



**NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS
&
UNIVERSITY OF PATRAS**

**SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS AND
DEPARTMENT OF PHYSICS
&
POLYTECHNIC SCHOOL
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING AND
DEPARTMENT OF MECHANICAL ENGINEERING AND ASTRONAUTICS**

**CROSSDEPARTMENTAL MASTER OF SCIENCE (MSc.) PROGRAM
“SPACE TECHNOLOGIES, APPLICATIONS AND SERVICES - STAR”**

MSc. THESIS

**Evolution of EU Secure Satellite Communications: From
GovSatCom to IRIS² and the Relevance of EuroQCI to EU's
Cybersecurity Strategy**

K. G. Giannaki

Supervisor: **Panagiotis Papakanellos**, Assistant Professor, Hellenic Air
Force Academy

ATHENS

JULY 2024



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

&

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΜΗΜΑ ΦΥΣΙΚΗΣ

&

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ
ΜΗΧΑΝΟΛΟΓΩΝ ΚΑΙ ΑΕΡΟΝΑΥΠΗΓΩΝ ΜΗΧΑΝΙΚΩΝ**

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

“ΔΙΑΣΤΗΜΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ, ΕΦΑΡΜΟΓΕΣ και ΥΠΗΡΕΣΙΕΣ”

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Εξέλιξη των Ευρωπαϊκών Ασφαλών Δορυφορικών
Επικοινωνιών: Από το GovSatCom στο IRIS² και τη Συνάφεια
του EuroQCI με τη Στρατηγική Κυβερνοασφάλειας της ΕΕ**

Κ. Γ. Γιαννάκη

Επιβλέπων:

**Παναγιώτης Παπακανέλλος, Επίκουρος Καθηγητής, Σχολή
Ικάρων**

ΑΘΗΝΑ

ΙΟΥΛΙΟΣ 2024

MSc. THESIS

Evolution of EU Secure Satellite Communications: From GovSatCom to IRIS² and the Relevance of EuroQCI to EU's Cybersecurity Strategy

Konstantina G. Giannaki

ID: 7115172200033

Supervisor: **Panagiotis Papakanellos**, Assistant Professor, Hellenic Air Force Academy

Examination Committee: **Panagiotis Papakanellos**, Assistant Professor, Hellenic Air Force Academy
Vaios Lappas, Professor, National and Kapodistrian University of Athens
Alexandros Kolovos, Associate Professor, National and Kapodistrian University of Athens

July 2024

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εξέλιξη των Ευρωπαϊκών Ασφαλών Δορυφορικών Επικοινωνιών: Από το GovSatCom στο IRIS² και τη Συνάφεια του EuroQCI με τη Στρατηγική Κυβερνοασφάλειας της ΕΕ

Κωνσταντίνα Γ. Γιαννάκη

A.M.: 7115172200033

Επιβλέπων: **Παναγιώτης Παπακανέλλος**, Επίκουρος Καθηγητής, Σχολή Ικάρων

Examination Committee: **Παναγιώτης Παπακανέλλος**, Επίκουρος Καθηγητής, Σχολή Ικάρων
Βάιος Λάμπας, Καθηγητής, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Αλέξανδρος Κολοβός, Αναπληρωτής Καθηγητής, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Ιούλιος 2024

ABSTRACT

Satellites have evolved into critical enablers for a diverse range of essential services, and therefore many aspects of our daily lives rely on the continuous and effective operation of satellite-based services, while the intersection of space and technology has proven instrumental in addressing numerous societal challenges. In this context, the current Thesis aims to perform a comparative analysis of three pivotal satellites-based initiatives, the Governmental Satellite Communications (GovSatCom) initiative, the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) initiative, as well as the European Quantum Communication Infrastructure (EuroQCI) initiative, that is included to the European Cybersecurity Strategy, defining their strategic objectives, operational and technical capabilities, as well as limitations and challenges, highlighting, also, both their synergies and main differences. Comprehensive bibliographic research was conducted to collect the required information regarding such initiatives. Furthermore, considering that the malicious actors consider space infrastructure as an attractive target, as well as that the cybersecurity threat landscape continuously evolves, this Thesis aims to define the main cybersecurity requirements and controls that should be implemented, considering the applicable legal and regulatory requirements, industry standards, and best practices, to ensure that the space-based and terrestrial infrastructure is protected against cybersecurity attacks, as well as that the initiatives' provided satellite communication services are cyber-secure and resilient. To achieve such objectives, cybersecurity should be integrated to all aspects of space activities, including the design phase, command and control, satellite operation, uplink/downlink, and ground segment, to promote, establish, and ensure security and resiliency of satellite communication services.

