The Use of Quantum-Based Technologies for Secure Satellite Communications in Support of European Union Space Security and Defence

August 2023
University of Glasgow: 2677876M
University of Trento: 233428
Charles University: 90101642

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word count: 21993
Supervisor: Prof. Georgios Glouftsios
Date of Submission: 06-08-2023

Table of Contents

Abstract

This research delves into the nexus between quantum technologies and their prospective role in enhancing secure satellite communications, with a particular focus within the European Union (EU) space security and defence. Embarking on an interpretivist research design, the study employs qualitative content analysis and fieldwork at the European Union Agency for the Space Programme (EUSPA) to elucidate the interplay between quantum principles and the EU's space endeavours. Through an exploration of quantum key distribution via space, the research shows a promising future for the secure transmission of critical data. To harness these quantum advancements effectively, substantial investments within the EU are essential. Against the backdrop of the evolving EU space strategy for security and defence, the research contemplates the centralisation of space matters within a singular, specialized EU body. In the broader context, the study underscores the urgency for international regulations to navigate the burgeoning complexities of space technology advancements and to safeguard against the threats of space weaponization. As the EU navigates unexplored space areas, the combination of quantum innovation, strategic coherence, and international cooperation emerges as crucial in guiding the EU towards a strong presence in space.

Introduction

In an international scenario characterised by technological dynamism and geopolitical turbulence, the role of space has transitioned from being solely a scientific laboratory and unexplored frontier to becoming a domain of strategic relevance.

Key to this research is the acknowledgement that space is no longer a sanctuary immune to terrestrial geopolitics. The interplay between space systems, signals, and security demands a comprehensive and anticipatory approach that embraces both the technological developments and the imperatives of strategic defence. The increasing role of space assets has simultaneously unveiled several vulnerabilities, exposing critical infrastructures to potential threats posed by hostile actors. As international norms waver and the once-clear skies become crowded with competing interests, the European Union (EU) finds itself at a crossroads, which requires a proactive posture to harness the potential of innovative technologies, particularly those rooted in quantum physics, to safeguard its space security.

At the heart of this study, lies in fact a key concern: how can the integration of quantum technologies enhance the security of satellite communications (satcom), thus bolstering the EU's space security and defence strategy? What are the effects of quantum technologies on space warfare and how do these effects impact the EU? What is the potential impact of quantum key distribution (QKD) on enhancing the security of communications for EU space assets?

Although existing literature has explored the applications of quantum technologies to satcom, there is a noticeable lack of comprehensive investigation into their convergence, specifically within the context of the EU's security framework. This research endeavours to address this lacuna by examining the potential of space-based QKD – a groundbreaking encryption

technique grounded in the laws of nature –, and assessing the feasibility of implementing such solution within the EU.

This research asserts that the integration of quantum technologies in satcom has the potential to greatly enhance the EU's space security and defence capabilities. This is due to the distinctive properties of quantum physics, which render quantum-based systems resistant to the vulnerabilities associated with conventional encryption methods. By strengthening its resilience against emerging threats and improving its strategic position in the space arena, the effective use of quantum technologies can significantly benefit the EU.

This research will embark on a journey guided by interpretivist methodologies and qualitative content analysis. It is structured into three analytical sections, following the literature review and the research design and methodology. The first chapter, provides a comprehensive examination of the EU's space programmes. The subsequent chapter delves into the threats to satcom and the EU's measures to mitigate these risks. The final analytical chapter explores the potential implications of employing quantum technologies in a warfare scenario, with particular emphasis on secure communications, focusing on the EU's Quantum Communication Infrastructure (EuroQCI) initiative.

In sum, this study will undertake a journey that blends theoretical investigation and empirical analysis to shed light on the synergy between quantum technology and secure satcom, foregrounding its implications for EU space security and defence.

Literature Review

Within the context of modern warfare, the notions of space strategy, space warfare, and spacepower have emerged as relatively recent concepts that frequently elicit confusion, and lack universally accepted definitions within the academia. However, it is important to understand the essence of these concepts in order to comprehend the strategic dynamics and security implications related to space activities.

Some interpretations of space strategy focus solely on the threat and the use of force in space and on Earth associated with the use of space assets. [1] However, space strategy can be described as the deliberate planning and implementation of a legitimate course of action designed to achieve an actor's objectives in space. It entails the strategic allocation of resources and the development of space capabilities to enhance a nation's or supranational entity's presence and influence in the realm of space. [2] Klein's research [3] on medium space powers' space strategies highlights the broad nature of space strategy, which encompasses various dimensions, such as scientific exploration, commercial endeavours, civil applications, and, most notably, military interests. The author classifies non-military activities typically covered within space strategies as follows: (i) Diplomacy: through active engagement in treaties and agreements, diplomatic influence enables the promotion and protection of interests in, and the guarantee of access to, space. (ii) Economic measures: in Klein's analysis, these are delineated as coercive economic pressure, i.e., economic warfare; hence, the purposes of such measures, which tend to be intertwined, consist of increasing their own commercial and financial space-related activities, and

[1] Bowen, B. E. (2019). *From the sea to outer space: The command of space as the foundation of spacepower theory*. In: *Journal of Strategic Studies*, 42:3-4, 532-556. p. 535.
[2] Sadeh, E. (2013). *Introduction: Towards space strategy*. In: Sadeh, E. (ed.), *Space Strategy in the 21st Century* (Routledge 2013). p. 2.
[3] Klein, J. J. (2012). *Space Strategy Considerations for Medium Space Powers*. In: *Astropolitics*, 10:2, 110-125. p. 112-116.

hindering or diminishing similar pursuits by a potential adversary. (iii) Establishing presence: closely connected to the first point, a strong presence in space and participation to space activities, treaties, and agreements, enables States and organizations to grow their influence on determining the course of the sector. (iv) Buying power: Despite its non-military classification, this category pertains to the procurement of commercial space capabilities with the end goal of enhancing military power in and via space.

In the area of military activities, it is necessary to establish distinctions between offensive and defensive actions, as well as between the militarization and weaponization of space. The adoption of the "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies"[4] (or Outer Space Treaty, OST) in 1966, which is the most relevant agreement on space activities, occurred during a time when the potential of space capabilities was considerably limited than what has since been demonstrated. Furthermore, due to the treaty's lack of comprehensive and detailed definitions and regulations, certain aspects of it remained subject to varying interpretations. The use of space solely for "peaceful purposes", as established by the OST, may preclude, as per the perspective of some countries, any engagement in military activities in space. Nevertheless, the simple reality of the dual-use potential of space assets renders this interpretation overly restrictive, and the interpretation of "non-aggressive purposes" appears as the most adequate one.[5] Here lies the difference between space militarization – the use of space for military purposes – and space weaponization – the deployment of weapons in space or against space assets. [6] However, some degree of ambiguity persists, as the term "non-aggressive" fails to draw a distinct

[4] UN (United Nations) General Assembly. (1966). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. 21st session. RES 2222 (XXI).
[5] *Op. cit.* Klein (2012). p. 117.
[6] Krepon, M., & Clary, C. (2003). *Is the Weaponization of Space Inevitable?*. In *Space Assurance or Space Dominance?: THE CASE AGAINST WEAPONIZING SPACE* (pp. 28–57). Stimson Center. p. 32-33.

boundary between offensive and defensive actions. Furthermore, the discussion surrounding the offensive and defensive nature of particular conducts remains a prominent issue, which, however, is not within the scope of this context to engage in. The current state of affairs shows that, perhaps due to mistrust, national prestige, scientific advancements, or probably a combination thereof, several States have tested space weapons, the role of space in supporting other domains and national security interests is ever-increasing, and the perception of war has undergone a major change since the introduction of space capabilities.[7] Such developments have led to the recognition of space as a new operational domain by NATO in 2019,[8] and by the EU in 2022.[9]

This context has given rise to the development of the notion of space warfare, encompassing a wide range of activities that leverage space-based systems and services to gain strategic, operational, or tactical advantages. These actions include electronic warfare, cyberattacks, anti-satellite weapons, as well as on-orbit capabilities hindering space systems (further elaborated upon in the chapter "Security Challenges, Satellite Communications, and EU Responses").[10] Bowen's seven propositions on space warfare shed light on the complexities of this concept and attempt at highlighting the need for a secure and sustainable space environment for the greater good of humanity.

The first proposition elucidates the link between space warfare and grand strategic goals. It points out that space control and space denial are equal subsets of space command, thereby implying that the capacity to wage war in space

[7] *Op. cit.* Klein (2012). p. 117.
[8] NATO. (23 May 2023, last updated). *NATO's approach to space*.
[9] Council of the European Union. (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*. 7371/22. p. 3.
[10] In this regard also see, e.g.: Johnson-Freese, J. (2016). *Space Warfare in the 21st Century: Arming the Heavens*. (1st ed.). Routledge.

encompasses not only its domination, but also the strategic prevention of adversary access.[11]

The second proposition emphasises the unique nature of space as a strategic environment and draws a parallel with sea warfare. In contrast to sea warfare, space warfare necessitates technical knowledge and is viewed as a supportive domain rather than a distinct battleground. Hence, although similarities with naval warfare exist, the peculiar environmental characteristics of space demand distinct strategic considerations.[12] In the case of naval warfare, decisive battles were sporadic and often strategically indecisive unless accompanied by a conscious exploitation of the command of the sea. Likewise, the notion of blockades in the bluewater context does not fully capture the dynamics of spacepower in Earth's orbit.[13] Bowen proposes that the future steps should draw from the continental perspectives put forth by strategists such as Raoul Castex, who viewed seapower from a continental perspective, thus preventing an excessive focus on geographically distant regions separated by oceans. This continental school of seapower conveys a novel perspective of Earth's orbit as a "cosmic coastline", offering relevant strategies for contemporary spacepower dynamics between neighbouring terrestrial powers that possess proximate and shared orbital coastlines.[14]

The third proposition seeks to balance the recognition of the strategic importance of space with a realistic understanding of its limitations in the context of terrestrial conflicts, asserting that dominance in space does not guarantee dominance on Earth. The idea of decisive battles in space should not be uncritically accepted as an axiom, as achieving space control does not constitute a key factor for victory, and space should not be regarded as a centre

[11] Bowen, B. E. (2020). *War in Space: Strategy, Spacepower, Geopolitics*. Edinburgh University Press. p. 55-65.
[12] *Ibid*. p. 66-68.
[13] *Ibid*. p. 97.
[14] *Ibid*. p. 98.

of gravity.[15] This approach opposes Dolman's *Astropolitik* theory, which presents space as a strategic *high ground* and asserts that exerting control over Low-Earth Orbit translates to Earth supremacy. [16] In Bowen's perspective, in contemporary strategic considerations, Astropolitik's visionary assumption exists as a theoretical testing ground rather than a pragmatic reality.[17]

The fourth proposition asserts that command of space is contingent not solely upon physical dominance, but it also involves the control or denial of channels for data and information transmission in the physical and electromagnetic spheres, that is, satellite communications, referred to as *celestial lines of communication* by Bowen. These links can be likened to the vital routes of space operations, that facilitate the transmission of crucial data and commands. This includes communication from ground stations to satellites (uplink), from satellites to ground stations (downlink), inter-satellite communications, as well as between space-based systems and other operational platforms across different domains, such as Unmanned Aerial Vehicles or naval vessels. Through the control of celestial lines of communication, a dominant space power can effectively affect information flow, thereby granting it the capability to deny or degrade an adversary's access to their own space-based assets. Similarly, protecting one's own celestial lines of communication is of utmost importance to ensure the uninterrupted operation of interconnected systems, both in times of peace and hostilities. The concept of celestial lines of communication extends beyond the *simple* notion of space dominance and delves into the intricacies of contemporary warfare, showing that effective command in space is not based merely on sheer brute force, but requires nuanced strategies involving communication and data exchange.[18]

---

[15] *Ibid*. p. 75-76.
[16] Dolman, E. C. (2002). *Astropolitik – Classical Geopolitics in the Space Age (1st ed.)*. Routledge. p. 83.
[17] *Op. cit.* Bowen (2020). p. 75.
[18] *Ibid.* p. 92.

The fifth proposition draws upon the language of marine strategy, to conceptualise Earth's orbit as a *cosmic coastline*, a zone of interaction between the terrestrial environment and space, which constitutes the foundational structure for the strategic planning and implementation of space operations.[19] It echoes proposition II, which emphasizes the nature of space operations as connected to Earth. The cosmic coastline provides a tactical arena, akin to what maritime coastlines have done for centuries, enabling actors to engage in strategic positioning, deployment, and safeguarding of their interests, without heralding a paradigm shift of international relations.[20] The concept of coastline also implies the presence of geographical limitations within the expanse of space, reflecting the orbital mechanics that determine the movement of spacecraft, in the same way tides and currents influence maritime navigation. Hence, comprehending the cosmic coastline necessitates a sound mastery of space technologies, as well as a deep understanding of the spatial-temporal dynamics of orbital mechanics, critical for the strategic deployment and protection of space-based assets.[21] Nevertheless, while space is a unique operational domain, its relevance and utility are predominantly derived from its proximity and connection to Earth. Moreover, in line with the third proposition and in contrast to Dolman's position, [22] Bowen emphasizes on how, in certain circumstances, the efficacy of space assets is diminished due to technological constraints, and that space warfare does not necessarily involve the utilisation of space-based weapons.[23] Once more, the latter concept evokes a notion rooted in naval warfare, specifically derived from Callwell's idea, which posits that dominance of the seas can be determined by the strength of land forces, rather than solely by naval battles.[24] The cosmic coastline enhances the strategic depth

[19] *Ibid.* p. 105, 109.
[20] *Ibid.* p. 114.
[21] *Ibid.* p. 123-124.
[22] *Op. cit*. Dolman (2002). p. 7-8.
[23] *Op. cit*. Bowen (2020). p. 109-110.
[24] Callwell, C.E. (1905). *Military Operations and Maritime Preponderance: Their Relations and Interdependence*. p. 167.

of terrestrial power, again a concept again elucidated by seapower history and theories, and exemplified by Mahan through the Franco-Dutch War in the second half of the XVII century, when the Dutch seapower thwarted France's attempts to outflank its land fronts. [25] The cosmic coastline, similarly to seapower in this example, also serves as a means to compensate for deficiencies in other domains, enhancing strategic depth through the broad uses that can be made of space capabilities by terrestrial forces. [26]

The sixth proposition postulates that our geocentric perspective significantly shapes our conception and application of spacepower, calling for the need of a transition towards a more *astrocentric* standpoint. This perspective mirrors the fact that, despite our projects in, and ventures into space, we continue to be inherently terrestrial beings, and the development of an *astroculture* [27] is consequently shaped by our geocentric standpoint, whether it be scientific exploration, economic expansion, or military advantage. In particular, military astroculture encompasses the dynamics of an actor's space capabilities and organisations, with a particular emphasis on the education, training, and career development necessary to build and maintain a cadre of highly competent and motivated military and civilian space professionals. [28] In the military spectrum, the geocentric perspective becomes particularly apparent, as the utilisation of spacepower predominantly serves to bolster terrestrial warfare capabilities, from precision targeting to secure communication, to intelligence, surveillance, and reconnaissance.

---

[25] Mahan, A. T. (1660–1783). *The Influence of Sea Power upon History*. Marston & Co., London, 1890. p. 168-169.
[26] *Op. cit*. Dolman (2002). p. 148.
[27] Astroculture is the human interpretation of outer space, or "the cultural significance and societal repercussions of outer space and space exploration". Geppert, A.C. (2018). *European Astrofuturism, Cosmic Provincialism: Historicizing the Space Age*. In: Geppert, A. (eds) *Imagining Outer Space*. Palgrave Studies in the History of Science and Technology. Palgrave Macmillan, London.
[28] *Op. cit*. Dolman (2002). p. 161.
McLaughlin, J. K. (2001). *Military Space Culture*. Prepared for the Commission to Assess United States National Security Space Management and Organization. p. 5.

The seventh and last proposition underscores the diffuse and distributed nature of spacepower. Unlike traditional forms of power, that can be centralized and constrained by geographical boundaries or physical infrastructures, spacepower is inherently dispersed.[29] Its vast expanse involves a distributed network of both space- and ground-based infrastructures. This dispersion poses distinctive strategic considerations for both offense and defence, in space as well as on the ground. Indeed, the proliferation of ground stations, control centres, and launch facilities on a global scale increases the possibility of these infrastructures becoming potential targets in a conflict, thus expanding the terrestrial battlefield as well. On the one hand, dispersion offers a form of resilience against adversarial attempts at disruption or destruction, given the inherent difficulty in disrupting a decentralised network compared to a singular facility. On the other hand, this dispersion carries its own challenges, as it requires resilient and distributed control and communication mechanisms to ensure effective operation. This dispersion demonstrates the successful utilisation of the celestial lines of communication and the cosmic coastline of prepositions IV and V in support of the grand strategic objectives of proposition I.[30]

In the area of spacepower, there has been a historical endeavour to develop a theoretical basis since the 1990s. However, these efforts have failed to deliver a comprehensive theoretical structure that offers a broad applicability across various timeframes and scenarios, enhancing judgment and critical analysis. This shortfall is partly attributable to the inconsistent use and understanding of key terms like "(space) strategy", "strategic theory", and "spacepower theory" within the spacepower literature. Hence, there exists a need for a comprehensive theoretical framework or "spacepower theory" which not only enhances comprehension and dialogue surrounding space-related endeavours, but also serves as a basis to strategize about space warfare and theorize the role of spacepower at the grand strategic level. According to the renowned military

[29] *Op. cit*. Dolman (2002). p. 196.
[30] *Ibid.* p. 194.

strategist and theorist von Clausewitz, theory makes order in a chaotic reality, thereby enabling a more thoughtful judgement.[31] Bowen's study attempts to address this gap by asserting that the command of space, a concept akin to the command of the sea in traditional seapower theory, serves as the cornerstone for understanding and interpreting space warfare – where command of space denotes the extent to which a party can exploit space for its own purposes or deny its use to adversaries.[32] Spacepower theory and space strategy are distinct concepts. While space strategy focuses on developing plans for specific scenarios, spacepower theory is a universal strategic theory that aims to educate individuals and stimulate thought. It provides conceptual tools that can be used to devise space strategies.

While spacepower theory could be applied in any case for the command of space and to develop space strategies, its strategic value and function vary depending on the specific type and case of conflict. [33] The line between space strategy, in particular that of the United States, and spacepower theory is blurred in John Klein's works.[34] Also, Klein's ideas about spacepower and space warfare stem from Julian Corbett's maritime strategy. When discussing seapower, Mahan and Corbett note that commanding the sea does not imply its complete domination, but rather controlling or denying specific areas within a certain timeframe, and that such command is not inherently decisive; they also reiterate the supporting nature of seapower for terrestrial scopes. Although Corbett's work serves as a seapower theory, it is possible to draw analogies between space and such assumptions on seapower, thus showing particular features and implications of spacepower.[35]

---

[31] Von Clausewitz, C. (1874). *On War*. (Graham, J. J., trans.). (Original work published 1832).
[32] Bowen (2019). p. 540-542.
[33] Gray, C. S. (1999). *Modern Strategy*. Oxford University Press. p. 264.
[34] See, in this regard: Klein, J. J. (2005). *Space Warfare – Strategy, Principles and Policy (1st ed.)*. Routledge.
[35] Bowen (2019). p. 545-550.

