, laser electro-magnetic wave); (ii) non-kinetic: if the capability does not produce a destructive physical effect (dazzling and jamming of space assess); (iii) electronic: capabilities which interfere the radiofrequency spectrum; and (iv) cyberattacks. Although no space specific, France also refers to "conventional threats", such as sabotage, malicious acts against ground infrastructure and the targeting of energy systems [32], in its space threat assessment.

In addition to the threats, defence and security space strategies also identify safety risks that on-orbit assets face in space. These risks are mainly associated to space weather and space debris.

5.2. Threats actors in space

Despite the common identification of counterspace capabilities as threats, not all defence and security space strategies qualify states possessing these capabilities as such. This becomes particularly compelling when assessing the role of China and Russia in the space domain. France states that Russia and China, but also the United States and India, have developed kinetic capabilities, whose employment could generate large amounts of debris [32], but it does not refer to these states as threats. Similarly, the European Union acknowledges that Russia and China have developed "capabilities to target critical space infrastructure" but, although it mentions Russia's anti-satellite weapon test in November 2021 and China's growing presence in space as a way to pursue its geopolitical agenda [33], it neither describes them as threats. In the same vein, NATO merely indicates that "a number of nations are developing counter-space and anti-satellite system" using a footnote to explain that China and Russia have advanced programmes, and "Iran and North Korea and some other nations also have some indigenous counter-space capabilities" [34]. The United Kingdom and the United States, however, use a more assertive language. The United Kingdom portrays China and Russia as "examples of international threats" [31] and the United States literally affirms that "China and Russia present the most immediate and serious threats to U.S. space operations, although threats from North Korea and Iran are also growing". The United States justify this statement not only because China and Russia possess counterspace capabilities, but also because they have the strategic intention and have developed doctrine (understood as "the fundamental principles by which the military forces guide their actions in support of their objectives" [47]), organizations and military strategies that aim to "reducing U.S., allied, and partner military effectiveness and for winning wars" [30]. In fact, the United States claims that "China and Russia have weaponized space" and "have transformed space into a warfighting domain" [30].

It is important to highlight that the assessments on China and Russia focus on their capabilities to disrupt or impede access to space, but they do not warn about the possibility that such increasing counterspace capabilities may challenge the US-hegemonic position in the space order. This is because, as argued by Stroikos [48], the United States not only remains the space greater power in terms of material (the U.S. operates by far the largest number of satellites) and ideational influence (U.S. space initiatives such as the Artemis Accords gather much more international support than the Chinese ones), but also leads and benefits from today's nature of space power, which is not state-centric anymore, but net-centric, based on the increasing role of the commercial sector and military space alliances, as suggested by Moltz [10].

Finally, as noted, all defence and security space strategies address the issue of state actors possessing counterspace capabilities, but just NATO posits that non-state actors could also represent a threat, including terrorist organizations, as they could conduct cyberattacks and jamming satellites' signals [34]. Regarding to non-state actors' space activity, it is worth mentioning how the role of New Space is perceived by different actors, particularly by France. The emerging private space sector is generally described as a one of the most important trends within the space, an area which was previously delimited to states. However, just France seems to appreciate the risks and challenges, and even threats, that this phenomenon represents and not only to its national space industry. France warns that "undercover of civilian objectives, states or private actors can openly finance potential anti-satellite technology" [32], which involves a grimmer characterization of the strategic environment than that provided by the rest of the selected actors

5.3. Responding to threats in space

As observed before, all the actors involved in this research share a common understanding of the threats endangering the space domain, albeit with nuanced variations. However, the approach and lines of action formulated to address them differ. These discrepancies can be attributed to the differing nature and extent of their space capabilities. The United States' strategic approach aims to increase "its spacepower capacity (. . .) to ensure space superiority and secure Nation's vital interests" [30]. Therefore, the major concern of the United States is not just to adopt new space capabilities, but to adapt its defence space enterprise to the current strategic environment [30] and "to transform its approach to space from a support function to a warfighting domain" [30]. France, which considers itself a genuine civil and military space power [32] and possesses extensive space capabilities, seeks to adapt its armed forces in order to guarantee its capacity to act in space [32]. The United Kingdom's vision on space stated in the UKDSS is "to be a meaningful actor in the space domain, securing UK interests alongside our allies and partner to ensure operational freedom in space [31]. The European Union, which owns and operates a civilian space programme, aims to protect, and enhance the resilience of its space assets and services and prepare them to support defence and security initiatives.