SUBJECT AREA: Satellite Communication and Cybersecurity

KEYWORDS: GovSatCom, IRIS², EuroQCI, Satellite Communication, Cybersecurity

ΠΕΡΙΛΗΨΗ

Οι δορυφόροι αποτελούν κρίσιμο παράγοντα για πληθώρα σημαντικών υπηρεσιών, και ως εκ τούτου πολλές πτυχές της καθημερινής μας ζωής βασίζονται στη συνεχή και αποτελεσματική λειτουργία αυτών, ενώ παράλληλα η συνέργια του διαστήματος και της τεχνολογίας έχει αποδειχθεί καθοριστική για την αντιμετώπιση πολλών κοινωνικών προκλήσεων. Σε αυτό το πλαίσιο, η παρούσα Διπλωματική στοχεύει στη συγκριτική ανάλυση τριών καίριων δορυφορικών πρωτοβουλιών, των Δορυφορικών Επικοινωνιών Κυβερνητικού Χαρακτήρα (GovSatCom), της Υποδομής για Ανθεκτικότητα, Διασυνδεσιμότητα και Ασφάλεια μέσω Δορυφόρου (IRIS²), καθώς και της Ευρωπαϊκής Κβαντικής Επικοινωνιακής Υποδομής (EuroQCI), το οποίο συμπεριλαμβάνεται στην Ευρωπαϊκή Στρατηγική Κυβερνοασφάλειας, καθορίζοντας τους στρατηγικούς τους στόχους, τις λειτουργικές και τεχνικές τους δυνατότητες, καθώς και τους περιορισμούς και τις προκλήσεις τους, επισημαίνοντας, επίσης, τόσο τις συνέργιές τους όσο και τις κύριες διαφορές τους. Για τη συλλογή των απαιτούμενων πληροφοριών σχετικά με τις εν λόγω πρωτοβουλίες πραγματοποιήθηκε εκτενής βιβλιογραφική ανασκόπηση. Επιπλέον, λαμβάνοντας υπόψη ότι οι κυβερνοεγκληματίες θεωρούν τη διαστημική υποδομή ως ελκυστικό στόχο, καθώς επίσης δεδομένου ότι το τοπίο των απειλών κυβερνοασφάλειας εξελίσσεται συνεχώς, η εν λόγω Διπλωματική στοχεύει στην ανάδειξη των σημαντικότερων απαιτήσεων κυβερνοασφάλειας και των σχετικών μέτρων ασφάλειας πληροφοριών που πρέπει να εφαρμόζονται, λαμβάνοντας υπόψη τις υπάρχουσες νομικές και κανονιστικές απαιτήσεις, τα διεθνή πρότυπα και τις βέλτιστες πρακτικές, ώστε να διασφαλιστεί ότι η δορυφορική και επίγεια υποδομή προστατεύεται επαρκώς από τις κυβερνοεπιθέσεις, καθώς και ότι οι παρεχόμενες δορυφορικές υπηρεσίες επικοινωνίας των προαναφερθέντων πρωτοβουλιών είναι κυβερνοασφαλείς και ανθεκτικές. Για την επίτευξη των εν λόγω στόχων, η κυβερνοασφάλεια πρέπει να ενσωματωθεί σε όλες τις πτυχές των διαστημικών δραστηριοτήτων, συμπεριλαμβανομένης της φάσης του σχεδιασμού, του ελέγχου, της λειτουργίας, καθώς και της επίγειας και διαστημικής διασύνδεσης, προκειμένου να προωθηθεί, να καθιερωθεί, και να διασφαλιστεί η ασφάλεια και η ανθεκτικότητα των δορυφορικών υπηρεσιών επικοινωνίας.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Δορυφορικές Επικοινωνίες και Κυβερνοασφάλεια

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: GovSatCom, IRIS², EuroQCI, Δορυφορικές Επικοινωνίες, Κυβερνοασφάλεια

To Katerina and Iasonas

ACKNOWLEDGEMENTS

First and foremost, I would like to express my warmest thanks to my supervising Professor Mr. Panagiotis Papakanellos for his invaluable guidance and support during the whole process of documentation of such Thesis. I would also like to warmly thank the other members of the Examination Committee, Mr. Alexandros Kolovos, and Mr. Vaios Lappas for supervising this Thesis, and always providing constructive feedback to ensure the highest quality level of such Thesis, helping me in parallel to academically advance and expand my knowledge horizon. It is a great honor for me to have closely worked with all of them, and it would be a great pleasure to collaborate again in the future.