The theories of spacepower, space strategy, and space warfare, which have been previously examined, are not solely theoretical concepts, but have manifested tangible expression in the growing militarization and potential weaponization of space. Through the escalating space arms race, driven by a lack of trust and cooperation among major space powers, real-world applications of spacepower and space strategies appear clear, reflecting the importance of these theories in contemporary geopolitical discourse and its understanding.

While there are currently no actual weapons deployed in space, capabilities serving military scopes such as Intelligence, Surveillance, and Reconnaissance (ISR), Earth observation, Space Surveillance and Tracking (SST), resilient communication, are indeed present. Satellites, though vital for operations, are challenging to protect and are vulnerable to counterspace weapons, that countries with substantial space capacity, such as China, India, Russia, and the US, and have demonstrated to be deployable. The potential for misinterpretation of an actor's actions, which can be perceived as hostile by others, can engender a vicious loop that intensifies the sense of mistrust, limited international cooperation, and thereby accelerates their military space programs.[36] Furthermore, akin to other contexts and domains, the increase of one's spacepower, gaining an advantage over adversaries, can potentially serve as a deterrent against hostile actions. An analogy can be drawn, e.g., to the pursuit of air superiority in North Africa, particularly between Morocco and Algeria. [37] In line with this idea was the 2001 US Commission to assess US national security space management and organization report by Donald Rumsfeld, who emphasised the vulnerability of US space assets, advocating for the

---

See, in this regard: Mahan, A. (2010). *The Influence of Sea Power upon History, 1660–1783*. (Cambridge Library Collection - Naval and Military History). Cambridge: Cambridge University Press.
Corbett, J. S. (1911). *Some principles of maritime strategy*. London: Longmans, Green.

[36] Webb, D. and Scheffran, J. (2021). *Anti-Satellite Weapons and Ballistic Missile Defense: the Siamese Twins?*. International Working Group MBMDS.

[37] Macci, F. (2023). *The Growth of the Moroccan Military Air Power*. Moroccan Institute for Policy Analysis.

comprehensive control of space to secure American space capabilities against a potential "Space Pearl Harbor".[38] Rumsfeld's perspective has influenced US strategic and military thinking, leading to a focus on achieving "full spectrum dominance", necessitating strong defensive and offensive capabilities, integration of all domains, and blending of civil, commercial, and military space operations, contradicting the idea of space as a common heritage of mankind.[39]

International bodies such as the United Nations (UN), the Conference on Disarmament (CD), or the International Telecommunication Union (ITU) have undertaken several attempts to deter an arms race in outer space. These initiatives address civil, military, or more technical space issues, and aim at preventing the deployment of weapons against space objects. Nonetheless, a significant challenge encountered in these efforts pertains to the difficulty in defining a space weapon. For instance, the definition proposed by Russia and China for their draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT) includes any device in space produced or converted to disrupt, destroy, or damage objects in space, on Earth, or in Earth's atmosphere.[40] This definition presents limitations, as it does not cover weapons launched from the ground or from aircraft, nor any verification tools. Moreover, achieving international consensus on what constitutes a "specially produced or converted"[41] device might prove difficult, and the draft treaty has been rejected most notably by the US. While international agreements restricting space weaponization are yet to be realized, the implementation of additional partial arms control measures could contribute to the mitigation of space weapon-related risks. For instance, such measures may encompass a ban on testing, deployment, or utilisation of

[38] Rumsfeld, D. (2001). *Report of the Commission to Assess United States National Security Space Management and Organization*. p. xiii-xv, 22.
[39] Webb, D. and Scheffran, J. (2021). *Prevention of an Arms Race in Outer Space (PAROS): Obstacles and Options*. p. 3.
[40] *Ibid.* p. 1-2, 5-6.
[41] Russian Federation and China. (2008). *Letter dated 2008/02/12. CD/1839.* Art. 1(c). p. 3.

weapons above specific altitudes.[42] Despite challenges, a novel code of conduct including major actors in space is still deemed achievable, owing to the substantial investments made by all actors involved and the common risks of warfare in space.[43] In order to address this issue, Porras put forth a proposition involving the formulation of guidelines for anti-satellite weapons (ASAT) testing, along with negotiations on a treaty prohibiting the destruction of in-orbit objects.[44] Nevertheless, the signing of a Prevention of an Arms Race in Outer Space (PAROS) treaty is hardly conceivable without the collaboration of major space powers like the US, Russia, China, and potentially India. However, the current geopolitical landscape further complicates the already intricate prospects of reaching a consensus on the matter.

Another critical and intricate facet of the space domain is the dual-use dilemma of space assets. This refers to the inherent capability of space systems to serve both civilian and military purposes. The very nature of space technologies straddles the fine line between the two spheres of application, and their duality is continuously expanding, as equivalent technologies are required by both military and civilian actors. For instance, the American and the Russian Global Navigation Satellite Systems (GNSS), namely, the GPS and the GLONASS respectively, serve both civilian and military purposes. These systems, e.g., can provide guidance civilian aircraft or precision-guided munitions, thus serving as a force multiplier for terrestrial military operations. The distinction between military and commercial space systems has become increasingly blurred with the expansion of the latter. In fact, US space industry used to be characterised by a division into civilian, commercial, military, and intelligence sectors. However, this division eroded with the expansion of the use of space after the Cold War, mainly on a commercial level. This trend has led the US government to establish the Dual Use Science and Technology program, ensuring access to

[42] *Op. cit.* Webb and Scheffran (2021). *PAROS.* p. 8.
[43] *Op. cit.* Webb and Scheffran (2021). *PAROS*. p. 10-11.
[44] Porras, D. (2019). *Anti-satellite warfare and the case for an alternative draft treaty for space security*. In: Bulletin of the Atomic Scientists, 75:4, 142-147. p. 142-147.

dual-use technology without having to invest in the technology's research and development.[45] Nevertheless, the accessibility of commercial technology also introduces a range of risks further analysed later in the research, and as demonstrated for instance by Saddam Hussein's acquisition of Russian-made jamming equipment through the internet during Operation Iraqi Freedom, which was subsequently employed against the US.[46]

Once again, it is necessary to emphasise the importance of establishing precise definitions for space weapons, as traditional definitions typically fail to account for the potential destructive capacity of dual-use technology. For instance, Hebert, echoed by Hitchens, Katz-Hyman and Lewis, defines a space weapon as any Earth-based or space-based asset intended to attack targets in space or on Earth, encompassing both space-to-space and Earth-to-space weapons.[47] The three authors additionally warn about the potential for the development of space-to-Earth weapons,[48] yet they refrain from including dual-use technologies within their definition. Furthermore, definitions usually do not take into account that hybrid operations, i.e., those conducted in the "grey zone", frequently rely on the utilisation of dual-use capabilities. According to Robinson *et al.*,[49] these encompass a wide range of activities, spanning from directed energy operations, that result in the creation of space debris, to electronic and cyber operations, to economic and financial operations targeting the space sector. The ambiguity around these activities illustrates the dual-use nature of many space technologies, such as active debris removal systems, satellites employed as weapon platforms, launch vehicles, small satellites, as well as information

[45] Pražák, J. (2021). *Dual-use conundrum: Towards the weaponization of outer space?*. In: *Acta Astronautica*, Volume 187, 397-405. p. 398.
[46] *Ibid.* p. 398.
[47] Hebert, K. D. (2014). *Regulation of space weapons: Ensuring stability and continued use of outer space*. Astropolitics, 12(1), 1-26. p. 3.
[48] Hitchens, T., Katz-Hyman, M., and Lewis, J. (2006). *U.S. SPACE WEAPONS: Big intentions, little focus*. The Nonproliferation Review, 13(1), 35-56.
[49] Robinson, J. *et al.* (2018). *Europe's Preparedness to Respond to Space Hybrid Operations*. Prague Security Studies Institute. p. 3.

technology.[50] As suggested by Pražák,[51] the concern also lies in the fact that the dual-use of such capabilities for hybrid operations could become an integral part of space strategies. Furthermore, the prevailing legal framework, formulated during the Cold War, fails to address the complexities introduced by technological advancements, and the international community faces difficulties in formulating comprehensive norms that align with these continuous developments.[52] The McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) and the Woomera Manual on the International Law of Military Space Activities and Operations exemplify efforts aimed at establishing guidelines to bridge the gap between historical regulations and the evolving landscape of space technologies. MILAMOS represents a collaborative effort by legal experts and scholars with a primary focus on addressing legal aspects and potential scenarios pertaining to military-related space endeavours. It attempts to clarify rights and responsibilities of actors engaged in space activities with military implications, encompassing topics that include but are not limited to the right of self-defence, compensation for damage, interferences, and weapons of mass destruction.[53] Similarly, Woomera seeks to elucidate the international legal framework relevant to space warfare and military uses of space assets.[54]

[50] *Op. cit.* Pražák (2021). p. 399-402.
[51] *Ibid.* p. 403.
[52] *Ibid.* p. 402.
[53] Jakhu, R. S. and Freeland, S. (eds.). (2022). *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I – Rules*. Montreal: Centre for Research in Air and Space Law.
[54] See, in this regard: The University of Adelaide. (2018). *Woomera Manual on the International Law of Military Space Operations*.

Research Design and Methodology

Research Design

The approach used to conduct this research is grounded in an interpretivist fashion, an epistemological stance that emphasises the need to understand phenomena within their specific context and their inherent characteristics. The underlying foundation of this approach rests on the premise that reality is not an external entity that can be objectively measured and comprehended, but rather, it is a construct shaped by individuals' experiences and perceptions.[55] Interpretivism constitutes a distinctive epistemological paradigm that sharply diverges from positivism – an approach deeply entrenched in the scientific examination of the natural world. Interpretivism encompasses the perspectives of scholars who oppose the application of a scientific method to the study of social phenomena, which instead necessitate a distinct research approach that resonates with the intrinsic uniqueness of human experiences vis-à-vis the natural order. Von Wright encapsulates such epistemological clash as a contest between positivism and hermeneutics.[56] Hermeneutics involves the interpretation of texts or behaviours to uncover additional layers of meaning and understanding. It is a theological term, which, when applied to social sciences, denotes the theory and method of interpreting human actions. [57] The origins of this dichotomy can be traced back to historical debates preceding the advent of modern social sciences, epitomized by Max Weber's advancement of the concept of *Verstehen* ("understanding"). Weber's assertion in 1947 captures the essence of interpretivism: sociology seeks to understand social actions through interpretation, serving as a foundation for causal explanations of their paths and outcomes.[58] A hermeneutic approach, which is inherently interpretivist, will in

[55] Bryman, A. (2012). *Social Research Methods*. 4th edition, Oxford: Oxford University Press. p. 28-30.
[56] Von Wright, G. H. (1971). *Explanation and Understanding*. London: Routledge.
[57] *Op. cit.* Bryman (2012). p. 560-561.
[58] *Ibid.* p. 28-30.

fact guide the research, as its principal aim is to understand human action and its repercussions through the interpretation of the meanings that people attribute to these actions. Hermeneutics exhibits similarities with the concept of the active audience perspective, as it gives value on the reception of texts and acknowledges the possibility of multiple interpretations. A critical hermeneutic approach incorporates qualitative content analysis practises and integrates them with formal textual analysis methods. [59] Therefore, this research endeavours to comprehend the subject matter by analysing the behaviour, interactions, and motivations of the actors involved in the space domain. An interpretivist design explores the complexities arising from the intersection between spacepower and technological advancements.

Acknowledging the complex and evolving nature of social realities, the research recognises the limitations of an objectivist ontology, typically employed in quantitative analyses. Indeed, objectivism posits an external reality that can be captured and understood, irrespective of the observers' perceptions or experiences.[60] Nevertheless, this study embraces a constructionist ontology. The constructionist perspective asserts that reality is shaped by social processes and is comprehended through the subjective interpretations of individuals based on their interactions and experiences within the social sphere. Constructionism enables a deeper exploration of the intricate social phenomena and acknowledges their dynamic nature, as individuals interact and interpret their experiences. Aligned with this constructionist ontology, the research focuses on the interplay between geopolitical, diplomatic, and technological factors shaping the EU's approach to space security and defence.

In sum, this research seeks to provide a contextualised understanding of the intricacies related to the use of quantum technologies for secure satellite

[59] *Ibid.* p. 561.
[60] *Ibid.* p. 179.

communications within the EU context by adopting an interpretivist approach, grounded in hermeneutics and constructionism.

Methodology

The selected methodology for this research is based on a qualitative approach, aligning with the myriad interconnections and nuanced dynamics prevalent in the field of space security and defence. Qualitative research aims to analyse relationships and conduct comprehensive analyses on specific issues, with the objective of revealing the fundamental connections between technological advancements, policy, and strategy. [61] Rather than analysing vast and diverse datasets, the present methodology adopts an inductive orientation, prioritising an in-depth examination of specific themes in order to generate a theory as an outcome of the study.[62]

Essential in this research is the utilization of fieldwork, an immersive approach that entails active engagement with the subject of study. To this end, the researcher completed a traineeship in the Security Authority Department of the European Union Agency for the Space Programme (EUSPA). This fieldwork experience proved highly valuable in acquiring first-hand comprehension of the dynamics that underpin the EU's endeavours in space security and defence. By immersing oneself within the organizational context, the researcher was able to gather nuanced perspectives and grasp the multifaceted challenges that shape the studied landscape.

In addition to fieldwork, the methodology employed in this research relies on qualitative content analysis. In this specific case, conducting a qualitative examination of official documents enables the researcher to identify underlying themes and strategic orientations. Precisely, the research methodology that

[61] *Ibid.* p. 380-387.
[62] *Ibid.* p. 24-27.

appears to serve most effectively the research objectives of this study is arguably Altheide's Ethnographic Content Analysis (ECA), which is characterised by continuous movement between the qualitative research steps of conceptualization, data gathering, analysis, and interpretation. In ECA, if certain predetermined variables and categories initially guide the study, it is expected for additional ones to emerge throughout the study. This approach entails a continuous commitment to discovering new information and constantly analysing relevant situations and nuances.[63]

[63] Altheide, D. L. (1996). *Qualitative Media Analysis*. Thousand Oaks, CA: Sage Publications, Inc. p. 16.

The European Union's Approach to Space

In a time characterised by the increasing reliance on space capabilities for security, defence, but also economic purposes, the European Union's (EU) endeavours in space have grown significantly in recent years. The initial chapter of this research outlines the EU's involvement in space by examining the various components of its space programmes. This chapter will serve as a foundation for comprehending the EU's strategic stance towards the broader space security challenges, the role of satellite communications, and the potential of quantum technologies, as will be explored in subsequent chapters.

The Union Space Programme

On 28 April 2021, the European Parliament (EP) and the Council adopted Regulation (EU) 2021/696 establishing the Union Space Programme (the "Programme") and the European Union Agency for the Space Programme (EUSPA), which replaced the 17-year-old European Global Navigation Satellite Systems Agency (GSA). The creation of the Programme is based on the unification of several programmes and corresponding regulations under the cap of a few entities, in particular that of EUSPA, whose role is no longer limited to the operational management of satellite navigation systems, but extended to additional responsibilities.

When the Programme was established, it consisted of five components of mainly civilian nature [64]. However, the continuous geopolitical, technological, economic, and natural evolutions on ground and in space require an equal response in order for the EU not to fall behind its competitors and maintain the security of its Member States and allies. In fact, in the timespan of less than one year, the EU approach to space has undergone important developments. Among

[64] The Regulation, however, acknowledges the possibility of the use of the programme component GOVSATCOM for military Common Security and Defence Missions and Operations. See, in this regard, *Regulation (EU) 696/2021* preambles n. 50, 100, 110.

these are the recognition, in the Strategic Compass for Security and Defence, of the role of space for defence purposes; Regulation (EU) 2023/588 establishing the Union Secure Connectivity Programme (USCP), which serves as a complementary addition to the Union Space Programme and introduces a sixth component of the Programme, IRIS^2; and the publication of the first EU Space Strategy for Security and Defence by the European Commission and the European External Action Service.

Galileo

Galileo is the European Global Navigation Satellite System (GNSS), interoperable with the American Global Positioning System (GPS) and the Russian GLONASS, providing positioning, navigation, and timing (PNT) services on Earth. Its constellation consists of 28 satellites placed in the Medium Earth Orbit (MEO), with 24 of them being utilised for service provision, catering a wide range of services to both civilian and governmental users around the globe.[65] It is owned by the EU, its technical development is entrusted to the European Space Agency (ESA), and EUSPA – on behalf of the European Commission (EC) – is in charge of its operational management.[66] Galileo's services are:

- The Galileo Open Service (OS) [67] provides a free of charge service for positioning, timing (i.e., the accurate Universal Time Coordinated), and ranging (i.e., the distance between the user and the satellite from which the signal is originated) through the transmission of navigation signals in three different frequency bands.

[65] ESA. (14 July 2023, last accessed). *What is Galileo?*
European GNSS Service Centre. (14 July 2023, last accessed). *Services*.
European GNSS Service Centre. (14 July 2023, last accessed). *Constellation Information*.
[66] European GNSS Service Centre. (14 July 2023, last accessed). *FAQ*.
[67] European GNSS Service Centre. (2021). *Galileo – Open Service – Service Definition Document*.

- The Open Service Navigation Message Authentication (OSNMA) assures that the navigation message received by Galileo has not been spoofed or jammed.
- The Commercial Authentication Service (CAS) delivers to users "a controlled access and authentication function".
- The High Accuracy Service (HAS)[68] allows the positioning accuracy to be <50 centimetres.
- The Search and Rescue Service (SAR) [69] implements the international COSPAS-SARSAT search and rescue distress alert detection system.
- The Public Regulated Service (PRS) is only accessible to government-authorised users and presents a higher level of protection against any possible issues that may interfere with the Signal-in-Space (SIS), including malicious activities such as spoofing and jamming.

EGNOS

EGNOS (European Geostationary Navigation Overlay Service) is the European regional satellite-based augmentation system (SBAS). It improves the precision of the GNSS GPS and, in the future, Galileo's performance as well. It also detects and sends warnings in cases of discontinuity and unavailability of a signal ("integrity information" function). In addition to the EGNOS Open Service and the Data Access Service, it provides the Safety of Life (SoL) Service. The latter enhances the navigation accuracy of civil aviation, and can potentially be used in the maritime, railway, and road fields as well. Aircraft, and in the future any vehicle, equipped with a SBAS-enabled receiver can conduct operations and landings in any weather condition thanks to the high accuracy and the integrity function of the Service. Along with Galileo, EGNOS enables the independence and sovereignty of the Union's navigation and timing

[68] European GNSS Service Centre. (2023). *Galileo High Accuracy Service – Service Definition Document (HAS SDD)*.
[69] European GNSS Service Centre. (2020). *SAR/Galileo Service Definition Document*.

services.[70] The EC, owner of EGNOS, has entrusted ESA with the technical developments of the programme, while EUSPA is responsible for its operational management and exploitation phase.[71]

Copernicus

Copernicus is the Union's Earth Observation (EO) and monitoring system managed by the EC in close cooperation with ESA and the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT)[72]. It provides free and open data, which are then processed to become valuable atmosphere, marine, climate, land, security, and emergency management information.[73] Seven dedicated satellites – the Sentinels –, thirty satellites of contributing missions from national, European, and international organisations (Space Segment), and in-situ sensors (Ground Segment) gather the data.[74] FRONTEX, the European Maritime Safety Agency, and the EU Satellite Centre (SatCen) provide the services for security applications of Copernicus, respectively for border surveillance, maritime surveillance, and external actions.[75] In particular, SatCen operates the Copernicus services in Support to EU External Action (SEA), the EU geospatial intelligence service, in support of the EC, the European External Action Service (EEAS), and Common Security and Defence Policy (CSDP) stakeholders.[76]

---

[70] GSA. (2021). *EGNOS Safety of Life (SoL) – Service Definition Document*.
EGNOS User Support. (14 July 2023, last accessed). *About EGNOS*.
Directorate-General for Defence Industry and Space. (14 July 2023, last accessed). *Safety-of-Life Service*.
[71] EGNOS User Support. (14 July 2023, last accessed).
[72] *Regulation (EU) 2021/696*, p. 15, para.86
[73] Copernicus. (14 July 2023, last accessed). *Copernicus in detail*.
Copernicus. (14 July 2023, last accessed). *Copernicus Programme*.
[74] Copernicus. (14 July 2023, last accessed). *Infrastructure Overview*.
[75] *Op. cit.* Copernicus. (14 July 2023, last accessed). *Copernicus Programme*.
[76] SatCen. (14 July 2023, last accessed). *Copernicus*.
Copernicus Service in Support to EU External Action. (14 July 2023, last accessed). *Copernicus Service in Support to EU External Action*.