Despite their differences as space powers, some common trends can be found among the objectives and lines of action formulated in the defence and security space strategies.

5.3.1. Enhancing the protection and resilience of space systems

This line of action widens its scope in order to include not only the protection and reliance of space assets, but also the space sector as a whole. Regarding the former, the defence and security space strategies focus on the development of capabilities that are able to "make space assets stronger, protect them better, extend their lifetime, or replace them quickly" [33], such as: self-protective infrastructure on-orbit, terrestrial and cyber infrastructure against potential threats from Earth (electromagnetic aggressions or cyberattacks), launch capabilities, space situational awareness services, in-orbit servicing and secured cloud dedicated to space services. Considering the pivotal role played by New Space in delivering these types of services, especially in satellite and constellation manufacturing, satellite communication, and launch operations, it is recommended to foster increased collaboration between the armed forces and commercial space service providers. [27, 31, 33]. The resilience and protection of the space sector is a particular concern of the European Union, which seeks to reduce its strategic dependencies on third countries, boost the resilience of critical industrial value chains, and protect its supply chains, and therefore enhance its strategic autonomy [28, 33]. In order to do so, the European Union proposes the establishment of new industrial alliances related to technologies that are relevant for space and defence; the integration of space with in relevant EU policies and initiatives, such as on quantum technologies, or artificial intelligence; to ensure access to raw advanced, and processed materials and semi-conductors; and to better assess the risks associated to foreign direct investments (FDI) transactions in the space sector and the procurement of space components.

As previously noted, France is aware of the risks that its national space industry, as well as the European space industry, are currently facing as a consequence of the New Space developments and the "potential return to the global markets of major American players" [32]. That is why France encourages to consolidate the European Defence and Technological Industrial Base mainly through mergers on a continental scale in the satellite, and related services, industry [32].

5.3.2. Responding to space threats

The approach adopted within the defence and security space strategies towards space threats is mainly preventive. First, this approach focuses on the need to anticipate, detect, seek out, characterize, identify, analyse, and attribute a threat in the space domain in order to react and respond to it in a timely, proportionate, coordinated, and coherent manner [31, 33]. In order to do so, it is necessary to develop the sufficient space domain awareness (SDA) capabilities, including SSA and space surveillance and tracking (SST) capabilities, which are addressed as key. Second, defence and security space strategies are also used to communicate to potential adversaries that transgressions against space systems will not be left unaddressed. France, in accordance with international law and the UN Charter, states that in case of an unfriendly, wrongful, or aggressive act in space it reserves the right to take retaliatory measures, countermeasures, or exercise its right of self-defence [32]. NATO points out that attacks to, from, or within space could trigger North Atlantic Treaty article 5 that regulates collective defence [29]. And the EU affirms that "any Member State can invoke the mutual assistance clause (Article 42.7 of the Treaty of the European Union) should a space threat or incident amount to an armed attack on its territory" [33]. Third, the responses to be implemented in the event of an attack on a space system encompass both military and non-military measures. Among the non-military measures, the European Union points out the possibility to adopt responses at technical, diplomatic, and economic level [33]. Regarding the military measures, there is a general recognition that space is an integral component of deterrence [30, 31, 33]. However, specific references to the utilization of military means are limited. Just NATO refers to "a range of potential options, for Council approval, across the conflict spectrum to deter and defend against threats to or attacks on Allies' space systems" [34]. Despite this, it is clear that the use of military measures to respond to space threat is not a lesser issue. The problem is that, as a new operational domain, there is a lack of doctrine, operational and tactical concepts, and spacepower expertise that all the state actors involved in this research attempt to address in their respective defence and security space strategies through the establishment of space doctrine, organizations, and space exercises.

5.3.3. Supporting military operations

Even though space has become an independent operational or warfighting domain (together to land, sea, air, and cyber), the main function of space is to provide support to military operations in other domains. This is acknowledged by France when asserts that "the first priority of space strategy is to enhance the capabilities already used to support land, sea and air operations" [32].

Therefore, this is a topic addressed by all defence and security strategies, existing also a common understanding on the type capabilities that should be enhanced. These include Position, Navigation and Timing (PNT), Satellite Communications, Intelligence, Surveillance and Reconnaissance (ISR), SDA and SST, EO, Space-based monitoring atmospheric and Early warning capabilities.