Additionally, a heartfelt thank you goes to the people who believed and believe in me more than anyone else, my sister Katerina, and her husband, my brother-in-law Iasonas, who were by my side at every moment during my studies, truly supporting and guiding me to this journey, and therefore whose presence was pivotal for successful completion of both my studies at the National and Kapodistrian University of Athens, as well as of such Thesis. Last but not least, I would also like to deeply thank my mother Eleni and my aunt Vaso who support me in every decision I make and stand by me in everything.

CONTENTS

INTRODUCTION	15
1. HISTORICAL ANALYSIS	18
2. GOVSATCOM INITIATIVE: PIONEERING SECURE GOVERNMENTAL SATELLITE COMMUNICATIONS.....	21
2.1 Overview of Governmental Satellite Communications (GovSatCom) Initiative ...	21
2.2 Vision and Strategic Objectives	28
2.3 Core Capabilities.....	32
2.4 Operational Requirements	36
2.5 Limitations and Challenges	41
2.6 Implementation Reasons	44
2.6.1 Technological Advancement and Innovation	44
2.6.2 Connectivity Across EU	45
2.6.3 Secure Satellite Communications.....	45
3. IRIS² INITIATIVE: ENABLING SECURE AND RESILIENT GOVERNMENTAL SATELLITE COMMUNICATIONS.....	47
3.1 Overview of Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS ²) Initiative	47
3.2 Vision and Strategic Objectives	51
3.3 Core Capabilities.....	53
3.4 Operational Requirements	56
3.5 Limitations and Challenges	59
3.6 Implementation Reasons	61

3.6.1	Technological Advancement and Innovation	61
3.6.2	Global Connectivity	63
3.6.3	Secure Satellite Communications.....	64
3.6.4	Resilient Satellite Communications	65
4.	EUROQCI INITIATIVE: A PART OF THE EUROPEAN CYBERSECURITY STRATEGY AND A QUANTUM LEAP TOWARDS SECURE COMMUNICATION INFRASTRUCTURE.....	67
4.1	The European Cybersecurity Strategy and the European Quantum Communications Infrastructure (EuroQCI).....	67
4.2	Vision and Strategic Objectives	73
4.3	Core Capabilities.....	75
4.4	Operational Requirements	79
4.5	Limitations and Challenges	83
4.6	Implementation Reasons	87
4.6.1	Technological Advancement and Innovation	87
4.6.2	Secure Satellite Communications.....	88
4.6.3	Enhanced Users' Trust.....	89
5.	SYNERGIES BETWEEN GOVSATCOM, IRIS² AND EUROQCI INITIATIVES	91
5.1	Comparative Analysis of GovSatCom, IRIS ² and EuroQCI Main Differential Aspects.....	91
5.2	Analysis of Potential Benefits of GovSatCom and EuroQCI to IRIS ²	93
6.	COMPREHENSIVE SECURITY REQUIREMENTS ACROSS THE GOVSATCOM LIFECYCLE.....	95

6.1	Enforcement of Security by Design Principle	95
6.2	Enablement of Secure Command and Control for Satellites	97
6.3	In-Orbit Security Monitoring and Threat Detection	99
6.4	Ensuring the Security of Satellite-to-Earth Communication	101
6.5	Safeguarding the Security of Ground-Based Infrastructure	103
7.	ASSESSING AND SECURING THE GROUND INFRASTRUCTURE: A FRAMEWORK	106
7.1	Current Threat Landscape	106
7.2	Assessment Methodology	111
7.3	Assessment Framework	113
8.	CONCLUSIONS	116
	LIST OF ABBREVIATIONS AND ACRONYMS	118
	BIBLIOGRAPHY	123

LIST OF FIGURES

Figure 1: Option 1 - Usage of commercial SatCom services [13]	22
Figure 2: Option 2 - Usage of Member States' space assets [13]	23
Figure 3: Option 3 - Sharing commercial (Phase 1) [13]	23
Figure 4: Option 3 - Public-Private Partnerships for future space assets (Phase 2) [13]	24
Figure 5: Option 4 - Usage of future EU space assets (Phase 2) [13]	24
Figure 6: IRIS ² initial implementation timeline [48]	49
Figure 7: IRIS ² initial procurement timeline [48]	49
Figure 8: IRIS ² SatCom market analysis [61]	55
Figure 9: Strategic objectives of 2013 Cybersecurity Strategy [75]	69
Figure 10: Quantum Key Distribution - QKD [84]	76
Figure 11: EuroQCI space and terrestrial segments [84]	78
Figure 12: Overview of threat actors and their motivations [61]	106
Figure 13: Motivation of satellite incidents and breakdown of used techniques [102] ..	109
Figure 14: Evolution of cyberattacks on space systems (amount of attacks / year over the last forty years) [61]	111
Figure 15: Tiers of satellite communications [13]	112