SSA/SST

Space Situational Awareness (SSA) aims at monitoring, tracking, and identifying space objects and space debris in order to ensure the continued and sustainable access to and use of space. SSA encompasses the monitoring of Near-Earth Objects (NEO) and Space Weather (SWE), as well as Space Surveillance and Tracking (SST) of artificial objects. SST gathers data from sensors belonging to Member States in order to offer the following services: risk assessment for space objects Collision Avoidance (CA), Re-entry Analysis (RE) of uncontrolled artificial objects into Earth's atmosphere, and Fragmentation Analysis (FG) of in-orbit objects.[77] On 1 July 2023, the SST Front Desk service, i.e., the interface for users to obtain SST information and services, was transferred from SatCen to EUSPA – which is managing it through one of its GSMC –, along with the security monitoring of the SST network.

GOVSATCOM

GOVSATCOM is the EU's Governmental Satellite Communications (satcom) programme established by Regulation (EU) 696/2021. Hence, the programme is a relatively new initiative still in its implementation phase. Its aim is to provide secure, cost-efficient, and reliable "communications capabilities to security and safety critical missions and operations"[78] in consideration of a variety of security risks characterizing satcom as well as communications in general. Such risks can threaten electromagnetic signals (e.g., spoofing, jamming), data (cyberattacks), or can also result from the lack of signal due to interruptions for disasters or unavailability for geographical features (e.g., in the

[77] EUSPA. (14 July 2023, last accessed). *Space Situational Awareness*.
EUSPA. (2022). *EUSPA takes on the Space Surveillance and Tracking helpdesk as of 2023*.
Regulation (EU) 2021/696, p. 15, para.88-90
[78] EUSPA. (2021). *GOVSATCOM*.

Arctic).[79] GOVSATCOM is initially conceived as a Hub that links its users via secure satcom, and to do so it utilizes the ground and space infrastructure of MSs or satcom service providers at least until 2025. In the meantime, thanks to the adoption of Regulation (EU) 2023/588 establishing the Union Secure Connectivity Programme, the Union's ground and space infrastructure – in the form of the new satellite constellation IRIS^2 – are being developed and built to provide secure satcom through the GOVSATCOM Hub. The use of GOVSATCOM services is limited to EU and MSs authorities, third countries – upon compliance with specific conditions –, and entrusted natural and legal persons and bodies. The use cases identified for GOVSATCOM span across three large, interconnected areas[80]:

- In crisis management situations, it allows actors in the field, rear bases, and command & control centres to communicate and exchange data minimising the risk of malicious interference on communication services such as email, messaging, voice, video, or specific information systems.[81]
- In border and maritime surveillance, it enables the timely exchange of reliable information – including but not limited to broadcast and multicast data services or high-resolution radar and optical images – among surveillance systems, surveillance agencies, mobile patrols, and authorities in order to respond in the minor possible time after the detection of an event.[82]
- In the management of key infrastructure, it provides secure satcom to police enforcement and to the European and national diplomatic network anywhere across the globe, a particularly relevant element in case of

[79] *Ibid.*
[80] Directorate-General for Defence Industry and Space. (2021). *Overview*. *Ibid.*
[81] Directorate-General for Defence Industry and Space. (20 July 2023, last accessed). *Support to Crisis Management Operations*.
[82] Directorate-General for Defence Industry and Space. (2021). *Support to Border and Maritime Surveillance*.

crisis or conflict; it also links control centres to energy, protection and transport infrastructure often located in remote areas.[83]

- In addition to the aforementioned applications, GOVSATCOM is expected to be generally utilised for the secure transmission of data to and from space systems, e.g., related to SSA and SST. Further scopes of GOVSATCOM may encompass communications in remote regions, operation and communication with onboard sensors of unmanned aerial vehicles (UAVs) for their control and data retrieval, and machine-to-machine communication for data retrieval from on-site sensors.[84]

IRIS²

IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) is the Union's satellite constellation for secure communication and worldwide broadband internet. It falls under the Union Secure Connectivity Programme (USCP), established in March 2023 via Regulation (EU) 2023/588. The USCP seeks to integrate and expand the scope of GOVSATCOM, enhancing its resilience and introducing a quantum encryption capability in the frame of the European Quantum Communication Infrastructure (EuroQCI). It would thus be not entirely proper, at least from a practical standpoint, to refer to it as a Programme independent from the Union Space Programme; rather, it would more apt to think of the USCP as an integral Programme component. IRIS² entails two connectivity services, that is, a prioritised governmental one, and a commercial service provided by the European private sector.[85] The Commission is responsible for the general management of the USCP, and entrusts EUSPA with its operational management and security accreditation.

[83] Directorate-General for Defence Industry and Space. (2021). *Support to Key Infrastructure Management*.
[84] *Ibid.*
Supra note 81, 82.
[85] *Regulation (EU) 2023/588*, p. 3, para. 11.

IRIS[2] is supposed to use the GOVSATCOM Hubs for its ground infrastructure, which, as per the Regulations, is expected to utilize Member States' facilities until roughly 2025; however, considering the temporal requirements associated with the deployment and full operability of the dedicated infrastructure, this timeframe may encounter delays. The integration of different assets brings a series of issues connected to the diversity of the systems and, among others, their approach to their security. The creation of a GOVSATCOM-IRIS [2] space and ground infrastructure will in fact align the capabilities of its assets, allowing the Union to integrate quantum communication when it will be ready for deployment, to implement, at its own pace, the security requirements needed to ensure the integrity and availability of the service, and eventually to provide "solutions for inter-satellite connectivity and data relay between satellites, the ground and the terrestrial infrastructure".[86] On the line of IRIS[2]'s synergy with GOVSATCOM, the connection of key infrastructures, crisis management and surveillance represent also the former main declared use cases, but not the only ones. Given IRIS[2]'s double service – governmental and commercial –, it also involves private sector-tailored applications, such as Business-to-Business (B2B) satellite trunking and cloud-based services, reinforced satellite broadband networks, and satellite access for transportation.[87]

[86] *Regulation (EU) 2023/588*, p. 4, para. 14.
[87] Directorate-General for Defence Industry and Space. (2023). *IRIS² - Factsheet (EN)*.

Security Challenges, Satellite Communications, and EU Responses

The pervasive nature of the cyber domain has resulted in the embedding of cybersecurity across all other domains – air, land, maritime, and space – and aspects of society. Satellite communications (satcom) are a crucial information exchange infrastructure that presents both opportunities and vulnerabilities, thereby requiring an increased focus on the implementation of its security. As we continue to advance in an era where cyber and space enable to enhance the potential of the other domains, the intersection between these two domains becomes a critical area of analysis. Therefore, this chapter starts with a presentation of the various typologies of counterspace weapons, including cyber. Then, the focus shifts to the fundamental principles of cybersecurity, which are essential for comprehending the next chapter of the research as well. The following sections delve into the key elements of satellite communications and engage in a discussion of the cyber threats satcom are vulnerable to, recognizing the central role of satcom in bolstering security and defence operations. The chapter concludes with an analysis of the European Union's efforts to enhance cybersecurity and space systems security measures, highlighting the proactive measures taken to address these complex threats.

Counterspace Weapons

As the number of space infrastructure, both state-owned and privately-owned, for both military and civilian purposes, grows, so do the risks that threaten their security. These threats can be either hazardous or intentional, and distinguishing between the two and attributing an attack can be extremely difficult. Furthermore, in the sphere of intentional attacks, there are large differences among counterspace weapons [88] in terms of the effects they produce, how they

[88] "Counterspace is [an operation aimed at negating] an adversary's use of space capabilities, reducing the effectiveness of adversary forces in all domains". Curtis E. LeMay Center for

are deployed, the ease with which they can be detected and attributed, and the level of resources and technology necessary to develop and deploy them,[89] making it difficult to develop preventive and mostly pre-emptive security measures against them. Counterspace weapons can be broadly classified into four categories:[90]

- *Kinetic Physical*: attacks to ground infrastructure, direct-ascent anti-satellite weapons (ASAT), and co-orbital ASATs belong to this category. These attacks are more easily attributable and are likely to produce orbital debris in the case of ASATs. They aim at the physical destruction of capabilities through direct strikes or bomb detonation in their proximity.
- *Non-kinetic Physical*: High-Altitude Nuclear Detonations, High-Powered Lasers, Laser Dazzling or Blinding, and High-Powered Microwave (HPM) are examples of such attacks. While they do not make physical contact with satellites, they have physical effects on the targeted satellite or satellite's components, such as sensor dazzling and blinding, electrical circuits damage, or accelerated degradation. The ease of attribution of these attacks varies. For instance, HPM can originate from other satellites and remain invisible, whereas a laser attack from Earth is easier to attribute since the targeted satellite must be within the laser's field of view at the time of the attack; such attacks require a certain level of sophistication, which might not be accessible to all actors.
- *Electronic*: this kind of counterspace weapons do not target satellites nor the transmitted data, but instead, their electromagnetic spectrum, that is the signal used for data transfer. Such weapons include uplink (Earth-to-space signal) and downlink (space-to-Earth signal) jamming, as well as

Doctrine Development and Education (2021). *Air Force Doctrine Publication (AFDP) 3-14 Counterspace Operations*. United States Air Force. p. 1.
[89] Harrison, T. *et al.* (2022). *Space Threat Assessment 2022*. p. 3.
[90] *Ibid.* p. 3-7.

spoofing techniques. Jamming attacks generate noise on the radio frequency band between a satellite and the ground station, resulting in a communication blackout for the duration of the attack. Spoofing involves transmitting false signals to a data stream, deceiving it into believing that the signals are authentic, thus disabling communication with the satellite and potentially enabling the attacker to take over control of its operations until the end of the attack. Meaconing, a type of spoofing, involves the rebroadcasting of an old signal without altering the data. These attacks can be challenging to attribute as jamming and spoofing devices are commercially available.

- *Cyber*: cyberattacks aim to attack the data itself and the systems responsible for its management and transmission. Such attacks can take various forms, such as the monitoring of data traffic patterns, data interception, or the introduction of corrupted or false data into a targeted system. The targeted attack surface can be on the satellites themselves or on ground station and end users' systems. A cyberattack against space systems carries can have severe consequences, including the theft, compromise, or manipulation of data, the disruption of communication networks; but also, in taking control of a satellite, intentionally damaging or disrupting its operations, or even permanently disabling the system. Attribution of cyberattacks can be challenging due to the inherent difficulty of tracing them and the possibility of State actors to deflect responsibility onto third-party actors (the so-called "hackers for hire" entities), further blurring the line between cyber criminals and State-sponsored attacks.

This brief presentation shows that counterspace weapons can be deployed both in space and on the ground and sea. The weaponization of space, which refers to the deployment of weapons in space or against space assets, is a relatively recent phenomenon that differs from the militarization of space, which involves

the use of space for military purposes. [91] Space militarization has been ongoing since the early days of the space age, and after decades of being perceived as an expansion of airspace, the operational support component of space systems started to be explored in greater detail in the 1990s. Space weaponization is a phenomenon strictly linked to cyber methods, as these techniques enable space assets to be utilised as weapons. [92] Along with electronic methods, this kind of attacks are very likely to have a paralysing effect on their direct target, causing a multi-domain ripple effect on the operations supported by the targeted space assets.

Support to military operations by space assets are not limited to, but include the provision of geospatial intelligence through Earth observation, Positioning, Navigation and Timing (PNT), Intelligence, Surveillance and Reconnaissance (ISR), and (secure) satcom. Satcom are a critical aspect of support to operations. Satellites provide essential connectivity for military and civilian communications, encompassing a wide range of transmissions such as voice, video, and data. Satcom find extensive application in a wide range of military operations, from battlefield communications to Communication, Command and Control (C3) of Unmanned Aerial Vehicles (UAVs). Satellites are also essential for providing reliable communication services in remote areas, disaster response, and Search and Rescue (SAR) missions. Satcom represent the link between ground and space infrastructure and as such, it should enable the transmission of data across a wide range of applications that rely on space-based data. Due to their crucial function and wide attack surface, satcom represent a prime target for attacks. Interruption of services, corrupted data, or interferences may disrupt significantly military operations, and shall hence be properly protected.[93]

[91] *Op. cit.* Krepon (2003). p. 32-33.
[92] European Space Policy Institute (ESPI). (2022). *ESPI Short Report 1 - The war in Ukraine from a space cybersecurity perspective*. p. 3.
[93] *Ibid.* p. 9.

Before delving into the discussion of the threats to satcom, it is important to first examine the cybersecurity tenets that guarantee the security of satcom, and satcom themselves. An analysis of the unique characteristics of cyber threats and satcom provides insight into how these two domains intersect and the potential risks that arise from their convergence, allowing for the development of more effective strategies to mitigate the threats' potential impact.

Cybersecurity

In the field of Information Technology (IT), threats are potential digital events that might cause damage to an information system or network.[94] They target the Confidentiality, Integrity, and Availability (often referred to as the CIA Triad), as well as the Authentication and Authorization, and Nonrepudiation of digital targets. These principles provide a framework that, if appropriately addressed by adequate security measures, ensures the protection of systems and data from potential threats. Analysing these concepts will provide a more comprehensive understanding of satcom security:

- Confidentiality: the sharing of information based on the "need-to-know" principle to protect sensitive or classified information from access by unauthorised users.[95] In IT, confidentiality in ensured by data encryption, which allows for the translation of plaintext or unsecured information into an unreadable format known as ciphertext through the use of a secret key and an algorithm. The process of decrypting the ciphertext and restoring it to its original plaintext form is possible either with the utilisation of the same key that was employed for the encryption process (symmetric encryption), or using a public key to encrypt data and a private key to decrypt it (asymmetric encryption). The latter case,

[94] Duane, C. W. (2021). *Who Attacked Me?*. In *Cybersecurity*, MIT Press, p. 68.
Regulation (EU) 2021/887. Art. 2, para. 3.
[95] Duane, C. W. (2021). *Foundations*. In *Cybersecurity*, MIT Press, p. 11.

despite being a slower process and only applicable to relatively small quantities of data, ensures a higher level of security, as the private key, kept by the recipient of the data, is not shared and cannot so be intercepted. Contrariwise, in symmetric encryption, one of the main vulnerabilities is a non-secure key exchange; the transmission of the key from one party to the other creates an opportunity for the key to be intercepted by malicious actors, thereby compromising the confidentiality of the transmitted information. By combining the two encryption methods, security can be enhanced for large amounts of data while maintaining a high transmission speed. Specifically, the data is protected by symmetric encryption, while the key required to decrypt it is transmitted using asymmetric encryption.[96]

- Integrity: the assurance that systems and data are trustworthy, reliable, and accurate.[97] In order to ensure integrity, the cryptographic method "hashing" is employed – along with secure boot, which switches off the device in case of detection of a cyberattack. Hashing consists in converting any amount of data into a representation of it in the form of a string of text, or hash value, of fixed length. As the hash resulting from the same piece of data is always the same, the sender and the recipient of information can produce the hash value for the given piece of data independently and then compare it to verify that the information was not compromised. Apart from the secure boot, system integrity is also ensured by hashing procedures of the file system and the hard disk.[98]

[96] *Ibid.* p. 12.
Duane, C. W. (2021). *Cryptography Demystified*. In *Cybersecurity*, MIT Press, p.35-37.
Yeboah-Boateng, E. O. (2013). *Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)*. (1 ed.) Institut for Elektroniske Systemer, Aalborg Universitet. p. 42.
[97] *Op. cit.* Duane (2021). *Foundations*. p. 17.
Op. cit. Yeboah-Boateng (2013). p. 43.
[98] *Op. cit.* Duane (2021). *Foundations*. p. 38-39.

- Availability: the ability of a system, network, or data, to be accessible and operational when needed by authorised users.[99] Availability is ensured by security measures of different kinds, from cryptography to protect data and systems from unauthorised access, to redundancy measures such as backup servers. The variety of measures is due to the multiple ways that can cause the unavailability of a service. For instance, simply cutting cables can deny the communication between two or more parties, and backup measures such as communication via satellite could, in such case, function as an effective solution to maintain the service available. An example that shows how crucial the availability of service is for defence is the US Army Joint Targeting with the Advanced Field Artillery Tactical Data System (AFATDS). Used in missions that require a highly timely coordination among units, the system offers automated support to plan, coordinate, and execute fire support. [100] The unavailability of this service would result in the delayed coordination for targeting and a general decrease of situational awareness among different units, leading to an increased risk for the personnel and the possible failure of the mission.
- Authentication: strictly tied to integrity, but also to confidentiality, is the verification that a user accessing a certain service or set of data is who they claim to be. It is performed via the provision of specific data – e.g., a smart card, password, biometric information, or cryptographic keys – requested to pass through the access control. In regards to communications sessions, it ensures the identification of the parties and that the transmitted information is valid. [101] To increase the security of

[99] *Ibid.* p. 20.
Op. cit. Yeboah-Boateng (2013). p. 43.
[100] Hughes, D. (2022). *Joint Targeting with the Advanced Field Artillery Tactical Data System (AFATDS)*. Air Land Sea Space Application (ALSSA) Center.
[101] National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations*. p. 145.

this process, a multi-factor authentication (MFA) can be implemented.[102]

- Authorization: once passed the access control, the access to specific resources – i.e., files, applications – inside the system can be allowed or denied depending on the level of clearance (permission) of the user. If the access control lists, which determine the specific permissions of groups of users, allow the access, a user can either read or read and edit or execute a resource.[103]
- Nonrepudiation: implementing authentication and integrity, this principle uses measures such as the digital signature to prevent from the denial by a user that they performed a certain action, i.e., (not) receiving or sending certain data, approving and creating information.[104]

Maintaining a balance among the three pillars of information security – the CIA Triad – is crucial in ensuring the protection and security of data, services, and systems. Yet, the equilibrium of said balance depends on the particular requirements of each situation, and giving prioritizing one component over others can affect the overall security posture. If controls for confidentiality are overly implemented, accessing information becomes more complicated and time-consuming. On the other hand, too much focus on availability would compromise confidentiality, since the integrity of data may be lost as access controls to systems might be too feeble. Finally, too much emphasis on integrity may lead to unavailability, as users may face increased difficulties in accessing and modifying information, and to reduced system flexibility, making it more problematic to adapt to changes.[105]

---

[102] *Op. cit.* Duane (2021). *Foundations.* p. 23.
[103] *Ibid.* p. 24-25.
[104] *Op. cit*. Duane, C. W. (2021). *Cryptography Demystified*. p. 39-42.
Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology, U.S. Department of Commerce. p. 76.
[105] Tyson, J. (2019). *The CIA Triad*.