However, as the United States and the United Kingdom state, the important strategic goal addressed in the defence and security space strategies of these states is to supersede the concept of joint operations, in which every domain independently support each other, and integrate space capabilities into all forms of military power [30], or Multi-Domain Integration, as the United Kingdom puts it [31]. Furthermore, this idea of integration is not a concept that only applies to national military forces. Operational integration of space capabilities with allies and partners, which entails enhancing space systems interoperability, is an objective sought by the United States [30]. In this regard, France goes a step further, affirming that the aim should be to consolidate an allied military space community [32].

It is worth noting that just one selected actor is concern with the effects that dependence on space systems have on the armed forces. Although possessing the most advanced space capabilities is critical, France aims at the necessity to strengthen the armed forces' capacity to act without space support [32] in case space infrastructure was disrupted in conflict.

5.3.4. Shaping the strategic environment

The lack of an updated legal framework regulating space and space activities is perceived as a source of instability in the space domain. Nonetheless, as reflected in Sections 3 and 4, the adoption of agreed international laws in the space domain is virtually impossible as the rules-based order is under a fierce strategic competition. That is why the defence and security space strategies support the adoption of standards, principles, or norms of appropriate or responsible behaviour [30, 31, 32, 33, 34] in order to avoid miscalculations that could lead to an open conflict in space.

It is interesting to note two different aspects in the United States approach towards this line of action. First, the United States is the only actor that openly states that the adoption of these norms and rules must be "favourable to U.S., allied, and partner interests" [30]. Although this statement is inherently true from an individual strategic perspective, the way it is formulated reinforces the idea that norms and rules do not respond to general or common perceptions, but are concocted in order to protect some interests and no others. Moreover, despite the fact that allies and partners' interests are included in such vision, the aim to shape the strategic environment may involve tensions among allies. Space Traffic Management (STM), defined as the "means and rules to access, conduct activities in, and return from outer space safely, sustainable and securely" [49], is a field where these tensions may potentially arise as the United States and the European Union have their own approaches. In 2018, the U.S. government published the Space Policy Directive-3 establishing a national STM policy [50], stating that "U.S. regulatory agencies should, as appropriate, adopt these standards and best practices in domestic regulatory frameworks and use them to inform and help shape international consensus practices and standards". In turn, the European Union released in 2022 a Joint Communication called "An EU Approach for Traffic Management" [49]. Although the EU explicitly conveys that it "will explore ways of ensuring closer cooperation and mutual interoperability and complementarity on STM with the US", the main goal is to preserve EU interests in a non-regulated strategic field and to promote this approach globally. Although in the past the United States and the European Union have reached agreements in important competing issues such as the interoperability between their own satellite-based navigation systems, the EU Galileo and the U.S. Global Positioning System (GPS) [51], the geopolitical implications of leading the definition of STM rules and norms makes the possibility of reaching an agreement in this regard more difficult.

Second, in addition to the adoption of norms of responsible behaviour, the United States includes the need to "inform international and public audiences of growing adversarial threats in space", as a way to shape the strategic environment and legitimize its space strategy and policy.

5.3.5. Enhancing cooperation and collaboration

Cooperation is a shared strategic goal among all defence and security space strategies, but also a cross-cutting principle affecting all the objectives set out in them [30, 31]. Consequently, as the USDSS points out, further cooperation is expected with different stakeholders (allies and partners, industry, research institutions, and government departments and agencies) in a wide range of fields, such as: information sharing, space policy, standards and norms of behaviour, research, development, and acquisition [30]. From a purely military perspective, France acknowledges that although military space cooperation has traditionally focused on exchanges of capabilities with European partners, in the future it will also apply to space operations, where the United States is a key partner [32]. The selection of the allies and partners whose relationship should be strengthened or expanded is based on strategic considerations. In this regard, France prioritizes cooperation with European partners (especially with Germany, Italy and the United Kingdom) in fields such as threat assessment, policy and strategy, and space industry; with the European Union and NATO; and with the following partners outside Europe: the United States, for its extended SSA capabilities and its expertise in military space operations; India, for the long-standing cooperation in the civilian space sphere, especially launchers; Japan, in the space surveillance sector; and Canada and Australia [32]. The United Kingdom will strengthen its bilateral and multilateral relation with the member of Five Eyes (particularly the United States) and NATO [31]. The European Union, whose main aim is to promote responsible behaviour in space, seeks to bolster its relationship with the United Nations, the United States, NATO, and other third countries such as Norway, Canada, and Japan [33]. Cooperation with potential adversaries is not excluded, but it is limited to space security dialogues, including the adoption of norms of responsible behaviour in space. It is interesting to note, that the EU Approach for STM [49] follows the same logic, as it seeks to collaborate and promote internationally its own norms and guidelines in four ways: contributing to a multilateral STM system within the framework of the UN; forging regional partnerships with the understanding that "STM relies on a certain level of trust among space-faring nations"; strengthening the cooperation with the US, which is recognized as the most advanced actor upon STM; and, finally, pursuing an active diplomacy related to STM with third countries including civil matters (such as operational safety and long-term sustainability of the orbital environment), but also related security and defence aspects of STM.