LIST OF IMAGES

Image 1: Satellite services' vertical markets' descriptions / definitions [1]	15
Image 2: ENTRUSTED GovSatCom demonstrations [17]	27
Image 3: ENTRUSTED GovSatCom demonstration by Greece [17]	28
Image 4: EU GovSatCom problem tree [13]	29
Image 5: EU GovSatCom main use-case families [13]	34
Image 6: EU GovSatCom architecture [32]	37
Image 7: EU GovSatCom Hubs architecture [13]	37
Image 8: EU IRIS ² initiative's services [60]	54
Image 9: Infrastructure and ownership of IRIS ² [48]	57
Image 10: Infrastructure of IRIS ² [60]	58
Image 11: EU Quantum Technologies Flagship and the quantum internet [84]	74
Image 12: QKD network hierarchy layers [87]	77
Image 13: Overview of EuroQCI and its main components [89]	80
Image 14: Delivery of key material to EuroQCI users via SpaceQCI [89]	82
Image 15: Phases of satellites' operations [101]	99
Image 16: Major communication links used in space systems [101]	101
Image 17: Actual cyberattacks and potential mitigation actions examples [61]	108
Image 18: Space threats [115]	110

LIST OF TABLES

Table 1: Summary of different GovSatCom implementation options' characteristics [13]	
.....	25
Table 2: Main differences of GovSatCom, IRIS ² , and EuroQCI initiatives	91
Table 3: Main cybersecurity vulnerabilities and the respective recommendations [94]	107

INTRODUCTION

Space-based technology has evolved into a valuable resource for everyday life terrestrial activities, in a way that was not imaginable at the inception of the space age in 1950. People rely on space technology, data, and services, indicatively, when using mobile / smart phones, navigation systems, watching satellite television (TV), or withdrawing money from Automated Teller Machines (ATMs). Additionally, the utilization of space technology supports multiple and critical services on Earth in fields such as, indicatively, disaster risk management, agricultural practices advancement, environment protection, climate changes monitoring and assessment, digital connectivity, as well as spatial planning, providing socioeconomic benefits and fostering innovation in a variety of areas that directly contribute towards sustainable development (e.g., digitalization, artificial intelligence, energy, etc.).

Focusing on space communications services, that were firstly designed and developed for military operations in sixties, they have rapidly evolved to address civilian also communication needs, such as regional and worldwide communication from seventies to eighties, TV broadcast since nineties, and multimedia applications more recently [Image 1].