Satellite Communications

Satellite communications (satcom) consist in the communication between two or more terminals on Earth through the use of artificial satellites orbiting the planet in space, thus providing beyond line of sight (BLOS) communications.[106] Satcom operate wider radio frequency bands (e.g., Ku-band, Ka-band) than terrestrial communication infrastructure, allowing for high-speed transmission of larger amounts of data. In addition to data centres and user terminals, satcom consist of two components: the ground segment and the space segment. The uplink signal is transmitted from Earth to a satellite – space segment –, which, thanks to communications payloads, functions as a relay station that amplifies the received signal and transmits it back to the ground equipment.[107] Satcom are less likely to be subject to disruption and natural disasters, and provide an alternative to terrestrial communications where such infrastructure is highly challenging to deploy or when it is unavailable.[108] Satcom offer global coverage, real-time connectivity, and lower probability of detection than terrestrial links, also supporting a more secure communication for Command and Control (C2) and intelligence, and, in some cases, preclude the need for terrestrial relay infrastructure.[109] The current state of satcom results from remarkable advancements that have taken place since the 1960s; a brief historical overview of these developments is hereinafter presented.

In May 1961, US President John F. Kennedy delivered a speech, [110] where he called for the rapid development of satcom systems and services, acknowledging their potential for worldwide communication. In the same year,

---

[106] Joint Chiefs of Staff. (2022). *Department of Defense Satellite Communications*. p. A-1.
[107] INTELSAT. (19 May 2023, last accessed). *Satellite Basics*.
[108] EUSPA. (18 May 2023, last accessed). *What is Secure SatCom?*.
Labrador, V. (18 May 2023, last accessed). *Satellite Communication*. Britannica.
[109] Joint Chiefs of Staff. (2020). *Joint Publication 3-14. Space Operations*. p. II-5.
[110] Kennedy, J. F. (1961). *Special Message to the Congress on Urgent National Needs*. The American Presidency Project, UC Santa Barbara.

the United Nations Resolution 1721 recognized the potential impact of satcom for meeting the informational and operational needs of the UN and nation States, as well as for fostering international cooperation on a non-discriminatory basis.[111] Kennedy's speech and UN Resolution's vision for an interconnected world via satellite served as the foundation for the advancement of satcom technologies and their successful deployment by several organizations in the following few lustra. One such entity was the Communications Satellite Corporation (Comsat), founded in 1962 with the goal of developing a global commercial satcom network. In 1964, the two Interim Intelsat Agreements were signed, consisting of an Intergovernmental Agreement signed by governments, and a Special Agreement signed by participating telecommunication entities. They established Intelsat as an international organization, in the form of a consortium providing global satcom services and including more than eighty countries in less than a decade. The socialist organization Intersputnik, comprising eight countries, was founded in 1971.[112]

The 1960s marked a period of notable surge in the advancement of satcom technologies. 1960 saw the launch of the first active communications satellite, Courier 1B. Two years later, the Telstar and the Relay satellites were launched, showcasing the technical feasibility of satcom to support teletype, voice, and television. In 1963, the Syncom, the first geostationary communications satellites were launched. They transmitted the television signals from the 1964 Olympics held in Japan to the US, and subsequently to Europe via the Relay satellite.[113] With the involvement of additional organizations and countries in the development of such systems, the prospect of establishing a worldwide network of communication satellites became increasingly realistic. In 1969, the Intelsat III series was the first to complete a worldwide network, allowing for

[111] UN. General Assembly (16th sess.: 1961-1962). (1961). *International co-operation in the peaceful uses of outer space*. A/RES/1721(XVI)[B].
[112] Pelton, J. N. (2015). *History of Satellite Communications*. In: Handbook of Satellite Applications. p. 6.
[113] *Ibid.* p. 7-8.

the global transmission of voice and television communication. Communication satellites soon underwent an evolution from analog to digital services, which brought about benefits such as enhanced quality, increased data rates, and expanded capacity.[114]

Endeavours were also taken to create regional-level satcom systems. For instance, the European Telecommunications Satellite Organization (Eutelsat) was established in 1977 to provide satcom services to the European region. [115] The privatization of satcom organizations like Intelsat, Eutelsat, and Inmarsat began to take place in the 1980s. Nevertheless, in order to guarantee that they continued to meet their public service obligations, part of Intelsat and Inmarsat was maintained public.[116] Privatizing these organizations also allowed for increased competition and innovation within the satcom industry. As a result, the industry's evolution has not ceased, and has been characterized by new technologies and applications aimed at meeting the ever-growing demands of users. In summary, the 1980s constituted a decade that spurred progress, innovation and broadened the spectrum of satcom services available. Until the beginning of the 2000s, military and commercial users interchanged systems developed for the counterparts, also because commercial satcom systems were evolving faster. With the increasing military communications traffic due to the wars in Europe and the Gulf in the 1990s, and then in Iraq in 2003, dedicated military satellites could no longer provide the capacity and coverage needed to support operations. Consequently, alongside dedicated military communication satellites, States partially started leveraging commercial satellite capacity to augment their communication needs for defence-related purposes, and this trend continues to these days![117] Today, the space systems' application in military

[114] *Ibid.* p. 12-13.
[115] Eutelsat. (2023). *Our History*.
[116] *Op. cit.* Pelton (2015). p. 13-15.
[117] *Ibid.* p. 28-29
Stanniland, A. & Curtin, D. (2015). *An Examination of the Governmental Use of Military and Commercial Satellite Communications*. In: Handbook of Satellite Applications. p. 4, 6.

operations is widespread and multifaceted, underpinning any aspect from intelligence gathering and navigation to battlefield communication.

The reliance of armed forces on commercial satellites expands communication capabilities and flexibility. However, this practice carries risks connected to the security needs required to ensure military communications' integrity and confidentiality, such as commercial systems' protection of transmitted data, resilience against interferences, availability of services, or, finally, the trust placed upon industry for managing sensitive information. Depending on the particular needs, militaries access commercial satellites communication capabilities in different ways:[118]

- Hybrid satellites are commercial systems that, before being launched, are installed a Hosted Payload, that is, a military co-payload to satisfy the security needs without needing to build dedicated platforms.
- Long-term leases of services are preferred by nations with a lower threat assessment given the aforementioned risks and that have backup solutions for more sensitive data transmissions.
- Ad-hoc capacity leases do not guarantee the availability of service any time it is needed, presents lower system security, but can be an economically more desirable solution.
- Intergovernmental agreements serve allied countries to support each other's satcom either with dedicated satellites or via backup capabilities.

After examining satcom's evolution, it is essential to delve into the foundations that make satellites a central enabler for communications, in particular in military operations.

The deployment of communication satellites constellations on different orbits depends on the specific requirements and purposes of the satellites.

[118] *Op. cit.* Pelton (2015). p. 8.

The Medium-Earth Orbit (MEO), generally between 10,000 and 20,000 kilometres above Earth's surface, is mainly used for navigation purposes (Galileo, GPS, GLONASS, BeiDou).[119]

The Low-Earth Orbit (LEO) hosts satellites between 160 and 2,000 km above Earth and is widely used for communication. These satellites have an orbit period of about 90 minutes; in fact, a single satellite has a narrow coverage area – due to the low altitude – and is linked to a ground station for a brief period of time. In order to maintain the signal and provide continuous global coverage, LEO satellites usually work in constellations, that is, groups of satellites functioning in conjunction, but each of which capable of autonomous navigation.[120] Ground stations linked to these satellites require a movable antenna for complex tracking, and when a satellite moves out of range, it passes the signal to another satellite in the constellation to maintain the connection. Due to the LEO's close proximity to Earth, the delay of radio waves transmitting the signal is minimal, making it the preferred orbit for real-time communication.[121] Low latency becomes crucial for military operations, e.g., missile defence, long-range precision fires, as well as communication among units.[122] In 2021, Airbus and OneWeb – that already founded the 50/50 joint venture Airbus OneWeb Satellites in 2012[123] – signed a distribution partner agreement to offer LEO satcom services for military and governmental use in Europe. The OneWeb LEO constellation – comprised of 648 satellites upon complete deployment[124] –, in conjunction with Airbus technology, can so

[119] Ground Control. (22 May 2023, last accessed). *Satellite orbit heights, and how they impact satellite communication*.
[120] Abashidze, A., Chernykh, I., Mednikova, M. (2022). *Satellite constellations: international legal and technical aspects*. Acta Astronautica, 196 (2022), pp. 176-185. p. 177.
[121] *Op. cit.* Labrador, V. (18 May 2023, last accessed).
Op. cit. Ground Control (22 May 2023, last accessed).
INMARSAT. (2020). *Why geostationary satellites are good for government communications*.
[122] Sheftick, G. (2020). *Army looks to leverage 'low Earth orbit' satellites*. U.S. Army.
[123] OneWeb Satellites. (22 May 2023, last accessed). *About Us – Transforming the Space Industry*.
[124] OneWeb. (2023). *OneWeb confirms successful deployment of 16 satellites including next-generation JoeySat*.

provide advanced capabilities to European forces. These include integrated mesh networks and combat cloud, enabling resilient high-speed communications and the capacity to switch between LEO and Geostationary Orbit (GEO) satcom.[125]

GEO, also referred to as geosynchronous, equatorial orbit, or Clarke orbit,[126] hosts satellites that travel at an approximate velocity of 3 km per second at an altitude of 35,786 km. By doing so, they have the same rotation rate as that of the planet, thereby appearing fixed over a certain location on Earth, with ground stations' antennas being stationary – pointed to the same direction. Moreover, given Earth's distance, a single satellite can cover about one third of the planet's surface; three satellites positioned approximately 120° apart are thus enough to cover the entire Earth surface – except for some polar regions. These satellites have a longer lifespan than LEO satellites, which if combined with the less complex network (constellation and receiving antennas) results in a less expensive solution. However, the distance between GEO satellites and ground stations causes communication delays, which might be vital in critical situations. Nevertheless, Clarke orbit satellites can assist non-GEO satellites that require permanent availability.[127] This is the case with the European Data Relay Satellite System (EDRS), a laser communication network that uses inter-satellite links to deliver high speed data rates. It is composed of two GEO satellites, Operations and Control Centres, and ground stations. It provides direct support to Copernicus, enabling capabilities such as timely provision of

[125] Airbus, OneWeb. (2021). *Airbus and OneWeb étendent leur coopération pour connecter les forces européennes de défense et de sécurité*. p. 1.
[126] The name "Clarke Orbit" comes from Arthur C. Clarke, who, in 1945, stated that placing three satellites at about 42.000km from the Earth's equator, would make them "revolve with the earth and would thus be stationary above the same spot on the planet". Clarke, A.C. (1945). *Extra-Terrestrial Relays: Can Rocket Stations Give World-wide Radio Coverage?*.
[127] *Op. cit.* Labrador, V. (18 May 2023, last accessed).
European Space Agency. (2020). *Types of orbits*.
Telecommunication Engineering Centre. (2019). *Communication using Medium Earth Orbit (MEO) Satellites*.

Earth observation data, real-time mission reconfiguration of aircraft, or inter-unit communication.[128]

Cyber Threats to Satellite Communications

The space infrastructure facilitates the provision of data and services across all domains, and its protection against malicious interferences thus emerges as an imperative task, as any vulnerabilities might propagate and impact all other domains. To attain comprehensive protection, the allocation of resources towards the implementation of robust mitigation and resilience measures of space systems assumes paramount importance, especially in times of crisis escalation.

Particularly, the dynamic and evolving nature of cyber threats poses a substantial risk to key technologies. It is important to acknowledge that cyber vulnerabilities have a significant impact not only on the performance of systems in case of attack, but also on the trustworthiness of the cybersecurity tenets outlined above, with far-reaching effects on factors such as misperception, strategic calculus, and attack attribution.[129] Furthermore, the rapid execution and the difficulty of pre-emptively detecting and thwarting cyberattacks underscore the importance of identifying a system's potential vulnerabilities – e.g., conducting exercises – and establishing appropriate security measures to address such flaws. The potential impact and consequences of a cyberattack were demonstrated through an exercise carried out during the CYSAT, a European space cybersecurity event held in late April 2023. In this occasion, a group of researchers successfully took control of a demonstration nanosatellite belonging to the European Space Agency (ESA) and to introduce malicious

[128] European Space Agency. (17 July 2023, last accessed). *European Data Relay Satellite System (EDRS) Overview*.
European Space Agency. (22 May 2023, last accessed). *Overview*.
[129] Unal, B. (2019). *Cybersecurity of NATO's Space-based Strategic Assets*. Chatham House. p. 2-3.

code in its system, compromising the data sent back to Earth. [130] Although the exercise was carried out on a non-military satellite, it demonstrated the necessity for robust cybersecurity measures that can effectively thwart threats and ensure the availability of the assets, as well as the confidentiality and integrity of the data they transmit.

Cyber counterspace attacks targeting space systems encompass both "soft kill" (reversible) and "hard kill" (irreversible) attacks, as, for instance, the seizure of control of a satellite would enable the attacker to potentially damage or destroy it.[131] The strategic doctrine of countries such as China and Russia places significant emphasis on disrupting and preventing the satcom of adversaries in the context of military operations.[132] Temporary and expeditious attacks can be achieved with minor difficulty through electronic warfare, whereas inflicting more significant disruptions require a focus on the digital or physical elements of the systems.

In order to impact satcom, cyberthreats do not necessarily have to target communications links, but can also be directed to the space and ground segments, necessitating heightened attention and robust security measures. Ground stations serve as access points to satellites but may lack authentication measures to avoid interruptions of operational activities. Moreover, the software systems housed within these terminals require regular patching and upgrading to effectively address threats. Vulnerabilities also encompass the security of the supply-chain of components and critical technologies, leasing commercial satellites for military purposes, encryption backdoors, and personnel and procedural aspects. [133] Contributing to these vulnerabilities are factors such as

---

[130] Thales. (2023). *Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of its Kind*.
[131] Nardon, L. (2017). *European Space Programs and the Digital Challenge*. Ifri. p. 71.
[132] *Op. cit.* Unal (2019). p. 6.
U.S. Department of Defense. (2022). *Military and Security Developments Involving the People's Republic of China*. p. 93.
[133] *Op. cit.* Unal (2019). p. 7.

the proliferation of data exchange interfaces increasing the attack surface, inconsistencies among actors regarding the security standards applied to protect data networks, and the use of outdated software and hardware. [134]

Furthermore, secure data exchange via satellite necessitates the utilization of cryptography, a fundamental component in safeguarding the cybersecurity tenets. Cryptography assumes a critical role in protecting sensitive information by employing cryptographic keys to encrypt and decrypt data. Paramount importance shall also be accorded to the protection of these cryptographic keys to ensure the confidentiality and integrity of systems and data, as well as the authentication of users. However, as computational capacity continues to grow, attackers have access to more sophisticated capabilities that can accelerate the process of breaking encryption algorithms or uncovering cryptographic keys. This includes the potential utilization of quantum computers. Despite not being widely available yet, these computers have the ability to deliver more accurate and exponentially faster solutions to mathematical problems than classical computers,[135] making many widely used cryptographic algorithms susceptible to rapid decryption.

Recent developments in this area have been made, e.g., by Germany, whose Federal Office for Information Security (BSI) published the *Cyber-Sicherheit für Weltraumanwendungen* ("Cybersecurity for space applications"), that is, minimum requirements and guidelines for the cybersecurity management of space systems at various stages. [136] Another example come from the American Air Force Research Laboratory, which is planning to launch four cubesats to LEO to conduct real-world cybersecurity exercises. [137]

[134] *Ibid.* p. 8.
[135] The Australian Army. (2021). *Army Quantum Technology Roadmap*. p. 31.
[136] Bundesamt für Sicherheit in der Informationstechnik. (2022). *Cybersicherheit für Weltrauminfrastrukturen*.
[137] Erwin, S. (2022). *AFRL developing 'cyber range' for space operators*.

Addressing and mitigating threats and vulnerabilities requires a comprehensive approach that includes robust security measures, standardized protocols, and continual monitoring and system upgrades to uphold the integrity and resilience of military operations, and the EU is also making progress in this direction.

EU Cybersecurity and Space Systems Security Measures

As the EU continues to expand its activities in space, ensuring the security of space-based assets, systems, and sensitive information has become an utmost priority. In order to address these challenges, the EU has developed a range of policies, strategies, and initiatives with the objective of mitigating potential cyber threats across all domains. However, these do not always apply to the protection of critical space-related information. Nevertheless, although specific provisions do not directly apply to the EU space programmes, it is worth noting that the Union's general objectives and certain measures in the cyber domain can be regarded as best practices that can be extended to all domains, including space.