6. Cybersecurity and space

6.1. National Security Strategies

Although none of the selected national security strategies provides a definition of cyber domain, this term is used together with cyberspace. According to the NATO Glossary of Terms and Definitions [47], the term “cyberspace” refers to

> The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.

The assessment of cyber domain or cyberspace within national security strategies is similar to the assessment of the space domain provided in these documents. Cyber domain is portrayed as a highly contested common domain, where a strategic competition is taking place, and competitors are able to threaten the free and secure access to it. In this regard, NATO states that cyberspace is a domain that is contested all times, where competitors conduct all kind of malign activities such as degrading critical infrastructure, interfering with government services, extracting intelligence, stealing intellectual property, or impeding military activities [29]. However, the main difference between both assessments is that cyber is addressed also as a threat and not only as a field of strategic competition. Indeed, cyber capabilities and cyberattacks are perceived as a highly complex and dangerous threat for several reasons: First, the growing dependence of modern societies on digital technologies have potentially increased the civil and military vulnerabilities that can be exploited by cyber tools. National health systems, power grids, pipelines, financial institutions, and critical infrastructures are just a few examples of assets targeted by cyberattacks pointed out in the national security strategies. In addition to this, the fact that cyber capabilities are also considered strategic enablers to conduct different military operations in all domains makes cybersecurity and cyber defence a strategic priority in all national security strategies.

Second, the level of sophistication and proliferation of cyberattacks. The growing dependence on digital technology has also an impact on the development of increasingly sophisticated cyber capabilities and proliferation of cyberattacks. As national security strategies highlight, cyber operations have become an essential tool of hybrid strategies and tactics (also referred as “threats below the threshold for armed conflict” by the United Kingdom), or closely linked to them, conducted by competitors [25, 27, 28]. The difficulty to track and attribute cyberattacks and the potential harm that can provoke has led to some actors to define cyber as a "weapon" that is employed to defend strategic interests in the context of geopolitical tension [27].

Third, the diverse nature of the malicious competitors. The threat posed by cyberattacks is not just a matter of state actors (among which Russia and China occupy a prominent place according to national security strategies). Cybercrime and the use of disruptive cyberattacks by non-state actors, both directly or as proxies of state actors, are perceived as a strategic challenge for national security [25, 27].

6.2. Defence and Security Space Strategies

The approach taken in addressing the cyber domain within the defence and security space strategies primarily centres on the cybersecurity perspective. Cyberattacks are considered one of the most probable threats that imperil space systems [32] for the following reasons:

First, the entire space infrastructure heavily relies on software components, making it particularly vulnerable to cyberattacks [32, 33]. This implies that effects of such attacks can vary, ranging from the total loss of control of payload or even the platform itself [32] to the denial, disruption, or deception of satellite data [31].

Second, even though conducting cyberattacks "require precise knowledge of the target's technical parameters" [32], an increase of such attacks on space systems is expected. This is explained by the availability of cyber capabilities to both state and non-state actors, including terrorist organizations [34], and because cyberattacks are very difficult to attribute [32]. Therefore, as the European Union states, analysing behaviours in the cyber domain, in addition to behaviours in orbit and on the ground, is essential to assess space threats [33].

As a fundamental element of space threat assessments, the cyber domain also plays a crucial role in the actions aimed at bolstering the resilience of space systems and services [31, 33]. This is an important concern particularly to the European Union, which expects that the implementation of the EU cybersecurity frameworks, such as the NIS 2 Directive and the Cyber Resilience Act, "will incentivise the uptake of cybersecurity requirement for critical digital products that are used in space". Moreover, as the space private sector is an increasing important space service provider, the European Union intends to "facilitate the exchange of best practices among commercial entities on resilience measures including cyber-related ones" [33].

7. Concluding remarks

The results of this study confirm a common approach among all selected actors in addressing the issues raised by the research questions. As seen, similar narratives to describe the current international environment and its underlying trends have been identified.