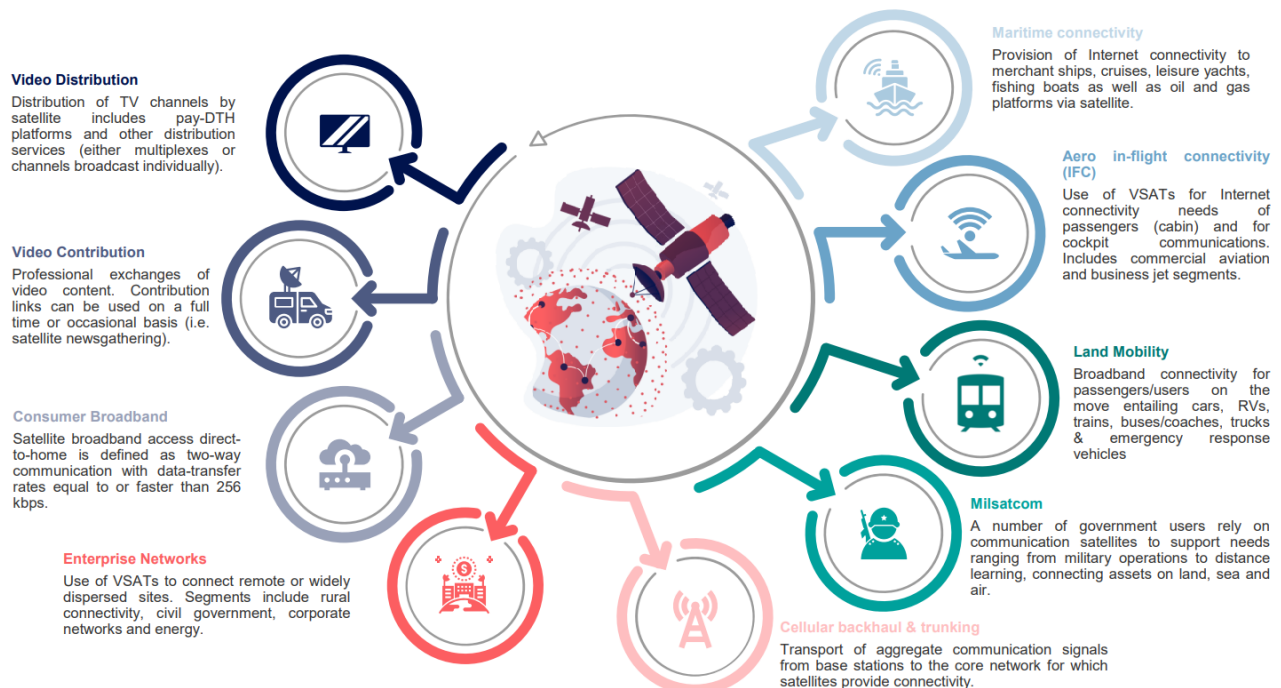


Image 1: Satellite services' vertical markets' descriptions / definitions [1]

Thus, it is easily understood that space-based information and services influence numerous aspects of human lives, such as augmenting public services' efficiency, enhancing the national security level, and providing new opportunities for scientific research and development.

Space technology, as already mentioned, is dual use, both for military and civilian purposes, being directly linked to the provision of communications and information related services. Access to secure satellite communications services is crucial and plays a vital role in defense and security related governmental communication, particularly, during crisis situations and network interruption incidents, when ground-based means of communication are not available or reliable, for example in cases of natural or human-

made disasters, unavailability instances, indicatively in maritime areas or in the Arctic region, and humanitarian missions in hostile territories.

Nowadays there is a misalignment between the emerging risks and new threats to the operational environment, the evolving requirements for secure satellite communications by public authorities at national and European level, as well as the available solutions, which in many cases are inappropriate, fragile, and not secure, increasing the attack surface and possibly affecting the efficient execution of missions and security operations, as well as the resiliency of space infrastructures of the Union and its Member States. Whether civil or military, nowadays practically all actors require better means of communication.

However, the existing communication capabilities are not considered fully satisfactory, whether bottom-up or top-down, indicatively due to slow speed, low bandwidth, absence of security and confidentiality, non-interoperability, and lack of reliability. More specifically, the current communication methods are perceived as non-satisfactory, as email accounts rapidly exhaust their storage limit, both telephone and fax lines exhibit irregular functionality, signal impairments and frequent mid-conversation disruptions lead to data loss, mobile phones are constrained by inconsistent network coverage, as well as satellite phones require predominant power-off status due to their extreme energy requirements.

Thus, in emergency and crisis situations there is not a failsafe method for maintaining connectivity of high quality and security level, while there is a widespread dissatisfaction among end users with the speed of existing satellite communications services [2]. Robust data transmission capabilities are universally defined as a requirement, and more specifically the ability to transmit visual information, including photos, and videos. Throughout various types of operations, there is a significant demand for image-based data transmission, thus necessitating high-bandwidth data transmission capabilities. The need to transmit photographic content is prevalent in multiple situations, including indicatively victim identification, real-time communication for strategic decisions, and as evidence against the perpetrators of violence. Additionally, the rapid transmission of vocal messages is equally vital, especially when they relate with urgent messages from individuals in need.

Due to the above-mentioned reasons, information transfer is rarely performed both efficiently and securely. For instance, during the Artemis operation in the Democratic Republic of Congo, images collected and analyzed in Entebbe could be transmitted to the operational headquarters without delay thanks to encrypted transmission. However, such seamless transfer was not possible to the operational headquarters in Bunia, where operational decisions were made, due to insufficient satellite bandwidth between Entebbe and Bunia. Consequently, the information had to be transmitted via CD-ROMs or via plane. In other circumstances, attempts to transmit information often encounter limitations in terms of inadequate security measures and insufficient bandwidth.

For example, individuals involved in post-tsunami operations expressed dissatisfaction with being forced to use certain email accounts because of the absence of other options, and that were vulnerable to cybersecurity attacks. In Thailand, for instance, an unknown entity created an account with an identical email title. For these reasons, both civil and military related stakeholders highlight that for effective information transmission, it is of paramount importance not only to have a high-capacity system, but also secure and resilient, which in practice, unfortunately up until now, is mainly assured only during military operations.

The key to meeting operational demands, overcoming interoperability challenges in crises, and progressing toward shared technologies lies in recognizing and leveraging the complementary aspects of civilian and defense space services. For example, missions related to disaster relief and crisis management encompass elements from both sectors, including transportation, medical care, food provision, and temporary housing.

Considering the demanding operational needs and the current communication capabilities, space technologies are considered as invaluable resources as they can serve as the method of maintaining constant, secure, resilient, high-speed communication between stationary and mobile terminals, delivering positioning and navigation signals, as well as establishing connections between headquarters, sensors, and user communities globally. Space technologies are particularly valuable in collecting and transmitting accurate and trustworthy information on a global scale. For these reasons, the 2021-2027 EU Space Program includes both Governmental Satellite Communications (GovSatCom) and Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) as new technologically demanding and knowledge intensive initiatives, as well as IRIS² as the European answer to the US Starlink mega-constellation programme.