The first European cybersecurity strategy, adopted in 2013, outlined the objectives necessary to achieve the EU's resilience in this domain.[138] However, the first Directive on cybersecurity was only adopted in 2016. It was the Directive on Security of Network and Information Systems across the EU, commonly referred to as NIS Directive,[139] and was transposed into the national legislation of the Member States by 2020. During the intervening years, proposals were put forth to strengthen the EU's cyber resilience through a renovated mandate of the EU Agency for Network and Information Security (ENISA) and amendments to the NIS Directive. Among a number of measures, also in the area of cyber defence cooperation, the 2013 strategy was reviewed

[138] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.
[139] *Directive (EU) 2016/1148. L 194/1*.

in 2017, and Regulation (EU) 2019/881 ("Cybersecurity Act") was eventually approved, providing a cybersecurity certification framework.[140]

On 1-2 October 2020, the European Council convened a special meeting. The discussions tackled, among other topics, the digital sector, reiterating the importance of high capacity and secure network infrastructures, and the protection of communications against cyber threats, underscoring the use of quantum encryption.[141] 2 October 2020 was also the closing date of a public consultation launched by the Commission in July of the same year on the revision of the NIS Directive. The consultation revealed the heterogeneity of the Member States' approaches in identifying security requirements, thereby increasing the vulnerability to cross-border cyber threats.[142] As a result, on 16 December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the 2020-2025 EU's Cybersecurity Strategy for the Digital Decade. The proposed strategy involved a revision of the NIS Directive in order to establish rules pertaining to the cyber resilience of strategic sectors, as well as revising the legislation concerning critical infrastructures' resilience.[143]

After almost two years of trilogues – Parliament-Council-Commission negotiations –, the NIS2 Directive was adopted in December 2022 as Directive (EU) 2022/2555, and is currently being transposed into the national legislation of the Member States. The general objectives of the Directive include: (i) reinforcing the cyber resilience of both public and private entities across relevant sectors by means of harmonising cybersecurity, risk and incident

---

[140] European Commission. (2020). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*.
[141] European Council. (2020). *Conclusions – 1 and 2 October 2020. EUCO 13/20*.
[142] Negreiro Achiaga, M. (2022). *Review of the Directive on security of network and information systems (20/09/2022 update)*.
Negreiro Achiaga, M. (2023). *The NIS2 Directive – A high common level of cybersecurity in the EU*. p. 4.
[143] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. p. 5-6.
Op. cit. Negreiro Achiaga (2023). p. 3.

reporting management. (ii) Enhancing situational awareness, preparedness, and responsiveness during crises through the establishment of dedicated national authorities and of the EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe). (iii) Strengthening the NIS Cooperation Group.[144] Although the Directive identifies space as a sector of high criticality, [145] its provisions only apply to national and private space systems, thereby excluding those falling under the EU Space Programme from its range of applicability.[146] Nevertheless, it is specified by the NIS2 Directive that EUSPA should engage in the works of the NIS Cooperation Group, demonstrating the broad applicability of cybersecurity practices across different domains.[147] The group, among other tasks, is responsible for facilitating strategic cooperation, as well as information and best practices exchange not only among Member States, but also among various EU entities.[148]

In the realm of space systems, it is important to note that both ground and space segments are particularly vulnerable to cyberattacks. The protection of critical information can only be ensured through effective cybersecurity measures, adding up to a thorough analysis of in-orbit and on-the-ground behaviours of other actors. [149] On 10 March 2023, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy presented the European Union Space Strategy for Security and Defence, which emphasizes the cyber dimension of space. Moreover, in accordance with the EU's Cybersecurity Strategy for the Digital Decade, it draws attention to aspects such as: (i) the divergence among national legislations regulating security aspects of space operations, affecting the broader security of the EU. (ii) A

[144] Negreiro Achiaga (2023). p. 7-8.
[145] *Directive (EU) 2022/2555*. *L 333/80*. Annex I.
[146] *Ibid*. Preamble (37).
[147] *Ibid*. Preamble (66).
[148] *Ibid*. Art. 14 para. 4.
[149] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2023). *European Union Space Strategy for Security and Defence. JOIN(2023)9*. p. 2.

higher level of integration of (cyber)security standards in the design phase of space systems. (iii) The need for an EU-wide framework and coordinated national plans for the resilience of space systems. [150] The latest proposal would be further bolstered by the establishment of security monitoring centres intended to enhance Space Domain Awareness (SDA). In light of EUSPA's current responsibility as the operator of the Galileo Security Monitoring Centre, [151] the Strategy proposes expanding its role to incorporate the security monitoring of all space programmes.[152] The information analysed by EUSPA (via its security monitoring centres), in cooperation with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and ENISA, would allow to carry out risk and threat analyses about space assets, as well as a first level analysis of security incidents. As established by Council Decision (CFSP) 2021/698 on the security of systems and services under the Union Space Programme, and as reiterated in the Strategy, the security monitoring centres shall inform the High Representative, who shall immediately notify the Council about any identified threats. The Council – or the High Representative in cases of immediate urgency – shall subsequently instruct about the necessary measures to be undertaken in response to the threats. [153] As brought forward by the Strategy, an amendment of Council Decision (CFSP) 2021/698 would grant the Space Threat Response Architecture – operated by the EEAS – the authority to issue threat attribution and responses at technical, diplomatic, and economic level.[154] The Single Intelligence Analysis Capacity (SIAC) [155], operating under

[150] *Ibid.* p. 3-4.
[151] *Regulation (EU) 2021/696*. Art. 34, para. 5.
[152] It should be highlighted that the Strategy does not only mention the security monitoring of the Union Space Programme components, but "of all EU space programmes". This extends the role of the Agency to the security monitoring of IRIS^2, which is a space programme of the EU, but is not part of the Union Space Programme. *Op. cit.* European Commission and High Representative. (2023). *JOIN(2023)9*. p. 4.
[153] *Council Decision (CFSP) 2021/698. L 170/178*. Art. 2.
Ibid. p. 8.
[154] *Op. cit.* European Commission and High Representative. (2023). *JOIN(2023)9.* p. 8-9.
[155] Referred to as "Single Intelligence Analysis *Capability*" in the EU Space Strategy for Security and Defence.

the EU Military Staff (EUMS), in turn under the authority of the High Representative, would also support such function.[156]

Additionally, an initiative that shares similarities with the NIS Cooperation Group is the proposal of the EU Space Information Sharing and Analysis Centre (ISAC), with its primary goal being exchanging best practices for the (cyber) resilience of space systems among public and private entities. The creation of an EU Space ISAC can be facilitated by the EU-ISACs Consortium. [157]the EU Space ISAC can draw inspiration from and potentially engage in cooperation, on specific matters, with the Space ISAC born under the aegis of NASA, the US Space Force, and the National Reconnaissance Office;[158] as well as other entities such as the Cyber Information and Intelligence Sharing Initiative (CIISI-EU)[159] or the NATO Space Centre of Excellence.[160]

With regard to encryption, the EU recognises that technological advancements pose serious threats to the current encryption methods, and is implementing measures to provide stronger protection to critical information and communication. In particular, following the European Council conclusions of 1-2 October 2020, the Council of the EU issued the Council Resolution on Encryption on 24 November 2020. While the Resolution does not explicitly address the need for stronger encryption methods for military communications, it acknowledges the importance of establishing a regulatory framework within the EU that would enable competent authorities to effectively carry out their operational responsibilities while safeguarding the security of

[156] *Op. cit.* European Commission and High Representative. (2023). *JOIN(2023)9.* p. 9. European External Action Service. (2021). *CSDP structure, instruments and agencies*.
[157] For more information, see: Empowering EU-ISACs Consortium. (13 July 2023, last accessed).
[158] Space ISAC. (13 July 2023, last accessed). *About Space ISAC*.
[159] For more information, see: European Central Bank. (2020). *Cyber Information and Intelligence Sharing Initiative (CIISI-EU) - Cyber information and intelligence sharing: a practical example*.
[160] For more information, see: NATO Space Centre of Excellence. (13 July 2023, last accessed). *Discover Our Organisation*.

communication,[161] and reiterates the Council conclusions' emphasis on quantum encryption. Also, the Cybersecurity Strategy of December 2020, almost anticipating the forthcoming IRIS [2], takes an important step by delving more into the nexus between secure satcom and encryption through the European Quantum Communication Infrastructure (EuroQCI).[162]

[161] Council of the European Union. (2020). *Council Resolution on Encryption - Security through encryption and security despite encryption. 13084/1/20 REV 1*. p. 5.
[162] *Op. cit.* European Commission and High Representative. (2020). *EU Cybersecurity Strategy for the Digital Decade*. p. 7-8.

Quantum Technology for Defence and the EuroQCI

In the evolving landscape of space technology, quantum technology (QT) presents inherent features that hold the potential to revolutionize our approach to space strategies. This chapter provides an introduction to QT and its applications in space. It explores the potential battlefield of Quantum Warfare, delves into the potential of secure satellite communications via Quantum Key Distribution (QKD), and finally presents the ambitious European Quantum Communication Infrastructure (EuroQCI) initiative. This chapter aims to provide a glimpse into the future of space security and defence, and their potential implications for the EU's strategic approach to space.

Introduction to Quantum Technology and its Space Applications

Satellite communications (satcom) constitute a vital element in facilitating the transmission of data at a global scale, allowing defence actors to communicate faster than ever before and access near real time intelligence.[163] However, given the escalating sophistication of cyber threats, upholding the security of these communication systems is a matter of utmost importance. Conventional cryptographic techniques, which rely on assumptions and calculus of computational complexity, present inherent vulnerabilities when confronted with quantum computing capabilities – or more in general with quantum attacks.[164] In order to effectively tackle these challenges, the field of quantum technology (QT) emerges as a propitious option by leveraging the application, for instance, of Quantum Key Distribution (QKD) for satcom. In order to increase the comprehension of the use of QKD for secure communications, an overview of the field of QT and its applications in security and defence shall be presented.

---

[163] Frąckiewicz, M. (2023). *Military Applications of Satellite Communication*. In *TS2 Space*.
[164] Quantum attack "refers to using quantum technologies to break, disrupt or eavesdrop on either classical or quantum security systems". Krelina, M. (2021). *Quantum technology for military applications*. In *EPJ Quantum Technology 8, 24*. p. 3.

QT as dealt with in this research refers to the physics and engineering field based on quantum-mechanical properties applied to individual quantum systems[165] of the second quantum revolution. In fact, if the first quantum revolution was characterised by the emergence of technologies such as lasers and nuclear energy and weapons, which employ quantum phenomena, but do not control individual quantum systems, the current, second quantum revolution aims at controlling individual quantum systems with quantum-scale accuracy measurements.[166] In fact, quantum mechanics is the branch of physics that studies the behaviour of particles on the atomic and sub-atomic scale.[167] A system of particles or quasi-particles, such as photons or electrons, whose dynamics are dictated by the laws of quantum physics, is a quantum system. [168] Another important concept is quantum information science (QIS), which attempts to explain the flow of quantum information. The quantum information carriers are the quantum bits, commonly referred to as qubits. QT encompasses a wide range of technologies, such as quantum computing, quantum communication, quantum sensing, and quantum cryptography, and each of these exploits different features of quantum mechanics to address challenges that would otherwise remain difficult or even impossible to overcome.

The majority of quantum technologies present dual use characteristics, wherein they can have both civilian and military applications. Despite academic proposals to classify the quantum domain as a novel warfare domain, [169] quantum technologies are widely regarded as a factor that can considerably alter the nature of warfare, enhancing all conventional domains.[170] The ever-

---

[165] *Op. cit.* Krelina (2021). p. 3.
[166] *Op. cit*. The Australian Army. (2021). p. 6.
Ibid. p. 1-2.
[167] Badhwar, R. (2021). *Quantum Encryption Is Not a Paradox*. In *The CISO's Next Frontier*. p. 31.
Morin, D. (2008). *Introduction to quantum mechanics*. Ch, 10, 1-20. p. 1.
[168] *Op. cit*. The Australian Army. (2021). p. 25.
[169] Davidson, A. (2020). *A new dimension of war: the quantum domain*. Canadian Forces College.
[170] *Op. cit.* Krelina (2021). p. 2-3.

increasing importance of space capabilities in the realms of security and defence, coupled with the rapid advancements in QT, has fostered a confluence of these two fields, giving rise to numerous applications and establishing a tangible space quantum ecosystem supporting defence actors, with its main components being the following.

- Quantum sensing and imaging. The use of technologies such as quantum magnetometers, detectors, or quantum-enhanced magnetic resonance imaging, will allow for unprecedented sensitivity and precision in sensing and measuring diverse kinds of fields – gravitational, electric, magnetic, and mechanical – and dynamics – forces, acceleration, and rotation.[171] The main obstacles encountered by quantum sensing and imaging pertain to (i) environmental factors, which create noise that deteriorates the properties of the qubits. (ii) The relatively short dynamic range of measurand[172] values. (iii) The low update rate of quantum sensors. In order to address the challenges posed by the range and update rate limitations, the integration of quantum sensors with other sensor technologies emerges as a viable solution.[173] Differently, the application of quantum technologies in free-space environments, where the surrounding conditions can impact the performance of qubits, poses challenges that have not yet been fully addressed with practically exhaustive solutions.[174]

  These technologies have a wide range of applications by military actors. Placing quantum sensors on LEO satellites will allow for a highly accurate mapping of the planet's surface and for enhanced space situational awareness (SSA) and space surveillance and tracking (SST).

[171] *Op. cit*. The Australian Army. (2021). p. 27.
Krelina, M. (2023). *The Prospect of Quantum Technologies in Space for Defence and Security*. In *Space Policy*. p. 2.
[172] A "measurand" is the quantity that needs to be measured. International Organization for Standardization. (2008). *JCGM 100:2008(E)*. Annex D, D.1.1.
[173] *Op. cit*. The Australian Army. (2021). p. 27.
[174] *Ibid.* p. 26.

Quantum gravimeters, gravitational gradiometers, and magnetometry will facilitate Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) missions by topographical and underground mapping and by geolocating anomalies such as the presence, absence, high, or low concentration of a specific material in a given detection area. Moreover, these maps, as well as atomic clocks – also based on quantum mechanics – can be employed for positioning, navigation, and timing (PNT) in GNSS-denied environments.[175] Concerning quantum imaging, studies are ongoing to develop a "ghost imaging" satellite able to detect stealth aircraft.[176]

- Quantum communication. While a comprehensive analysis of this subject will also be provided in a subsequent section, it is apt to briefly discuss it within this framework. The strength of quantum communication does not lie in its data transfer speed rather in the unparalleled security it provides by protecting data through qubits. To maximize its potential applications, quantum communication can be combined with laser communication to provide a data security layer. [177] In fact, the very narrow beam of the laser provides laser links with characteristics such as low probability to detect (LPD) and to interfere (LPI). Moreover, laser communication allows for the transfer of 1000 times more data, 10 times faster than satcom based on the traditional radio-frequency bands. [178] Laser communication initiatives are already ongoing in the European context. In 2016, the SpaceDataHighway (SDH) partnership between the European Space Agency (ESA) – an

[175] *Op. cit*. Krelina (2021). p. 31-32.
Op. cit. Krelina (2023). p. 2.
[176] Trevithick, J. (29 June 2019, last update). *China Says It's Building a "Ghost Imaging" Satellite to Detect Stealth Jets*. The War Zone.
Van Amerongen, M. (2021). *Quantum technologies in defence & security*. NATO Review.
[177] *Op. cit*. Krelina (2023). p. 5.
[178] Airbus. (2021). *Airbus and TNO to develop aircraft laser communication terminal*.
Airbus. (2023). *Airbus and VDL Group join forces to produce an airborne laser communication terminal*.

intergovernmental organisation – and Airbus – a private company – created a laser communication infrastructure. The SDH enables LEO satellites data to be transferred using laser links to two GEO satellites hosting the payloads EDRS-A and EDRS-C of the European Data Relay Satellite System (EDRS), and from these satellites to ground stations in Europe.[179] The SDH will also serve UltraAir, a terminal for laser communications, again developed by Airbus in partnership with the VDL Group, and supported by other entities such as ESA though its ScyLight (Secure and Laser Communication Technology) programme, which will exploit the SDH to connect military aircraft to a multi-domain combat cloud.[180]

- Quantum countermeasure. Quantum satellites – satellites equipped with a quantum payload – are akin to their traditional counterparts, implying that they share analogous vulnerabilities with traditional satellites, leaving them exposed to the same kinds of counterspace weapons employed against conventional satellites or their communication links. These attacks can be thought of as analogous to electronic attacks targeting conventional communication links and the utilisation of laser weapons.[181]

The confluence of space capabilities and QT is forging a promising space quantum ecosystem to support defence actors. The continuous advancements in QT offer prospects to establish secure communication links and enhance sensing capabilities crucial for defence applications. As defence operations increasingly rely on space-based assets, the integration of quantum technologies within this domain offers the potential to provide resilient solutions, reinforcing security

[179] See section "Satellite Communications" for a brief outline about the European Data Relay Satellite System (EDRS).
Airbus. (Last accessed, 17 July 2023). *Laser Communications*.
Op. cit. European Space Agency. (17 July 2023, last accessed). *EDRS.*
[180] Airbus. (2023). *Airbus and VDL Group join forces to produce an airborne laser communication terminal*.
[181] *Op. cit*. Krelina (2023). p. 5.

measures and developing advanced defence capabilities. However, the emergence of quantum space warfare opens up a new range of threats and opportunities, calling for a more thorough examination of the relationship between quantum technologies and the security of space assets.

The next section will explore the complexities and implications arising in contemporary warfare from this emerging convergence, shedding light on risks and opportunities that demand attention of defence actors.

Quantum Warfare in Space

The convergence of quantum technologies and space-based assets opens up unparalleled potential to enhance SSA, data processing, secure satcom, and advanced sensing capabilities for defence purposes. Nevertheless, the integration of new technologies in the defence sector also introduces novel vulnerabilities that adversaries may exploit. Understanding the nuances of quantum space warfare is essential to develop effective strategies to protect the space (quantum) ecosystem and maintain space superiority.

Quantum computing, characterised by its power to perform complex calculations at unprecedented speeds, has the potential to facilitate rapid data processing and enable real-time decision-making capabilities. This could result in the form of faster target identification, optimised orbital manoeuvres, and a better analysis of enemy capabilities and behaviours, as well as in the possibility to model complex chemical reactions to design new materials or to crack cryptography or advanced artificial intelligence tools.[182]

In the area of quantum communications, (i) quantum key distribution (QKD) presents the ability to provide robust cryptographic security in the transmission of cryptographic keys, and to alert the sender and receiver in case of any

[182] Buchholz, S. *et al.* (2020). *The realist's guide to quantum technology and national security*. Deloitte.

eavesdropping attempt. (ii) A different application can be the quantum-secure direct communication (QSDC), which, through both single photons and entangled photons,[183] enables the transmission of low quantities of data without key distribution, mitigating the vulnerabilities related to the storage of cryptographic keys.[184] (iii) In position-based quantum cryptography, the geographical position of a party becomes the credential to access the information transmitted, as it is only accessible from that specific location – e.g., military bases. (iv) Through quantum digital signature (QDS), after signing a message, this becomes protected from possible intrusion or damage.[185] (v) Connected to the authentication tenet is the quantum secure identification, which, without exposing authentication credentials, enables user identification through quantum features.[186]

Establishing a secure quantum communication infrastructure can thus be vital in strengthening the confidentiality of communications. The distinctive characteristics of quantum communication channels set them apart from conventional communication channels, revolutionizing Signals Intelligence (SIGINT) and Communications Intelligence (COMINT): (i) as mentioned earlier in the paragraph, as quantum data is carried by individual quanta, any attempt to intercept the signal would be detected by the communicating parties. (ii) The low signal-to-noise ratio usually used by quantum imaging technologies makes it challenging to distinguish between signal and noise. (iii) As the quantum data is usually carried by coherent photons,[187] the behaviour of which

[183] Entangled photons are two particles that become and share the same quantum state, irrespective of the distance separating them, and an action on one of them affects the dynamics of the other one as well. Wolf, S.a. *et al*. (2019). *Overview of the Status of Quantum Science and Technology and Recommendations for the DoD*. Institute for Defence Analyses. p. 18.
[184] Also cryptographic keys transmitted via QKD are then stored in classical computers, which thus become the main target of cyberattacks.
Qi, R. *et al.* (2019). *Implementation and security analysis of practical quantum secure direct communication*. p. 2.
[185] *Op. cit*. Krelina (2021). p. 28.
[186] *Ibid.*
[187] Coherent photons are photons produced by lasers that oscillate in phase with each other, and have the same frequency. As such, they can create narrow light beams to securely transmit data over long distances.

is akin to that of a laser beam, it becomes extremely arduous to find the quantum communication link without knowledge of the position of at least one of the parties.[188]

Regarding quantum sensing and radar technologies, these could potentially enable stealth aircraft detection and tracking, bypassing traditional radar countermeasures, resulting in the continuation of the never-ending detection and evasion race, currently busy with the development of sixth generation fighter jets (SGFA).[189] In fact, characteristics of SGFA include radar-absorbent composite materials, next-generation jammers and spoofers to infiltrate adversary networks, features to reduce aircraft temperature, and a design, which unitedly strongly contribute to a decreased probability of detection of the fighter jets.[190] The SGFA encompasses various initiatives [191] across Europe, namely: the Global Combat Air Programme (GCAP),[192] which involves the joint efforts of the UK, Italy, Japan, and Sweden, with the Tempest[193] SGFA bringing together the UK, Italy, and Japan. Furthermore, France, Germany, and Spain are also collaborating to develop a Future Combat Air System (FCAS).[194]

However, quantum radars uses the principle of quantum entanglement where two particles become linked and share the same quantum state, irrespective of the distance separating them, and an action on one of them affects the dynamics

[188] *Op. cit*. Krelina (2021). p. 35.
[189] Sixth generation fighter jets or sixth generation fighter aircraft (SGFA).
[190] Aerospace & Defence Analyst. (2023). *Advancements in Sixth-Generation Stealth Technology: Escalating the battle of stealth and counter-stealth in military aviation*.
[191] Martin, T. (2023). *FCAS? SCAF? Tempest? Explaining Europe's sixth-generation fighter efforts*. Breaking Defense.
[192] Leonardo UK. (2022). *UK industry to play key role in new Global Combat Air Programme, delivering next phase of combat air fighter jet development*.
[193] For more information, see: Taylor, T. and Antinozzi, I. (2022). *The Tempest Programme – Assessing Advances and Risks Across Multiple Fronts*. Royal United Services Institute for Defence and Security Studies (RUSI).
Turato, M. (2022). *Tempest è il sistema Fcas del futuro. Parla il gen. Camporini*. Formiche.
[194] For more information, see: Airbus. (18 July 2023, last accessed). *Future Combat Air System (FCAS)*.

of the other one as well.[195] Therefore, if one of these particles interacts with an object, such as an aircraft, the other particle can provide information about the object. As this interaction does not depend on radio frequencies, the traditional stealth mechanisms of absorption and redirection are rendered ineffective, potentially impairing the evasion measures of stealth aircraft. In addition to that, the highly sensitive and precise quantum sensing and measurement capabilities would allow for the detection of changes in a wide range of physical phenomena – fields and dynamics –, thus increasing the possibility to detect and track even stealth aircraft.