Additionally, the results of this study also show that all the selected actors share a common understanding on the strategic importance that space currently plays and how the strategic competition pervades the space domain. The space assessment provided by the strategy documents reviewed shows a similar approach towards the identification of space threats and risks; the implications to their national interests of the development of more complex counterspace capabilities by their competitors and adversaries; the key role of cybersecurity within the space domain; the type of responses that should be adopted in order to confront space threats; the type of technologies that should be developed to improve the resilience and protection of space systems; and the cutting-edge technologies that need to be bolstered in order to keep pace with the technological competition that is currently undergoing. Among these common approaches, one should be highlighted: the strategic importance that all selected actors provide to international cooperation as an essential line of action to address all kind of space issues.

International cooperation in space has been deeply explored from an International Relations (IR) theory perspective, particularly by liberalism [52]. Unlike realism, which envisions space as "an arena for growing competition based on an inevitable quest for power" [53], liberals consider international cooperation as a driving force behind the space exploration and exploitation, even among superpowers [54], or, more broadly, as "the chief pattern of interaction in the practice of international space relations" [52]

This explains why liberalism pays much attention to the development of multilateral cooperation, particularly to the role that institutions, such as the United Nations, play in this regard. This is consistent not only with the goals stated in the reviewed strategic documents, but also with the proposals that these actors have made in international fora, such as the EU Draft International Code of Conduct for Outer Space Activities. Moreover, as the current international system is grounded in liberal principles, and the selected actors see themselves as upholders of such system, they tend to promote their proposals through the existing multilateral channels or even suggest to create new ones, as the recently established UN OEWG on rules on reducing space threats through norms and principles of responsible behaviour shows.

However, despite the undeniable success of cooperative endeavours in space such as the International Space Station, the justification behind this cooperative endeavour has been primarily political [1], indicating that beyond practical considerations, there is a political rationale underpinning space cooperative efforts.

The main political motivation behind the call to enhance international cooperation in space security and defence among the actors in this study is driven by the assessment of the international environment and, consequently, by the ongoing strategic competition between those states that support the current international order and those that aim to change it. Consequently, the existing strategic competition alters the dynamics of international cooperation: further international cooperation is expected, but it is likely to occur only among national security allies and partners. This rationale also emerges in the context of the UN, where China and Russia, the most prominent contenders of the international liberal order, voted against the UNGA resolution calling to ban DA-ASAT tests, while the US and all its allies voted in favour. This polarization within the international space order questions the possibility of updating its international legal framework because any proposal in this regard is interpreted as a way to limit the freedom of action in space of the other.

Moreover, while not strictly within the field of security and defence, these evolving dynamics of cooperation and competition in space are currently exemplified by two lunar cooperative platforms: the US-led Artemis Program and the China-led International Lunar Research Station (ILRS). As of May 2024[1], 40th states have signed the Artemis Accords, a pre-requisite to participate in the Artemis Program, including the United Kingdom and France. While China and Russia, through their space agencies China National Space Agency (CNSA) and Roscosmos, announced at the 2021 Global Space Exploration Conference a public invitation to participate and cooperate to all interested countries in the ILRS project [55].

Wu suggests that the involvement of the ESA, the European Union and their member states in the ILRS is highly likely as it could alleviate the impact of sole dependence on the United States in lunar exploration activities [56], but her assessment does not fully consider the influence of strategic competition on such decisions, nor the possibility that "the Artemis Accords can be seen as a U.S. diplomatic tool using the Artemis programme as a lever to push U.S. position on the international scene" [57]. This could potentially hinder signatories of the Artemis Accords from participating in the ILRS initiative.

Naturally, enhancing international cooperation among allies, partners, and like-minded actors, as proposed by the security and defence space strategies, could play a pivotal role in achieving the main strategic objectives identified in this study, namely: enhancing the protection and resilience of space systems; effectively responding to space threats; proving support for military operations; and shaping the strategic environment. In fact, through further international cooperation improvements in the interoperability among different space systems while bolstering their resilience can be achieved [58]. This not only benefits the involved actors but also indirectly imposes costs on potential adversaries, since, in case of an open conflict in space, they would find more difficulties in disrupting the space systems of a given actor and would need to prepare to confront opposition not only from the targeted actor but also from its allies [59].