Moreover, space technologies are the only means that can recover communications in instances when the ground communication infrastructures are damaged. Hence, an operational assured space system can fulfill the previously mentioned needs, for worldwide connectivity, quick deployment, large transmission capacity, and high resiliency and security. Some of the available space related services are the Fixed Satellite Services (FSS), which allow links between static terminals at different network locations as well as terminals that have been deployed, the Mobile Satellite Services (MSS), which provide links for mobile users, particularly maritime, terrestrial, and aeronautical, allowing for constant communication while on the move, as well as the Data Relay Services (DRS), which provide high-speed communication between different systems, such as space, Unmanned Aircraft Vehicles (UAVs), and airborne, among others, and processing centers to enhance the overall response time. Hence, the existing space related services can serve various operational objectives.

Summarizing, considering that the existing satellite space communications programs, in many cases are inappropriate, fragile, and not secure, as well as could represent a single point of failure with significant safety and security threats, especially during disruptions caused by natural or man-made disasters or by cybersecurity attacks increasing the attack surface and possibly affecting the efficient execution of missions and security operations, and additionally taking into consideration that the secure and resilient space communication is identified as critical operational requirement for both civil and military operations, it is of paramount importance to define the security requirements of GovSatCom and IRIS², as well as to highlight any synergies with alternative initiatives, such as the European Quantum Communications Infrastructure (EuroQCI) that will be an integral part of IRIS², enabling a “security first” approach.

Amidst a geopolitical landscape with evolving cybersecurity threats, concerns over security and resilience are intensifying. Consequently, there is a rising demand for the European Union to enhance its governmental satellite communications in both scope and quality, shifting toward solutions with greater security, reduced latency, and increased bandwidth. Furthermore, synergies with the cybersecurity field should be identified, as cybersecurity plays a vital role for all aspects of space activities, including the design phase, the command and control, the satellite operation, the uplink/downlink, and the ground segment, to promote, establish, and ensure security and resiliency to space communication related services.

1. HISTORICAL ANALYSIS

As space can be described as the fifth operational domain, being mainly critical for military, but also for civilian missions and operations at the land, sea, air domain and cyberspace, satellite communications (SATCOM) are defined as an operational requirement in every Common Security and Defense Policy (CSDP) related European Union's (EU) official document. While North Atlantic Treaty Organization (NATO) exists to defend its members, most of which are European, from external attacks, Europe needs to have the capability to safeguard its own territory, react to crises beyond its borders, and support the development of security and defense capabilities. It must tackle issues that have both domestic and international implications, including terrorism, organized crime, cybersecurity, hybrid threats, energy security, and management of its external borders.

For example, to missions and operations under the Common Security and Defense Policy can collaborate with the European Border and Coast Guard and specialized EU agencies to improve border security and maritime safety, aiming to save more lives, combat international crime, and interrupt smuggling networks upon utilization of space technologies. Starting from the beginning of the 2000s, space communications were considered as a vital operational requirement for every civil and military mission, such as command and control.

As the space sector is going through massive transformation and rapid industrialization at a global level, and for Europe to respond to global challenges, in November 2004, the European Council defined that secure and reliable satellite communications are essential for exercising political and strategic direction of any operation [3]¹. The global European Space Policy (ESP), which was released in May 2007, identified the need to meet Europe's security and defense requirements regarding space [4]². In the same context, the report from the European Space and Human Security Working Group (ESHS-WG), which was developed in January 2006 and its final version published in October, highlighted the importance of establishing adequate and effective space capabilities in Europe, such as remote sensing, meteorology, telecommunications, and navigation capabilities, providing a detailed roadmap, including the engagement of user communities and enforcement of pre-existing services [5]. In order the information transmission to be effective, as reliable communication is essential for worldwide operations, it should not only provide large capacity but should also ensure the confidentiality, integrity, and availability of transmitted information to enable secure communications.

Furthermore, as the security environment and threat landscape continuously evolve and become increasingly complex and challenging, characterized by terrorist attacks, mass murders, as well as sophisticated cybersecurity attacks, secure satellite communications become an operational requirement for both civilian and military missions. More specifically, the demand for secure and resilient satellite communications primarily

¹ Council of the European Union, European space policy: ESDP and space, 11616/3/04 REV 3. Brussels. Available at: <http://register.consilium.europa.eu/pdf/en/04/st11/st11616-re03.en04.pdf>.