Highlighting the swiftness of quantum warfare are also the Harvest Now, Decrypt Later (HNDL) attack method, and the prospective emergence of post-quantum cryptography, which employs mathematical problems that are more secure against attacks from quantum computers than traditional cryptography schemes, in particular asymmetric encryption.[196] In the HNDL method, the attacker acquires and stores encrypted data along with the corresponding encrypted keys, with the purpose of decrypting the data in the future, when quantum computing will be powerful enough to break the keys.[197]

Although the current state of quantum warfare in space is still in its early developmental phase, it shows significant effects on the present security and defence systems. The integration of QT within space systems, characterised by the ever-present dual-use conundrum, has the potential to lead to increase the likelihood of tensions and to an accelerated proliferation of capabilities in space with military purposes. At the same time, it also increases the necessity for multilateral endeavours to establish a regulatory framework that takes into

---

[195] Wolf, S. A. *et al*. (2019). *Overview of the Status of Quantum Science and Technology and Recommendations for the DoD*. Institute for Defence Analyses. p. 18.
[196] Chamola, V. *et al.* (2021). *Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography*. In: *Computer Communications*, 176, 99-118. p. 99, 106.
[197] *Op. cit*. Krelina (2021). p. 24.
Op. cit. Krelina (2023). p. 4.

account the different applications of quantum technologies in space. Such initiative could originate from the European Union, which is already active in the space quantum sector and in space law, respectively with the EuroQCI initiative and the prospective proposal of an EU Space Law, announced in the EU Space Strategy for Security and Defence,[198] as well as the 2014 International Code of Conduct for Outer Space Activities.[199]

Secure Satellite Communications via Quantum Key Distribution

Quantum Key Distribution (QKD) is a method of secure communication based on the laws of nature that leverages the principles of quantum mechanics to distribute cryptographic keys. While the keys necessary to access encrypted data are transmitted via quantum particles, the actual data is transmitted through conventional communication channels.[200] The physical carriers of information in QKD are typically photons, due to the fact that they can be easily controlled, they are the fastest-travelling qubits, and for their robustness.[201] Unlike classical cryptographic methods, QKD offers information-theoretic security, ensuring that any eavesdropping attempt can be detected, making it inherently secure. In fact, due to the no-cloning theorem, it is impossible to clone quantum states;[202] hence, any attempt to alter the quantum state of particles is detectable by the parties.

QKD represents a faster solution than traditional key exchange methods over long distances, while guaranteeing and enhancing the security of the transmission. In fact, a considerable amount of classified information is currently protected using symmetric encryption, involving the utilisation of a

[198] *Op. cit.* European Commission and High Representative. (2023). *JOIN(2023)9.* p. 3.
[199] European External Action Service. (2014). *DRAFT – International Code of Conduct for Outer Space Activities*.
[200] *Op. cit*. Van Amerongen (2021).
[201] Liao, SK., Cai, WQ., Liu, WY. *et al*. (2017). *Satellite-to-ground quantum key distribution*. In: *Nature* 549, 43–47.
[202] Wootters, W., Zurek, W. (1982). *A single quantum cannot be cloned*. Nature 299, 802–803. p. 802.

shared key known to both the sender and the receiver. Although this encryption method presents a high degree of resilience against decryption attempts, it requires the physical exchange of the keys, e.g., via hand courier, truck, or aircraft, rendering QKD a particularly suitable solution.[203]

The operational principles behind QKD rely on the peculiar characteristics of quantum particles. At its core are the concepts of quantum entanglement and quantum superposition, depending on the protocol chosen for the communication. The two most prominent QKD protocol classes are CV-QKD (Continuous Variable QKD) and DV-QKD (Discrete Variable QKD), with the latter being the most widely used for QKD via satellite. DV-QKD encompasses two kinds of protocols: prepare-and-measure, and entanglement-based-protocols.[204] The most extensively employed protocols are respectively the BB84, proposed by Bennett and Brassard in 1984,[205] and the E91 protocol, proposed by Artur Ekert in 1991.[206]

The BB84 protocol heavily relies on the no-cloning theorem, and does not require particles entanglement. Instead, it utilizes quantum superposition, a principle that allows a quantum system to exist in multiple states simultaneously. In quantum communication channels, the parties involved are commonly referred to as Alice, who sends the information; Bob, who receives it; and Eve – the eavesdropper. In this protocol, Alice uses photons to prepare a series of qubits, each representing a bit of the secret key. She randomly encodes each qubit in one of two non-orthogonal – or "diagonal" – (+45° and −45°) quantum states, typically using different polarizations of photons, which shifts their rectilinear (0° and 90°) polarization, represented with the states as $|0\rangle$ and

[203] *Op. cit*. Buchholz (2020).
[204] Bedington, R., Arrazola, J.M. and Ling, A. (2017). *Progress in satellite quantum key distribution*. In: *npj Quantum Inf* 3, 30. p. 2.
[205] Bennett, C.H. and Brassard, G. (1984). *Quantum Cryptography: Public Key Distribution and Coin Tossing*. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984, 175-179.
[206] Ekert, A. K. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67(6), p. 661-663.

|1⟩, into the non-orthogonal states |↗⟩ and |↖⟩, respectively.[207] The diagonal encoding, because of the uncertainty principle,[208] prevents Eve – and Bob – from extracting complete information from the photons. [209] At this point, Alice can send the qubits to Bob over a quantum communication channel, such as optical fibres or free-space communication. Upon receiving the qubits, Bob randomly chooses one of the two measurement bases (rectilinear or diagonal) to measure each qubit. The random choice ensures that he measures the qubits independently of Alice's choices during encoding, but it also increases the probability of errors and consequently of raw key bits loss.[210] In order to decrease this loss, Alice and Bob can pick the bases with significantly different probabilities. This increases the likelihood of both parties employing the same basis, thereby reducing the amount of discarded data, and thus achieving a notable improvement in efficiency.[211]

After the transmission, Alice and Bob communicate over a classical authenticated channel to disclose the bases they used for encoding and measuring each qubit. In this process called reconciliation, divided into error estimation and error correction, they retain only the measurements where they both used the same basis, discard the rest, and correct errors. Regarding free-space transmission, i.e., quantum-based satcom, the probability of errors exponentially increases, e.g., due to the noise generated by environmental

---

[207] Pivk, M. (2010). *Quantum Key Distribution*. In: Kollmitzer, C., Pivk, M. (eds). In: *Applied Quantum Cryptography*. Lecture Notes in Physics, vol 797. Springer, Berlin, Heidelberg. p. 24.

[208] According to Heisenberg's uncertainty principle, in quantum mechanics, it is not possible to measure simultaneously the position and the momentum (mass, times velocity) of a particle. For instance, if its momentum were to be predicted, the measurement of its position would result in all outcomes having equal probability to occur. Oppenheim, J. and Wehner, S. (2010). *The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics*. In: *Science*. 330,1072-1074.

[209] Bennett, C.H., Brassard, G., Crépeau, C. and Maurer, U. (1995). *Generalized Privacy Amplification*. In: *IEEE Transactions on Information Theory*, vol. 41, no. 6, p. 1915-1923. p. 3.

[210] *Op. cit*. Pivk (2010). p. 26.

[211] Lo, HK., Chau, H. and Ardehali, M. (2005). *Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*. J Cryptology 18, 133–165. p. 135.

conditions, the dimensions of the telescope receiving the information, or Bob's detection.[212] The step of authentication of the error correction then serves in verifying that during the reconciliation phase there has been no man-in-the-middle attack by Eve. Finally, the amplification phase is the process that distils the key from the shared raw key.[213]

Differently, the E91 protocol is based on quantum entanglement, and is thus more challenging to implement than the BB84 protocol.[214] Here, Alice, Bob, or a third party – such as a satellite – generates an entangled pair of photons; one is transmitted to Alice, and one to Bob. Once in possess of the particles, Alice and Bob measure them using a random measurement basis. Then, on a classical communication channel, they share the bases used, and the qubits that were measured in different bases will show whether (i) the photons are maximally entangled, forming a shared secure key, or (ii) the entanglement correlation presents errors, meaning that there were eavesdropping attempts, and that Alice and Bob have to start the process over.[215]

The first QKD experiment took place in 1989, when Bennett and Brassard managed to exchange a key at a distance of about 30 centimetres between the two parties.[216] After over thirty years of progress, QKD has reached a distance of 509 kilometres via optical fibre;[217] and 144 kilometres via free-space between two terrestrial points – the Canary Islands La Palma and Tenerife – without the

---

[212] Sharma, V. and Banerjee, S. (2018). *Analysis of Quantum Key Distribution based Satellite Communication*. p. 2.
[213] *Op. cit*. Bennett *et al.* (1995). p. 2.
[214] Krelina (2021). p. 13.
[215] Zhai, A. (2022). *An Overview of Quantum Key Distribution Protocols and Experimental Implementations*. p. 2-3.
Diep, D.N., Nagata, K. and Wong, R. (2020). *Continuous-Variable Quantum Computing and its Applications to Cryptography*. Int J Theor Phys 59, 3184–3188. p. 3185, 3187.
[216] Bennett, C. H. & Brassard, G. (1989). *Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working!*. ACM Sigact News 20, 78–80. p. 79-80.
[217] Chen J. P. *et al.* (2020). *Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km*. Phys Rev Lett. 124(7):070501.

use of quantum repeaters.[218] In 2016, China established the first successful satellite-to-ground QKD using the quantum-dedicated satellite Micius.[219] Nevertheless, the implementation of terrestrial free-space QKD encounters limitations due to the presence of environmental noise, rendering it unattainable for distances exceeding a few hundred kilometres without quantum repeaters. The use of satellites equipped with a quantum payload provides a viable solution for establishing long distance communication channels. Indeed, in light of the fact that the transmission travels for approximately only 10 kilometres through the atmosphere, which presents more noise than empty space, the satellite-to-ground link presents a much less significant attenuation compared to the terrestrial point-to-point free-space link and to the transmission via fibre.[220]

With the long-term goal being the creation of a global quantum communications network, terrestrial quantum repeaters do not represent the optimal solution because of issues connected to topographical factors, to the line-of-sight transmissivity, as well as to the physical security of the repeaters and the relatively low qubit transmission rates and high losses.[221] This is also why supporting the quantum communication network with space-based infrastructures appears like the necessary and most promising answer. The use of satellites mitigates the need for a large quantity of ground quantum repeaters, as a single trusted-node satellite can potentially cover the distance between the sender and the receiver, limiting the losses to the uplink and downlink channels alone. Moreover, in the case where more than one satellite is employed in the communication network, the advantages of inter-satellite communications

---

[218] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T. *et al*. (2007). *Entanglement-based quantum communication over 144 km*. Nature Phys 3, 481–486.
Quantum repeaters are intermediate nodes that operate in a way akin to the amplifier used in classical optical networks. However, a quantum repeater shall obey to the no-cloning theorem. *Op. cit*. Krelina (2021). p. 12.
[219] Liao, SK., Cai, WQ., Liu, WY. *et al*. (2017). *Satellite-to-ground quantum key distribution*. Nature 549, 43–47. p. 43, 44, 46.
[220] *Op. cit*. Bedington (2017). p. 1, 2.
[221] Sidhu, J.S., *et al*. (2021). *Advances in space quantum communications*. IET Quant. Comm. 2(4), 182– 217. p. 183, 185.

include decreased noise and loss compared to ground links, enhancing efficiency and reliability.[222] In order to reduce the likelihood of service unavailability, the quantum infrastructure could consist of a constellation of satellites and multiple optical ground stations (OGSs) situated in close proximity. Indeed, the reliability of quantum communication infrastructure can be significantly affected by environmental factors, such as cloud coverage, which can have a strong impact on the optical photon links used in QKD. However, considering the natural inhomogeneity of clouds, the simultaneous communication among one or more satellites and multiple OGSs would render the quantum communication infrastructure more reliable.[223]

The implementation of satellite-based QKD, nonetheless, presents additional challenges connected to the actualization of the key transmission as well as to its security. It is important to note that the deployment of a quantum communication space infrastructure is feasible in any orbit, wherein the associated challenges and advantages closely resemble those faced by traditional satcom. In Low-Earth Orbit (LEO), the satellites' proximity to the Earth's surface leads to reduced losses caused by beam diffraction. Nevertheless, the drawbacks include the fact that QKD can only be performed within the limited flyover time of the satellite above the OGS, and the satellite's high speed relative to the Earth's surface, making precise beam pointing during the transmission challenging. On the contrary, in Geostationary Orbit (GEO), the inherent characteristic of the satellite's fixed position in relation to the Earth's surface facilitates more accurate beam pointing and the potential for uninterrupted QKD. However, the trade-off in GEO is higher losses due to the greater distance from the OGS.[224]

---

[222] *Ibid*. p. 185.
[223] *Ibid*. p. 187.
Ntanos, A., Lyras, N.K., Zavitsanos, D., Giannoulis, G., Panagopoulos, A.D. and Avramopoulos, H. (2021). *LEO Satellites Constellation-to-Ground QKD Links: Greek Quantum Communication Infrastructure Paradigm*. Photonics 2021, 8, 544. p. 2.
[224] *Op. cit*. Bedington (2017). p. 3.

From a more general perspective on space-born QKD, additional natural challenges posed to the quantum signal that are being addressed by the scientific community can be, e.g., atmospheric turbulence, space radiation, thermal fluctuations of the optical systems on satellites, or background solar noise in daylight, which is the reason why, currently, quantum satcom are only realized at night.[225] Moreover, the security of QKD networks can be object of threats that are akin, under several aspects, to the counterspace weapons presented in the previous chapter. Among these is the Man in the Middle attack, that can also translate into a Photon-Number-Splitting attack. Following precaution measures, i.e., respectively sharing an initial key to establish the communication channel, and using single photons, can mitigate these threats.[226] Jamming, spoofing, and optical attacks can affect quantum satcom too, using light pulses directed towards photon detectors on OGSs and satellites. [227] Denial of Service attacks can consist in sending a high volume of fake traffic to the channel, as well as physically cutting fibre optic cables. [228] It is also worth noting that as long as the space QKD network is not dense, and thus presents a low level of interconnectivity, it will be very challenging to reroute transmission channels in case of service denial of a node. [229] Also, the increasing space congestion will become an obstacle for QKD performance.[230] Furthermore, cyberattacks and ASAT weapons can target quantum satellites, and OGSs are potential targets of physical and cyberattacks as well. The main threat to QKD lies in fact in the potential attacks to the hardware and software of the end and intermediate nodes. Their vulnerability lies in the fact that nodes – both satellites and devices in the OGSs – that store the data are conventional computers, that consequently lack the security provided by quantum mechanics, and are exposed to classical

[225] *Op. cit.* Sidhu (2021). p. 195-197.
[226] For more information, see: Badhwar (2021). p. 34-35.
[227] *Op. cit.* Sidhu (2021). p. 194.
Op cit. Badhwar (2021). p. 34-35.
[228] *Op. cit.* Badhwar (2021). p. 35.
[229] *Op. cit.* Krelina (2023). p. 6.
[230] *Op. cit.* Sidhu (2021). p. 195.

cyber threats and attacks. In fact, an inherent vulnerability often arises from the assumption that end nodes are trusted devices. This assumption is a critical keystone for the establishment of the security framework of QKD networks, as it is the basis of the security of the data and keys at rest. For instance, a malicious actor's tampering with the OGS could allow them to take control of the system and obtain the raw keys stored there. To counter threats relative to the security of traditional trusted devices and protect them from unauthorized access, stringent measures should be implemented for securing the nodes and rendering them soundly trustworthy. For instance, these devices shall be isolated and the public communication among them shall be authenticated. [231] Moreover, other measures include general procedures such as regular security audits, continuous intrusion detection, physical security measures for the facilities, software updates, following the principle of least privilege, strong encryption, and software and hardware security certification. [232]

The path to achieving this quantum revolution in space is not straightforward, and developing a wide space-based QKD infrastructure requires a collaborative effort that combines technological expertise, political commitment, and significant financial resources.

EuroQCI

The European Quantum Communication Infrastructure (EuroQCI) is an initiative aimed at establishing a global QKD service for actors within the European Union (EU), which covers all 27 Member States of the EU, including their overseas territories, and, in the long-term, a fully-fledged quantum communication network. It builds upon the Quantum Technologies Flagship initiative.[233] In this endeavour, the European Commission, which manages the

[231] *Ibid.* p. 195.
[232] *Op. cit*. Krelina (2021). p. 13.
[233] Quantum Flagship. (3 August 2023, last accessed). *Quantum Communication Infrastructure*.

programme,[234] the European Space Agency (ESA), and the Member States, are engaged in a collaborative effort to conceive, develop and implement the EuroQCI, comprising ground and space (SpaceQCI), and terrestrial (TerrQCI) segments. The terrestrial segment, which refers to earth-based connection between trusted nodes, differs from the ground segment, which refers to infrastructure necessary for the operations of the space segment.[235] The terrestrial segment will rely on fibre communication networks to link national and cross-border sites, while the space component will utilise satellites. The EuroQCI is set to become an integral part of the EU's satellite constellation for secure communication and worldwide broadband internet, i.e., the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²).[236] The PETRUS Project coordinates the implementation of the EuroQCI initiative. PETRUS is led by a consortium formed by Deutsche Telekom, Airbus, the Austrian Institute of Technology (AIT), and Thales.[237]

The Eagle-1 satellite, developed under a partnership between the Commission, ESA, and European space companies, set to launch in 2024, represents the first European satellite to demonstrate and validate QKD in Europe. In its three in-orbit years, it will generate valuable data for the deployment of the EuroQCI.[238]

The EU's endeavours in pursuing this route stem from its gradual acknowledgment of the need to establish a secure and reliable communication infrastructure, encompassing both space-based and terrestrial components, to

---

For additional information on the research goals of the Quantum Technologies Flagship concerning QKD, see: European Quantum Flagship. (2020). *Strategic Research Agenda of the Quantum Flagship*.