However, the dual-use nature of space technologies and the adoption of strategic competition as the main driver of this kind of segmented international cooperation entails the impossibility of addressing collective problems that affect the entire international community, such as space debris. And, as West suggests, it could also further escalate military tensions and even conflict in outer space [58].

Despite the opportunities and challenges associated with this limited cooperation among national security allies and partners, it is crucial to bear in mind that strategies are crafted to match means with ends and advance national interests. Therefore, international cooperation, whether within a competitive framework or not, will only materialize if it aligns with and serves these national interests. This is important because all targeted actors underscore the need for enhanced cooperation in areas where such cooperation is inherently challenging due to the national industrial and economic interests involved.

[1] https://www.state.gov/artemis-accords/

One of the shared objectives included in the defence and security space strategies is bolstering the defence and industrial technological base, including supporting New Space companies. In addition to increasing public investments, the targeted actors seek to improve national procurement processes, export control regulations, and operational standards related to space activities aiming to avoid technology dependence with third parties, and protect supply and supply chains. The result is an approach towards national "protectionism" that has the potential to hinder international cooperation.

"Standards" setting serves as a prime example of this tension. While an international approach to standardization has the potential to improve the interoperability of space systems, it can also be employed as part of a broader strategy to establish market dominance [60]. In this context, it may act as an economic incentive to discourage cooperation, becoming a point of concern even among allies[61], as the different STM regimes proposed by the United States and the European Union may indicate

Several international space security policy topics have arisen throughout this study that could benefit from new research. Specifically, as this study provides a fixed picture of the strategic narratives employed by the selected actors for describing the role that space plays within their strategic thinking, as well as how they address cybersecurity in the context of space, new research could analyse how these narratives have evolved from previous strategic documents or will evolve in the future, or whether national strategic narratives are aligned with the narrative employed by the international organizations of which they are part. From different IR theories' perspective, new research could provide useful insights about what are the main drivers (domestic, systemic, both?) behind the strategic thinking of the involved actors. Additionally, as international cooperation has emerged as one of the essential lines of action to address all kind of space issues, future research should delve into the possibility of further cooperation particularly among allies, given the potential tensions that may arise among their initiatives to shape the strategic space environment. Related to this, and from the EU perspective, it would be promising to look into how the fact that the major space EU actors have signed the U.S. Artemis Accords may influence future EU Space Law.

References

[1] M. Sheehan, The International Politics of Space, Routledge, 2007.

[2] B. Dobos, Geopolitics of the Outer Space. A European Perspective, Springer, 2019.

[3] L. Dawson, The Politics and Perils of Space Exploration. Who will Compete, Who Will Dominate? Springer, 2021.

[4] B. E. Bowen, War in Space. Strategy, Spacepower, Geopolitics, Edin- burgh University Press, 2020.

[5] B. Einhorn, "It's Wrong!": Top Chinese Scientist Says India's Moon Landing Not Even Close to South Pole, Time (2023). URL https://time.com/6318208/chinese-scientist-questions-india-moon-landing-s

[6] High Representative of the EU, Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, Council of the EU. Press Release (2022). URL https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russia

[7] R. Iyengar, Why Ukraine Is Stuck with Elon (for Now), Foreign Policy (2022). URL https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-

[8] J. Pennington, Starlink in use on all front lines, CNN (2023). URL https://edition.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-cri

[9] D. Baiocchi, W. Welser IV, The Democratization of Space: New actors need New Rules, Foreign Affairs, May/June 2015. https://www.foreignaffairs.com/articles/space/2015-04-20/democratization-space

[10] J.C. Moltz, The Changing Dynamics of Twenty-First-Century Space Power, Strategic Studies Quarterly, Vol. 13, No. 1 (Spring 2019), 66-94. URL: https://www.jstor.org/stable/10.2307/26585375

[11] H. A. M. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten national cyber security strategies: A comparison, in: Critical Information Infras- tructure Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 1–17. doi: https://doi.org/10.1007/978-3-642-41476-31.

[12] A. J. S. Craig, R. A. I. Johnson, M. Gallop, Building cyber- security capacity: a framework of analysis for national cybersecurity strategies Journal of Cyber Policy 7 (3) (2022) 375–398. doi: https://doi.org/10.1080/23738871.2023.2178318.