² Council of the European Union, Resolution on the European space policy, Outcome of proceedings of the council (competitiveness) on 21-22 May 2007 10037 / 07. Brussels, May 25, 2007. Available at: <https://data.consilium.europa.eu/doc/document/ST-10037-2007-INIT/en/pdf>.

originates from the security and defense sector, as various authorities' and agencies' suggestions highlighted the secure satellite communications as the main operational requirement.

In this context, in June 2013, the European Defense Agency (EDA) presented its "Secure Telecom by Satellite" (SECTELSAT) concept as the future governmental SATCOM, which was characterized as critical technology, while in July 2013, the European Commission pinpointed that the space technologies, infrastructures, and services require further intervention, as they could be beneficial for both civilian and defense purposes.

A few months later, in October 2013, the High Representative stated that by the end of this decade, the existing military satellite communication (MILSATCOM) systems of current EU Member States would reach their operational lifespan. For this reason, the objective was to develop a future dual civil-military capability by 2025 through a user-driven approach, guided by a comprehensive, strategic, and prioritized roadmap.

Similarly, the significance of the secure and resilient satellite communications was highlighted as in December 2013 the EU Council approved the commitment of additional efforts for the development of the upcoming generation of Governmental Satellite Communication through a collaboration between the Member States, the Commission, and the European Space Agency (ESA), which has a cooperation agreement with the EU.

A few years later, in February 2015, the EDA requested the submission of proposals regarding the execution of a feasibility study on "Governmental Satellite Communication (GovSatCom)". The objective was the initiation of the project in 2016 and the development of the next generation of GovSatCom by 2025, which would rely on mutually agreed military user needs. The EU Commission performed a study regarding the necessary technologies for the next generation of GovSatCom, the results of which was published to the 2015 EU Commission's Report on the Implementation of the European Commission's Communication on Defense. Finally, on 26 June 2015, the EDA launched a one (1) million euros, eighteen (18) month feasibility study program to prepare the GovSatCom [6].

Furthermore, the Global Strategy for the European Union's Foreign and Security Policy (EUGS), that was published in June 2016, highlighted the existing gap in satellite communications, requiring the investment in surveillance, reconnaissance, and intelligence, including Remotely Piloted Aircraft Systems (RPAS), satellite communications, and autonomous access to space and permanent earth observation [7]. Generally, the European External Action Service, the Diplomatic Service, as well as the Ministry of Foreign Affairs and Defense of the EU, are responsible for issuing Security Strategies.

Nonetheless, the 2014 - 2020 EU Space Program, which was the practical implementation of the ESP, did not had integrated satellite communications, regardless the institutional recommendations that have been made, especially given the fact that satellite communications were the main requirement of the European space industry. In contrast and fortunately, the 2021 - 2027 EU Space Program, which was adopted in 2021, included an ambitious agenda for an innovative, and resilient European space ecosystem, implementing space initiatives related to the fields of satellite navigation, Earth observation, space research and innovation, as well as, connectivity, investing in critical infrastructures and disruptive technologies. On top of this, in February 2022, at the same time of the Russian invasion in Ukraine, the European Commission proposed a new initiative to enhance satellite secure connectivity, which was the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), aiming to ensure worldwide

access to secure and cost-effective satellite communications services, for governmental communications and commercial use, protecting critical infrastructures, supporting surveillance and crisis management activities, as well as enabling high-speed broadband everywhere in Europe.

More specifically, the 2021-2027 EU Space Program includes both Governmental Satellite Communications (GovSatCom) and Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) as new technologically demanding and knowledge intensive initiatives, while the IRIS² being the European answer to the US Starlink mega-constellation programme. One of the main objectives of IRIS² is to complement and integrate the existing and future capabilities of GovSatCom. The EU Space Program is implemented in close cooperation with the EU Member States, the European Union Agency for the Space Program (EUSPA), the European Space Agency (ESA), EUMETSAT and many other stakeholders [8]. Supporting Europe's civil, private, and governmental sectors, EUSPA boasts of programs, such as Copernicus, EGNOS (European Geostationary Navigation Overlay Service), Galileo, GovSatCom (Governmental Satellite Communications), IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite), and SSA (Space Situational Awareness) that endeavor to be an integrated family of systems designed to support the EU internal market [9].

As society undergoes simultaneous digital and environmental shifts, the role of connectivity becomes crucial for maintaining societal stability. The significance of satellite communication is heightened as it becomes a vital resource for ensuring the uninterrupted functioning of essential services, managing emergencies, and supporting general surveillance and security measures. Despite the growing reliance on secure communication services for both societal and economic needs, the European Union and its Member States currently depend on a scarce selection of geostationary satellites for government communication services. In contrast, other countries with space capabilities have already deployed their own satellite constellations, provided broader coverage, and simultaneously limited the available orbits for future constellations.