[234] European Commission Directorate-General for Communications Networks, Content and Technology. (2023). *EuroQCI Concept of Operations (ConOps) – Document Version 2.0 dated 19/06/2023*. p. 11.

[235] European Commission Directorate-General for Communications Networks, Content and Technology. (2023). p. 4.

[236] European Commission. (20 July 2023, last update). *The European Quantum Communication Infrastructure (EuroQCI) Initiative*.

[237] Williams, J. (3 August 2023, last accessed). *Deutsche Telekom leads build of high-security communications network for the EU*.
PETRUS. (3 August 2023, last accessed). *PETRUS Consortium*.

[238] European Space Agency. (3 August 2023, last accessed). *Eagle-1*.

ensure the provision of continuous and worldwide access to secure satellite communication services. As a result, the European Commission's proposal for an EU secure connectivity programme was endorsed by the parliamentary resolution of 17 February 2022, calling for its prompt completion. The initiation of governmental services is scheduled to begin in 2025, with subsequent implementation of private services.[239] The IRIS² infrastructure offers an excellent platform for deploying emerging cybersecurity technologies, such as QKD, as outlined in the EuroQCI declaration. [240] In fact, QKD will represent one of the main functions of the EuroQCI, although the current state of this QT is not sufficiently advanced to be used for the protection of EU classified information (EUCI). The standardisation of QKD protocols, along with side channel analysis and evaluation methodology, constitute important issues related to QKD security.[241] However, in regard to the first issue, it is important to note that there are ongoing advancements on the international level, but the decision to comply with international standards will ultimately rest with the EU. Specifically, the International Organization for Standardization (ISO) is developing the ISO/IEC 23837-1 and the ISO/IEC 23837-2, that is, the international standards "Information security – Security requirements, test and evaluation methods for quantum key distribution" – respectively "Part 1: Requirements" and "Part 2: Evaluation and testing methods" –, which are scheduled to be published in August 2023.[242]

As mentioned earlier, the EuroQCI comprises SpaceQCI and TerrQCI. The SpaceQCI is under the ownership of the EU, whereas the TerrQCI facilities are national infrastructures – or "Domains" –, which are managed and typically

[239] Evroux, C. (2023). *EU secure connectivity programme 2023-2027 – Building a multi-orbital satellite constellation*. European Parliamentary Research Service. p. 2-4.
[240] *Declaration of Cooperation Between Royaume de Belgique/Koninkrijk België and Bundesrepublik Deutschland and Reino de España and Repubblica italiana and Grand-Duché de Luxembourg and Republika ta' Malta and Koninkrijk der Nederlanden*. Digital Assembly 2019. (2019). p. 2.
[241] *Op. cit. Regulation (EU) 2023/588*. p. 4, para. 15.
[242] ISO. (3 August 2023, last accessed). *ISO/IEC 23837-1*.
ISO. (3 August 2023, last accessed). *ISO/IEC 23837-2*.

owned by Member States, or partially by the EU. In order to ensure the security sovereignty of Member States, the National Security Authority (NSA) or National Cyber-Security Agency (NCSA) of the Member State responsible for managing the respective Domain authorises the exchange of cryptographic keys between NatQCI Domains. When the key exchange is performed via satellite, i.e., via SpaceQCI, rather than TerrQCI's optical fibres, the NatQCI Domains involved can request to be connected to other Domains through the Quantum Hub (QH), which is responsible for managing these requests, including addressing any conflicts related to service and prioritisation. It is ought to be noted that not all NatQCI can be connected to SpaceQCI, as only specific TerrQCI nodes – known as QCI Space Interface Points (QSIP) – are interconnected with the space infrastructure.

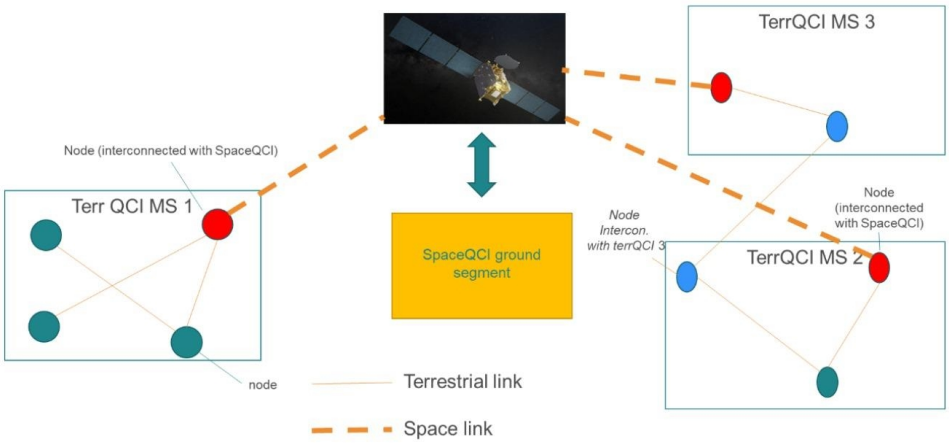

Figure 1 – Overview of the functioning of the EuroQCI.[243]

The responsibility for the security monitoring of the EuroQCI is entrusted to an entity that is tasked with the following duties: (i) monitoring that the

[243] *Op. cit.* European Commission Directorate-General for Communications Networks, Content and Technology. (2023). p. 11. [Figure].

management and operations of the Quantum Hub and SpaceQCI are conducted in accordance with the prescribed security requirements. (ii) In the event that the security requirements are not met, notifying the High Representative, as well as providing expertise regarding the impacts of, and responses to the nonconformity. (iii) Ensuring the cybersecurity of SpaceQCI and respond to potential security breaches. Here, a small step back shall be made. The EuroQCI, including its budget, was initially included in the Digital Europe Programme (DIGITAL) Work Programme 2021-2022, [244] which is an EU funding programme. However, the DIGITAL Work Programme 2023-2024, published on 24 March 2023, no longer covers the EuroQCI. [245] In fact, Regulation (EU) 2023/588 of 15 March 2023 establishing the Union Secure Connectivity Programme (USCP) took over the EuroQCI in order to develop the initiative and gradually integrate it into the USCP system. [246] The EuroQCI has so become an integral part of the governmental infrastructure of the secure connectivity system.[247] The protection of space and ground infrastructure – SpaceQCI –, as well as the provision of services against physical and cyberattacks, i.e., the security governance of the USCP, is a responsibility of the Commission, supported by the EU Agency for the Space Programme (EUSPA).[248] In fact, EUSPA is entrusted with several tasks, including the operational management of the governmental infrastructure, and its operational security; this includes its security monitoring, performing risk and threat analyses, setting procedures and monitoring their compliance with the general security requirements, which are determined by the risk and threat analyses. [249]

[244] European Commission. (2021). *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 – 2022. C(2021) 7914 final – annex*. p. 98-101.
[245] European Commission. (2023). *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024 and amending the Commission Implementing Decision C(2021) 7914 on the adoption of the multiannual work programme for 2021-2022. C(2023) 1862 final – annex 1*. p. 3.
[246] *Op. cit. Regulation (EU) 2023/588*, art. 3(2c).
[247] *Ibid.* art. 5(2b).
[248] *Ibid.* art. 30(1).
[249] *Ibid.* art. 27(2), 30(3).

Furthermore, as proposed in the EU Space Strategy for Security and Defence, EUSPA could be responsible for the security monitoring of all space programmes of the EU. In such position, in case of security incidents, EUSPA would also perform first level analyses and notify the High Representative. [250] Such context suggests an exponential increase of EUSPA's role in the area of the security governance of the EU space programmes.

The objectives and the use cases of each NatQCI Domain differ among Member States and Domains. For instance, use cases of National QCI involve, among others, research, secured healthcare information, authorities communication, secure critical infrastructure, or defence and military. Interestingly, only 9 out of 27 Member States have presently identified defence and military among their use cases, according to PETRUS.[251] Namely, these are Belgium, Bulgaria, Czechia, Denmark, Estonia, Latvia, Portugal, and Romania.[252]

EuroQCI represents not merely an advanced technology initiative, but a crucial framework that ensures the resilience and security of communication infrastructures within European authorities and defence actors. The differences in the objectives and use cases of each NatQCI Domain among Member States underscore the diverse potential applications of QKD. A European quantum communication infrastructure is not just a technological leap, but a strategic endeavour that could integrate QT into everyday applications and that could empower Europe to be at the forefront of the ongoing quantum revolution, fostering innovation while safeguarding its cyberspace.

[250] *Op. cit.* European Commission and High Representative. (2023). *JOIN(2023)9*. p. 8.
[251] Although all 27 Member States have signed the EuroQCI Declaration, Lithuania's objectives and use cases have not been laid out yet. PETRUS. (3 August 2023, last accessed).
[252] *Op. cit.* PETRUS. (3 August 2023, last accessed).

Conclusion

In an era characterised by the pervasive integration of technology and militarization, quantum-based capabilities offer the promise to enhance security through space. This research attempted to shed light on such transformative advancements in order to provide the European Union (EU) with the insights required to address the prospective challenges and opportunities in space.

The investigation of quantum technologies, especially for secure satellite communications, has navigated an exploration of the intersection between quantum physics and their disruptive potential for defence purposes. However, while these prospects hold great potential, it is imperative to allocate adequate investments for the integration of these technologies into the EU's space infrastructure.

Furthermore, the ongoing evolution of the EU's space strategy, which emphasises security and defence, highlights the advantages of centralising all matters related to space security within a single EU body.

Lastly, there exists an urgent need for comprehensive international regulations extending beyond traditional space threats. As humanity embarks upon the quantum era and faces the potential weaponization of space, new legislation should be forward-thinking, taking into account the emerging technological developments that pose threats to the stability and peace in space.

The future of the EU in space appears to be bright, yet more complex than ever. Quantum technologies, although displaying considerable potential, present a unique array of challenges that need to be strategically addressed. Investing adequately, centralising efforts, and initiating international regulatory action are thus essential steps towards a secure future in EU's space endeavours.

Bibliography

Abashidze, A., Chernykh, I., Mednikova, M. (2022). *Satellite constellations: international legal and technical aspects*. Acta Astronautica, 196 (2022), pp. 176-185. https://doi.org/10.1016/j.actaastro.2022.04.019

Aerospace & Defence Analyst. (2023). *Advancements in Sixth-Generation Stealth Technology: Escalating the battle of stealth and counter-stealth in military aviation*. https://www.financialexpress.com/business/defence-advancements-in-sixth-generation-stealth-technology-escalating-the-battle-of-stealth-and-counter-stealth-in-military-aviation-3078771/

Airbus, OneWeb. (2021). *Airbus and OneWeb étendent leur coopération pour connecter les forces européennes de défense et de sécurité*. https://www.airbus.com/sites/g/files/jlcbta136/files/2021-12/EN_Airbus-Press-Release-Oneweb.pdf

Airbus. (18 July 2023, last accessed). *Future Combat Air System (FCAS)*. https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas

Airbus. (2021). *Airbus and TNO to develop aircraft laser communication terminal*. https://www.airbus.com/en/newsroom/press-releases/2021-04-airbus-and-tno-to-develop-aircraft-laser-communication-terminal

Airbus. (2023). *Airbus and VDL Group join forces to produce an airborne laser communication terminal*. https://www.airbus.com/en/newsroom/press-releases/2023-01-airbus-and-vdl-group-join-forces-to-produce-an-airborne-laser

Airbus. (Last accessed, 17 July 2023). *Laser Communications*. https://securecommunications.airbus.com/en/pioneering/laser-communications

Altheide, D. L. (1996). *Qualitative Media Analysis*. Thousand Oaks, CA: Sage Publications, Inc. https://doi.org/10.4135/9781412985536

Badhwar. (2021). *Quantum Encryption Is Not a Paradox*. In: *The CISO's Next Frontier*. https://doi.org/10.1007/978-3-030-75354-2_3

Bedington, R., Arrazola, J.M. and Ling, A. (2017). *Progress in satellite quantum key distribution*. In: *npj Quantum Inf* 3, 30. https://doi.org/10.1038/s41534-017-0031-5

Bennett, C. H. & Brassard, G. (1989). *Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working!*. ACM Sigact News 20, 78–80. https://doi.org/10.1145/74074.74087

Bennett, C.H. and Brassard, G. (1984). *Quantum Cryptography: Public Key Distribution and Coin Tossing*. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984, 175-179. https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf

Bennett, C.H., Brassard, G., Crépeau, C. and Maurer, U. (1995). *Generalized Privacy Amplification*. In: *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915-1923. https://doi.org/10.1109/18.476316

Bowen, B. E. (2019). *From the sea to outer space: The command of space as the foundation of spacepower theory*. In: Journal of Strategic Studies, 42:3-4, 532-556. https://doi.org/10.1080/01402390.2017.1293531

Bowen, B. E. (2020). *War in Space: Strategy, Spacepower, Geopolitics*. Edinburgh University Press. https://doi.org/10.3366/edinburgh/9781474450485.001.0001

Bryman, A. (2012). *Social Research Methods*. 4th edition, Oxford: Oxford University Press.

Buchholz, S. et al. (2020). *The realist's guide to quantum technology and national security*. Deloitte. https://www.deloitte.com/global/en/our-thinking/insights/industry/government-public-services/the-impact-of-quantum-technology-on-national-security.html

Bundesamt für Sicherheit in der Informationstechnik. (2022). *Cybersicherheit für Weltrauminfrastrukturen*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Weltrauminfrastrukturen/Cyber-Sicherheit_Weltrauminfrastrukturen.pdf?__blob=publicationFile&v=3

Callwell, C.E. (1905). *Military Operations and Maritime Preponderance: Their Relations and Interdependence*.

Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021). *Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography*. In: *Computer Communications*, 176, 99-118. https://doi.org/10.1016/j.comcom.2021.05.019

Chen JP, Zhang C, Liu Y, Jiang C, Zhang W, Hu XL, Guan JY, Yu ZW, Xu H, Lin J, Li MJ, Chen H, Li H, You L, Wang Z, Wang XB, Zhang Q, Pan JW. (2020). *Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km*. Phys Rev Lett. 124(7):070501. https://doi.org/10.1103/physrevlett.124.070501

Clarke, A.C. (1945). *Extra-Terrestrial Relays: Can Rocket Stations Give World-wide Radio Coverage?*. https://doi.org/10.1016/B978-1-4832-2716-0.50006-2

Copernicus Service in Support to EU External Action. *About Copernicus SEA*. https://sea.security.copernicus.eu/about-copernicus-sea/

Copernicus. *Copernicus in detail*. https://www.copernicus.eu/en/about-copernicus/copernicus-detail

Copernicus. *Copernicus Programme*. https://www.copernicus.eu/sites/default/files/documents/Copernicus_Programme_v2.pdf

Copernicus. *Infrastructure Overview*. https://www.copernicus.eu/en/about-copernicus/infrastructure-overview

Corbett, J. S. (1911). *Some principles of maritime strategy*. London: Longmans, Green.

Council of the European Union. (2020). *Council Resolution on Encryption - Security through encryption and security despite encryption. 13084/1/20 REV 1*. https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

Council of the European Union. (2021). *Council Decision (CFSP) 2021/698 of 30 April 2021on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP. L 170/178.* http://data.europa.eu/eli/dec/2021/698/ojt

Council of the European Union. (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. 7371/22.* https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

Curtis E. LeMay Center for Doctrine Development and Education (2021). *Air Force Doctrine Publication (AFDP) 3-14 Counterspace Operations*. United States Air Force. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf

Davidson, A. (2020). *A new dimension of war: the quantum domain*. Canadian Forces College. https://vdocuments.site/a-new-dimension-of-war-the-quantum-domain-a-new-dimension-of-war-the-quantum.html?page=1

Declaration of Cooperation Between Royaume de Belgique/Koninkrijk België and Bundesrepublik Deutschland and Reino de España and Repubblica italiana and Grand-Duché de Luxembourg and Repubblika ta' Malta and Koninkrijk der Nederlanden. Digital Assembly 2019. (2019). Available via: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

Diep, D.N., Nagata, K. and Wong, R. (2020). *Continuous-Variable Quantum Computing and its Applications to Cryptography*. Int J Theor Phys 59, 3184–3188. https://doi.org/10.1007/s10773-020-04571-5

Directorate-General for Defence Industry and Space. (2021). *Overview*. https://defence-industry-space.ec.europa.eu/system/files/2021-04/DEFIS_EU_SPACE_GOVSAT%20-%20Overview.pdf

Directorate-General for Defence Industry and Space. (2021). *Support to Border and Maritime Surveillance*. https://defence-industry-space.ec.europa.eu/system/files/2021-04/DEFIS_EU_SPACE_GOVSAT%20-%20Border%20Maritime%20Surveillance.pdf

Directorate-General for Defence Industry and Space. (2021). *Support to Key Infrastructure Management*. https://defence-industry-space.ec.europa.eu/system/files/2021-04/DEFIS_EU_SPACE_GOVSAT%20-%20Infrastructure_0.pdf

Directorate-General for Defence Industry and Space. (2023). *IRIS² - Factsheet (EN)*. https://defence-industry-space.ec.europa.eu/system/files/2023-03/IRIS%C2%B2_Factsheet%20%28EN%29.pdf

Directorate-General for Defence Industry and Space. *Safety-of-Life Service*. https://defence-industry-space.ec.europa.eu/eu-space-policy/egnos/safety-life-service_en

Directorate-General for Defence Industry and Space. *Support to Crisis Management Operations*. https://defence-industry-space.ec.europa.eu/govsatcom/support-crisis-management-operations_en

Dolman, E. C. (2002). *Astropolitik – Classical Geopolitics in the Space Age*. (1st ed.). Routledge. https://doi.org/10.4324/9780203016640

Duane, C. W. (2021). *Cryptography Demystified*. In Cybersecurity, MIT Press. https://doi-org.ezproxy.lib.gla.ac.uk/10.7551/mitpress/11656.003.0005

Duane, C. W. (2021). *Foundations*. In Cybersecurity, MIT Press. https://doi-org.ezproxy.lib.gla.ac.uk/10.7551/mitpress/11656.003.0004

Duane, C. W. (2021). *Who Attacked Me?*. In: Cybersecurity, MIT Press. https://doi-org.ezproxy.lib.gla.ac.uk/10.7551/mitpress/11656.003.0007

EGNOS User Support. *About EGNOS*. https://egnos-user-support.essp-sas.eu/egnos-system/about-egnos

Ekert, A. K. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67(6). https://doi.org/10.1103/PhysRevLett.67.661

Empowering EU-ISACs Consortium. (13 July 2023, last accessed). https://www.isacs.eu/#services

Erwin, S. (2022). *AFRL developing 'cyber range' for space operators*. SpaceNews. https://spacenews.com/afrl-developing-cyber-range-to-test-vulnerabilities-of-space-networks/

ESA. *What is Galileo?* https://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo

European Central Bank. (2020). *Cyber Information and Intelligence Sharing Initiative (CIISI-EU) - Cyber information and intelligence sharing: a practical example* https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_practical_example.pdf

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2023). *European Union Space Strategy for Security and Defence. JOIN(2023)9.* Accessible via: https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en