[13] M. Adriaensen, C. Giannopapa, D. Sagath, A. Papastefanou, Priorities in national space strategies and governance of the member states of the European Space Agency, Acta Astronautica 117 (2015) 356–367. doi: https://doi.org/10.1016/j.actaastro.2015.07.033. URL https://www.sciencedirect.com/science/article/pii/S0094576515003148

[14] D. Sagath, A. Papadimitriou, M. Adriaensen, C. Giannopapa, Space strategy and governance of ESA small member states, Acta Astronautica 142 (2018) 112–120. doi:

https://doi.org/10.1016/j.actaastro.2017.09.029. URL https://www.sciencedirect.com/science/article/pii/S0094576517307543

[15] D. Sagath, C. Vasko, E. van Burg, C. Giannopapa, Development of national space governance and policy trends in member states of the European Space Agency, Acta Astronautica 165 (2019) 43–53. doi: https://doi.org/10.1016/j.actaastro.2019.07.023. URL https://www.sciencedirect.com/science/article/pii/S0094576519311920

[16] A. Papadimitriou, M. Adriaensen, N. Antoni, C. Giannopapa, Perspective on space and security policy, programmes and governance in Europe, Acta Astronautica 161 (2019) 183–191. doi: https://doi.org/10.1016/j.actaastro.2019.05.015. URL https://www.sciencedirect.com/science/article/pii/S0094576518303485

[17] A Miskimmon, B. O'Loughlin, L. Roselle, Forging the World: Strategic Narratives and International Relations, Royal Holloway, 2012, https://pureadmin.qub.ac.uk/ws/portalfiles/portal/147369822/Forging_the_World_Working_Paper_2012_Final.pdf

[18] T. Balzacq, P. Dombrowski, S. Reich, Comparative Grand Strategy: A Framework and Cases, Oxford University Press, 2019.

[19] T. D. Biddle, et al., Strategy and Grand Strategy: What Students and Practitioners Need to Know, Strategic Studies Institute, US Army War College (2015). URL http://www.jstor.org/stable/resrep11726

[20] H. Brands, The New Maker of Modern Strategy. From the Ancient World to the Digital Age, Princeton University Press, 2023.

[21] L. Freedman, Strategy: A History, Oxford University Press, Oxford, 2013.

[22] R. Hooker, The Grand Strategy of the United States, National Defense University Press, 2014.

[23] P. Feaver, What is grand strategy and why do we need it? Foreign Policy (2009). URL https://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-nee

[24] B. Pavel, A. Wendt, Purposes of national security strategy, Atlantic Council (2019). URL https://www.atlanticcouncil.org/content-series/strategy-consortium/purpose-of

[25] US Government, National Security Strategy, Strategy Document (2022). URL https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF

[26] UK Government, Integrated Review Refresh. Responding to a more con- tested and volatile world, Strategy Document (2023). URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/at

[27] French Government, National Strategic Review, Strategy Document (2022). URL https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf

[28] European Union, Strategic Compass for Security and Defence, Strategy Document (2022). URL https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[29] NATO, Strategic Concept, Strategy Document (2022). URL https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[30] US Government, Defence space strategy, Strategy document (2020). URL https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020DEFENSESPAC

[31] UK Government, Defence Space Strategy: Operationalizing the Space Domain, Strategy Document (2022). URL https://assets.publishing.service.gov.uk/media/61f8fae7d3bf7f78e0ff669b/20220

[32] French Government, Space Defence Strategy, Strategy Document (2019). URL https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2020/08/f

[33] European Union, European Union Space Strategy for Security and Defence, Strategy document (2023). URL https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy

[34] NATO, NATO's overarching space policy, Strategic document, NATO (2022). URL https://www.nato.int/cps/en/natohq/officialtexts190862.htm?selectedLocale =en

[35]US Government, National Cybersecurity Strategy (2023), Available from: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[36]US Government, DoD Cyber Strategy (2023), Available from: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[37] UK Government, Cyber Security Strategy. Building a cyber resilient public sector (2022), Available from: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[38] French Government, Strategic Review of cyber defence (2018) Available from: https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf

[39] EU, The EU's Cybersecurity Strategy for the Digital Decade (2020), Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[40] NATO, NATO's approach to cyber defence (2023), Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm#defence

[41] J. J. Klein, Fight for the Final Frontier: Irregular Warfare in Space, Naval Institute Press, 2023.

[42] European Union, Draft International Code of Conduct for Outer Space Activities, March 2014, Available from: https://www.eeas.europa.eu/sites/default/files/space_code_conduct_draft_vers_31-march-2014_en.pdf

[43] United Nations General Assembly (2020) Resolution 75/36: Reducing space threats through norms, rules and principles of responsible behaviours (16 December 2020). [Online] A/RES/75/36. Available from: https://documents.un.org/doc/undoc/gen/n20/354/39/pdf/n2035439.pdf?token=WeRvH15fcixWyjxqiZ&fe=true

[44] United Nations General Assembly (2021) Resolution 76/231: Reducing space threats through norms, rules, and principles of responsible behaviours (30 December 2021) [Online]. A/RES/76/231. Available from: https://documents.un.org/doc/undoc/gen/n21/417/21/pdf/n2141721.pdf?token=3AWMDRxj50lzYehpYA&fe=true

[45] United Nations General Assembly (2022) Resolution 77/41: Destructive direct-ascent anti-satellite missile testing (12 December 2022) [Online]. A/RES/77/41. Available from: https://digitallibrary.un.org/record/3997622?v=pdf

[46] US Government, Fact Sheet: Vice President Harris Advances National Security Norms in Space, April 18, 2022, Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/

[47] NATO, Glossary of Terms and Definitions (AAP-06, Edition 2020) Available from: https://www.coemed.org/files/stanags/05_AAP/AAP-06_2020_EF_(1).pdf

[48] D. Stroikos, Power Transition, Rising China, and the Regime for Outer Space in a US-Hegemonic Space Order, in: T.B, Knudsen, C. Navari (Eds.), Power Transition in the Anarchical Society: Rising Powers, Institutional Change and the New World Order, Palgrave MacMillan, Cham, 2022, pp. 329-352.

[49] European Union, Joint Communication to the European Parliament and the Council, An EU Approach for Space Traffic management, An EU contribution addressing a global challenge (2022) Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0004

[50] US Government, Space Policy Directive 3, National Space Traffic Management, June 18, 2018, Available from: https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/

[51] European Union, Council Decision on the conclusion of the Agreement on the promotion, provision and use of Galileo and GPS satellite-based navigation systems and related applications between the European Community and its Member States, of the one part, and the United States of America, of the other part (12 December 2011) [Online]. 2011/901/EU. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011D0901

[52] D. Stroikos, International Relations and Outer Space, Oxford Research Encyclopaedias, International Studies, https://doi.org/10.1093/acrefore/9780190846626.013.699

[53] R. L. Pfaltzgraff, International Relations Theory and Spacepower, in: Lutes, C. *et. al.* (Eds.)Toward a Theory of Spacepower. Selected Essays, National Defense University Press, Washington, D.C., pp. 37-56.

[54] M. Machay, V. Hajko, Transatlantic space cooperation: An empirical evidence, Space Policy 32 (2015) 37-43. doi: https://doi.org/10.1016/j.spacepol.2015.02.001.URL https://www.sciencedirect.com/science/article/pii/S026596461500020X

[55] Xinhua, China, Russia invite international partners in lunar research station cooperation, XinhuaNet (2021). URL http://www.xinhuanet.com/english/2021-06/17/c1310011788.htm

[56] X. Wu, The International Lunar Research Station: China's New Era of Space Cooperation and Its New Role in the Space Legal Order, Space Policy 65 (2023) 101537. doi: https://doi.org/10.1016/j.spacepol.2022.101537. URL https://www.sciencedirect.com/science/article/pii/S0265964622000637

[57] ESPI, ESPI Brief Nº 46: "Artemis Accords: What Implications for Eu- rope?", European Space Policy Institute (2020). URL https://www.espi.or.at/briefs/artemis-accords-what-implications-for-europe/

[58] J. L. West, Space Security Cooperation: Changing Dynamics, Springer International Publishing, 2020, pp. 145-162.

[59] G. Toyoma, Countering threats in space through international cooperation, Space Policy 55 (2021) 101387. doi: https://doi.org/10.1016/j.spacepol.2020.101387. URL https://www.sciencedirect.com/science/article/pii/S0265964620300291

[60] S. Chiu, Promoting international co-operation in the age of global space governance - a study on on-orbit servicing operations, Acta Astronautica 161 (2019) 375-381. doi: https://doi.org/10.1016/j.actaastro.2018.07.019. URL https://www.sciencedirect.com/science/article/pii/S0094576518301802

[61] C. Giannopapa, N. Antoni, Space traffic management and its dual use: Space security strategies and cooperation in Europe, Acta Astronautica 212 (2023) 41-47. doi: https://doi.org/10.1016/j.actaastro.2023.01.038. URL https://www.sciencedirect.com/science/article/pii/S0094576523000498