European Commission Directorate-General for Communications Networks, Content and Technology. (2023). *EuroQCI Concept of Operations (ConOps) – Document Version 2.0 dated 19/06/2023*. Available via: https://digital-strategy.ec.europa.eu/en/euroqci-conops-concept-operations

European Commission. (20 July 2023, last update). *The European Quantum Communication Infrastructure (EuroQCI) Initiative*. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

European Commission. (2020). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Commission. (2021). *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 – 2022. C(2021) 7914 final – annex*. https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf

European Commission. (2023). *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024 and amending the Commission Implementing Decision C(2021) 7914 on the adoption of the multiannual work programme for 2021-2022. C(2023) 1862 final – annex 1*. Available via: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital

European Council. (2020). *Conclusions – 1 and 2 October 2020. EUCO 13/20*. https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

European External Action Service. (2014). *DRAFT – International Code of Conduct for Outer Space Activities*. https://www.eeas.europa.eu/sites/default/files/space_code_conduct_draft_vers_31-march-2014_en.pdf

European External Action Service. (2021). *CSDP structure, instruments and agencies*. https://www.eeas.europa.eu/eeas/csdp-structure-instruments-and-agencies_en

European GNSS Service Centre. (2020). *SAR/Galileo Service Definition Document*. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-SAR-SDD.pdf

European GNSS Service Centre. (2021). *Galileo – Open Service – Service Definition Document*. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OS-SDD_v1.2.pdf

European GNSS Service Centre. (2023). *Galileo High Accuracy Service – Service Definition Document (HAS SDD)*. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-HAS-SDD_v1.0.pdf

European GNSS Service Centre. *Constellation Information.* https://www.gsc-europa.eu/system-service-status/constellation-information

European GNSS Service Centre. *FAQ*. https://www.gsc-europa.eu/galileo/faq#PRS

European GNSS Service Centre. *Services*. https://www.gsc-europa.eu/galileo/services

European Parliament and Council of the European Union. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. L 194/1*. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Parliament and Council of the European Union. (2021). *European Parliament and Council Regulation (EU) 696/2021 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. (2021). OJ L 170/69.* https://eur-lex.europa.eu/eli/reg/2021/696/oj

European Parliament and Council of the European Union. (2021). *Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. (2021). L 202/1*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0887

European Parliament and Council of the European Union. (2022). *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). L 333/80*. http://data.europa.eu/eli/dir/2022/2555/oj

European Parliament and Council of the European Union. (2023). *European Parliament and Council Regulation (EU) 2023/588 of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027. (2023). OJ L 79/1*. https://eur-lex.europa.eu/eli/reg/2023/588

European Quantum Flagship. (2020). *Strategic Research Agenda of the Quantum Flagship*. Accessible via: https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies

European Space Agency. (2020). *Types of orbits*. https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

European Space Agency. (22 May 2023, last accessed). *European Data Relay Satellite System (EDRS) Overview*. https://artes.esa.int/european-data-relay-satellite-system-edrs-overview

European Space Agency. (22 May 2023, last accessed). *Overview*. https://www.esa.int/Applications/Telecommunications_Integrated_Applications/EDRS/Overview

European Space Agency. (3 August 2023, last accessed). *Eagle-1*. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1

European Space Policy Institute (ESPI). (2022). *ESPI Short Report 1 - The war in Ukraine from a space cybersecurity perspective*.

https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf

EUSPA. (18 May 2023, last accessed). *What is Secure SatCom?*. https://www.euspa.europa.eu/european-space/eu-space-programme/what-secure-satcom

EUSPA. (2021). *GOVSATCOM*. https://www.euspa.europa.eu/european-space/govsatcom

EUSPA. (2022). *EUSPA takes on the Space Surveillance and Tracking helpdesk as of 2023*. https://www.euspa.europa.eu/newsroom/news/euspa-takes-space-surveillance-and-tracking-helpdesk-2023

EUSPA. (8 June 2023, last accessed). *Space Situational Awareness*. https://www.euspa.europa.eu/european-space/space-situational-awareness

Eutelsat. (2023). *Our History*. https://www.eutelsat.com/en/group/our-history.html

Evroux, C. (2023). *EU secure connectivity programme 2023-2027 – Building a multi-orbital satellite constellation*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729442/EPRS_BRI(2022)729442_EN.pdf

Frąckiewicz, M. (2023). *Military Applications of Satellite Communication*. In: TS2 Space. https://ts2.space/en/military-applications-of-satellite-communication/

Geppert, A.C. (2018). *European Astrofuturism, Cosmic Provincialism: Historicizing the Space Age*. In: Geppert, A. (eds). *Imagining Outer Space*. Palgrave Studies in the History of Science and Technology. Palgrave Macmillan, London. https://doi.org/10.1057/978-1-349-95339-4_1

Gray, C. S. (1999). *Modern Strategy*. Oxford University Press.

Ground Control. (22 May 2023, last accessed). *Satellite orbit heights, and how they impact satellite communication*. https://www.groundcontrol.com/en/knowledge/guides/satellite-orbit-heights-impact-satellite-communication/

GSA. (2021). *EGNOS Safety of Life (SoL) – Service Definition Document*. https://egnos-user-support.essp-sas.eu/sites/default/files/library/official_docs/egnos_sol_sdd_in_force.pdf

Harrison, T et al. (2022). *Space Threat Assessment 2022*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220404_Harrison_SpaceThreatAssessment2022.pdf?VersionId=DfdcNDlBOYINwhkIVeqfSJ.yfmOx_5ZB

Hebert, K. D. (2014). *Regulation of space weapons: Ensuring stability and continued use of outer space*. Astropolitics, 12(1), 1-26. https://doi.org/10.1080/14777622.2014.890487

Hitchens, T., Katz-Hyman, M., and Lewis, J. (2006). *U.S. SPACE WEAPONS: Big intentions, little focus*. The Nonproliferation Review, 13(1), 35-56. https://doi.org/10.1080/10736700600861350

Hughes, D. (2022). *Joint Targeting with the Advanced Field Artillery Tactical Data System (AFATDS)*. Air Land Sea Space Application (ALSSA) Center. https://www.alsa.mil/News/Article/3043548/joint-targeting-with-the-advanced-field-artillery-tactical-data-system-afatds/

INMARSAT. (2020). *Why geostationary satellites are good for government communications*. https://www.inmarsat.com/en/insights/government/2020/why-geostationary-satellites-are-good-for-government-communications.html

INTELSAT. (19 May 2023, last accessed). *Satellite Basics*. https://www.intelsat.com/resources/tools/satellite-101/

International Organization for Standardization. (2008). *JCGM 100:2008(E)*. https://www.iso.org/sites/JCGM/GUM/JCGM100/C045315e-html/C045315e_FILES/MAIN_C045315e/Start_e.html

ISO. (3 August 2023, last accessed). *ISO/IEC 23837-1*. https://www.iso.org/standard/77097.html

ISO. (3 August 2023, last accessed). *ISO/IEC 23837-2*. https://www.iso.org/standard/77309.html

Jakhu, R. S. and Freeland, S. (eds.). (2022). *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I – Rules*. Montreal: Centre for Research in Air and Space Law. https://www.mcgill.ca/milamos/files/milamos/mcgill_manual_volume_i_-_rules_final_0.pdf

Johnson-Freese, J. (2016). *Space Warfare in the 21st Century: Arming the Heavens*. (1st ed.). Routledge. https://doi.org/10.4324/9781315529172

Joint Chiefs of Staff. (2020). Joint Publication 3-14. Space Operations. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdfr

Joint Chiefs of Staff. (2022). *Department of Defense Satellite Communications*. https://www.jcs.mil/LinkClick.aspx?fileticket=2U2SkBz2Ews%3d&tabid=19767&portalid=36&mid=46626

Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Jones, B. A., Bryant, D. S., Vo, B. -T., and Vo B. -N. (2015). *Challenges of multi-target tracking for space situational awareness*. 18th International Conference on Information Fusion (Fusion), Washington, DC, USA. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7266704

Kennedy, J. F. (1961). *Special Message to the Congress on Urgent National Needs*. The American Presidency Project, UC Santa Barbara. https://www.presidency.ucsb.edu/documents/special-message-the-congress-urgent-national-needs

Klein, J. J. (2005). *Space Warfare – Strategy, Principles and Policy*. (1st ed.). Routledge. https://doi.org/10.4324/9780203963982

Klein, J. J. (2012). *Space Strategy Considerations for Medium Space Powers*. In: Astropolitics, 10:2, 110-125. https://doi.org/10.1080/14777622.2012.698929

Krelina, M. (2021). *Quantum technology for military applications*. In: EPJ Quantum Technology 8, 24.

Krelina, M. (2023). *The Prospect of Quantum Technologies in Space for Defence and Security*. In: Space Policy. https://doi.org/10.1016/j.spacepol.2023.101563

Krepon, M., & Clary, C. (2003). *Is the Weaponization of Space Inevitable?. In Space Assurance or Space Dominance?: THE CASE AGAINST WEAPONIZING SPACE (pp. 28–57)*. Stimson Center. http://www.jstor.org/stable/resrep10980.7

Labrador, V. (18 May 2023, last accessed). *Satellite Communication*. Britannica. https://www.britannica.com/technology/satellite-communication

Leonardo UK. (2022). *UK industry to play key role in new Global Combat Air Programme, delivering next phase of combat air fighter jet development*. https://uk.leonardo.com/en/news-and-stories-detail/-/detail/uk-industry-to-play-key-role-in-new-global-combat-air-programme-gcap

Liao, SK., Cai, WQ., Liu, WY. et al. (2017). *Satellite-to-ground quantum key distribution*. Nature 549, 43–47. https://doi.org/10.1038/nature23655

Lo, HK., Chau, H. and Ardehali, M. (2005). *Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*. J Cryptology 18, 133–165. https://doi.org/10.1007/s00145-004-0142-y

Macci, F. (2023). *The Growth of the Moroccan Military Air Power*. Moroccan Institute for Policy Analysis. https://mipa.institute/en/10553

Mahan, A. T. (1660–1783). *The Influence of Sea Power upon History*. Marston & Co., London, 1890. https://doi.org/10.1017/CBO9780511783289

Martin, T. (2023). *FCAS? SCAF? Tempest? Explaining Europe's sixth-generation fighter efforts*. Breaking Defense. https://breakingdefense.com/2023/06/fcas-scaf-tempest-explaining-europes-sixth-generation-fighter-efforts/

McLaughlin, J. K. (2001). *Military Space Culture. Prepared for the Commission to Assess United States National Security Space Management and Organization*. https://www.globalsecurity.org/space/library/report/2001/nssmo/article02.pdf

Morin, D. (2008). *Introduction to quantum mechanics*. Ch, 10, 1-20. https://scholar.harvard.edu/files/david-morin/files/waves_quantum.pdf

Nardon, L. (2017). *European Space Programs and the Digital Challenge*. Ifri. https://www.ifri.org/en/publications/etudes-de-lifri/european-space-programs-and-digital-challenge

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations. p.145. https://doi.org/10.6028/NIST.SP.800-53r5

NATO Space Centre of Excellence. (13 July 2023, last accessed). *Discover Our Organisation*. https://www.space-coe.org/organisation

NATO. (23 May 2023, last updated). NATO's approach to space. https://www.nato.int/cps/en/natohq/topics_175419.htm

Negreiro Achiaga, M. (2022). *Review of the Directive on security of network and information systems (20/09/2022 update)*. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive?sid=6201

Negreiro Achiaga, M. (2023). *The NIS2 Directive – A high common level of cybersecurity in the EU*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Ntanos, A., Lyras, N.K., Zavitsanos, D., Giannoulis, G., Panagopoulos, A.D. and Avramopoulos, H. (2021). *LEO Satellites Constellation-to-Ground QKD Links: Greek Quantum Communication Infrastructure Paradigm*. Photonics 2021, 8, 544. https://doi.org/10.3390/photonics8120544

OneWeb Satellites. (22 May 2023, last accessed). *About Us – Transforming the Space Industry*. https://airbusonewebsatellites.com/about-us/

OneWeb. (2023). *OneWeb confirms successful deployment of 16 satellites including next-generation JoeySat*. https://oneweb.net/resources/oneweb-confirms-successful-deployment-16-satellites-including-next-generation-joeysat

Oppenheim, J. and Wehner, S. (2010). *The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics*. In: Science. 330,1072-1074. https://doi.org/10.1126/science.1192065

Pelton, J. N. (2015). *History of Satellite Communications*. In: Handbook of Satellite Applications. https://doi.org/10.1007/978-1-4614-6423-5

PETRUS. (3 August 2023, last accessed). https://petrus-euroqci.eu/

PETRUS. (3 August 2023, last accessed). *PETRUS Consortium*. https://petrus-euroqci.eu/petrus-consortium/

Pivk, M. (2010). *Quantum Key Distribution*. In: Kollmitzer, C., Pivk, M. (eds) *Applied Quantum Cryptography*. Lecture Notes in Physics, vol 797. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04831-9_3

Porras, D. (2019). *Anti-satellite warfare and the case for an alternative draft treaty for space security*. In: Bulletin of the Atomic Scientists, 75:4, 142-147. https://doi.org/10.1080/00963402.2019.1628470

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

Qi, R. et al. (2019). *Implementation and security analysis of practical quantum secure direct communication*. https://doi.org/10.1038/s41377-019-0132-3

Quantum Flagship. (3 August 2023, last accessed). *Quantum Communication Infrastructure*. https://qt.eu/ecosystem/quantum-communication-infrastructure

Robinson, J., Šmuclerová, M., Degl'Innocenti, L., Perrichon, L. and Pražák, J. (2018). *Europe's Preparedness to Respond to Space Hybrid Operations*. Prague Security Studies Institute. https://www.pssi.cz/download//docs/8252_597-europe-s-preparedness-to-respond-to-space-hybrid-operations.pdf

Rumsfeld, D. (2001). *Report of the Commission to Assess United States National Security Space Management and Organization*. https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf

Russian Federation and China. (2008). *Letter dated 2008/02/12 from the Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament addressed to the Secretary-General of the Conference transmitting the Russian and Chinese texts of the draft "Treaty on Prevention of the Placement of Weapons in Outer*

Space and of the Threat or Use of Force against Outer Space Objects (PPWT)" introduced by the Russian Federation and China. CD/1839. Accessible via: https://digitallibrary.un.org/record/633470?ln=en

Sadeh, E. (2013). *Introduction: Towards space strategy*. In: Sadeh, E. (ed.), *Space Strategy in the 21st Century* (Routledge 2013). https://doi.org/10.4324/9780203098288

SatCen. *Copernicus*. https://www.satcen.europa.eu/what-we-do/copernicus

Sharma, V. and Banerjee, S. (2018). *Analysis of Quantum Key Distribution based Satellite Communication*. https://www.researchgate.net/publication/326505412_Analysis_of_Quantum_Key_Distribution_based_Satellite_Communication

Sheftick, G. (2020). *Army looks to leverage 'low Earth orbit' satellites*. U.S. Army. https://www.army.mil/article/233587/army_looks_to_leverage_low_earth_orbit_satellites

Sidhu, J.S., et al. (2021). *Advances in space quantum communications*. IET Quant. Comm. 2(4), 182– 217. p.183, 185. https://doi.org/10.1049/qtc2.12015

Space ISAC. (13 July 2023, last accessed). *About Space ISAC*. https://s-isac.org/about-us/

Stanniland, A. & Curtin, D. (2015). *An Examination of the Governmental Use of Military and Commercial Satellite Communications. In: Handbook of Satellite Applications*. https://doi.org/10.1007/978-1-4614-6423-5_8-3

Taylor, T. and Antinozzi, I. (2022). *The Tempest Programme – Assessing Advances and Risks Across Multiple Fronts*. Royal United Services Institute for Defence and Security Studies (RUSI). https://static.rusi.org/OP_356_Tempest_Programme_final_web1.pdf

Telecommunication Engineering Centre. (2019). *Communication using Medium Earth Orbit (MEO) Satellites*. https://www.tec.gov.in/pdf/Studypaper/Approved%20STUDY_PAPER_MEO_Radio_Division.pdf

Thales. (2023). *Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of its Kind*. https://www.thalesgroup.com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first

The Australian Army. (2021). *Army Quantum Technology Roadmap*. https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf

The University of Adelaide. (2018). *Woomera Manual on the International Law of Military Space Operations*. https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf

Trevithick, J. (29 June 2019, last update). *China Says It's Building a "Ghost Imaging" Satellite to Detect Stealth Jets*. The War Zone. https://www.thedrive.com/the-war-zone/16488/china-says-its-building-a-ghost-imaging-satellite-to-detect-stealth-jets

Turato, M. (2022). *Tempest è il sistema Fcas del futuro. Parla il gen. Camporini*. Formiche. https://formiche.net/2022/12/intervista-camporini-tempest/

Tyson, J. (2019). *The CIA Triad*. https://blog.jamestyson.co.uk/the-cia-and-dad-triads

U.S. Department of Defense. (2022). *Military and Security Developments Involving the People's Republic of China*. https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-

MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

UN (United Nations) General Assembly. (1966). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. 21st session. RES 2222 (XXI)*. https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf

UN. General Assembly (16th sess.: 1961-1962). (1961). *International co-operation in the peaceful uses of outer space*. A/RES/1721(XVI)[B]. https://digitallibrary.un.org/record/665195

Unal, B. (2019). *Cybersecurity of NATO's Space-based Strategic Assets*. Chatham House. https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets

Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T. et al. (2007). *Entanglement-based quantum communication over 144 km*. Nature Phys 3, 481–486. https://doi.org/10.1038/nphys629

Von Clausewitz, C. (1874). *On War*. (Graham, J. J., trans.). (Original work published 1832).

Von Wright, G. H. (1971). *Explanation and Understanding*. London: Routledge.

Webb, D. and Scheffran, J. (2021). *Anti-Satellite Weapons and Ballistic Missile Defense: the Siamese Twins?*. International Working Group MBMDS. http://inesglobal.net/wp-content/uploads/2021/10/section-12-webb-scheffran.pdf

Webb, D. and Scheffran, J. (2021). Prevention of an Arms Race in Outer Space (PAROS): Obstacles and Options. International Working Group MBMDS. http://inesglobal.net/wp-content/uploads/2021/10/section-10-webb-scheffran-space-ban.pdf

Williams, J. (3 August 2023, last accessed). *Deutsche Telekom leads build of high-security communications network for the EU*. https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-leads-build-of-high-security-communications-network-for-the-eu-1026404

Wolf, S.a. et al. (2019). *Overview of the Status of Quantum Science and Technology and Recommendations for the DoD*. Institute for Defence Analyses. https://www.ida.org/-/media/feature/publications/o/ov/overview-of-the-status-of-quantum-science-and-technology-and-recommendations-for-the-dod/d-10709.ashx

Wootters, W. and Zurek, W. (1982). *A single quantum cannot be cloned*. Nature 299, 802–803. https://doi.org/10.1038/299802a0

Yeboah-Boateng, E. O. (2013). *Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)*. (1 ed.) Institut for Elektroniske Systemer, Aalborg Universitet. https://vbn.aau.dk/ws/portalfiles/portal/316448052/PhD_Thesis_Boateng_Final_for_print.pdf

Zhai, A. (2022). *An Overview of Quantum Key Distribution Protocols and Experimental Implementations*. https://wp.optics.arizona.edu/opti646/wp-content/uploads/sites/55/2022/12/Zhai_Term_Paper.pdf