Governmental and institutional entities need to rely on satellite communications whenever standard communication links are not available and secure communication is needed. GovSatCom and IRIS² aim to ensure the provision of long-term available, resilient, reliable, secure, and cost-effective governmental satellite communications services for EU and Member States' governmental entities, enabling effective decision making and proactive implementation of countermeasures during crisis situations.

2. GOVSATCOM INITIATIVE: PIONEERING SECURE GOVERNMENTAL SATELLITE COMMUNICATIONS

2.1 Overview of Governmental Satellite Communications (GovSatCom) Initiative

Space technologies, applications, and services play a vital role in achieving many European strategic objectives. The EU's space industry is one of the most competitive industries, however the new players, the development of emerging technologies, as well as the operational environment for European security actors which is increasingly hostile, and threats constantly emerge, transform, and revolutionize the traditional industrial models. Therefore, for the EU to remain a leading international player in the space domain, it is crucial to encourage scientific and technological progress, as well as to support innovation. Since the end of 1990s, EU has been developing space related capabilities, including the European Geostationary Navigation Overlay Service (EGNOS), Galileo, as well as Copernicus.

However, as the ECA audit showed [10]³, although their services were launched, the uptake needs a further boost. So, these initiatives should be continued, and their provided services should be improved, to meet the fast-paced growing users' needs and growing demand for secure and reliable satellite communication services by the EU governmental actors, which is primarily driven by situations where ground-based communication systems are either nonexistent, compromised, or unreliable, to remain up to date with the technological advancement in the digital and Information and Communications Technology (ICT) domains, as well as to meet the political priorities, such as indicatively climate change, transport, security, and defense.

Today, affordable satellite communication is essential in regions lacking ground-based infrastructure, like oceanic expanses and isolated locations, or where such infrastructure is susceptible to disruptions or unreliable during emergencies. Satellite communication bolsters the robustness of communication networks by providing a backup option in the event of physical or cyber-attacks on terrestrial infrastructure, as well as in the aftermath of incidents, whether natural or man-made catastrophes.

In this context, the European Council's meeting held in 19-20 December 2013 welcomed the preparations for the next generation of GovSatCom, through cooperation between Member States, European Commission, EDA, and ESA, aiming to enable secure communication in locations and/or situations where normal communication is unavailable. GovSatCom is a satellite communications service, with a strong security dimension, under civil and governmental control, enabling the provision of reliable, resilient, secure, and cost-efficient satellite communications capabilities and services to EU's and its Member State's authorities that manage security and safety critical missions and infrastructures [11].

Therefore, non-dependence from third parties is required, covering all GovSatCom's components, such as space and ground technologies, manufacturing entities, owners and operators of space systems, and physical location of ground infrastructure. The initial satellite communication operational needs for European civil and military actors identified

³ European Court of Auditors, EU space programmes Galileo and Copernicus: services launched, but the uptake needs a further boost. Special Report No 07/2021. Available at: <https://www.eca.europa.eu/en/publications?did=58347>.

in the conduct of national and CSDP operations/missions, were gathered by EDA in the Common Staff Target document and endorsed by the EDA Steering Board in November 2014 [12]. Furthermore, GovSatCom was included to the Global Strategy for the European Union's Foreign and Security Policy of June 2016, the EU Global Strategy, as well as the European Defense Action Plan. GovSatCom, also, should support the EU Maritime Security Strategy and the EU Arctic Policy. With the support of a feasibility study, EDA developed the Common Staff Requirements document and associated Business Case, detailing the GovSatCom requirements and proposing the way ahead to meet the defined requirements, which were approved at the EDA Steering Board in March 2017 [12].

The implementation of GovSatCom started in 2021 under the framework of the new Space Program Regulation, while the initiative's preparatory activities initiated by the European Parliament in 2019. GovSatCom can provide three (3) different use-cases, which are operational scenarios in a particular environment in which GovSatCom services are required, and these are the crisis management, surveillance, and key infrastructures support. The implementation of GovSatCom had four (4) alternative options, the utilization of commercial [Figure 1] or national satellites [Figure 2] which were the first two (2) options respectively but neither of them were able to provide all required capabilities, the utilization of both security-accredited commercial [Figure 3] and national satellites [Figure 4] either via a public-private partnership between EU and industry, which was the third option, or through EU-owned assets [Figure 5], which was the fourth. The third option was considered as the most effective and diversified one in terms of access, security, and geographic and frequency coverage, for all users, allowing the usage of existing user equipment as well, providing scalability and flexibility [Table 1].

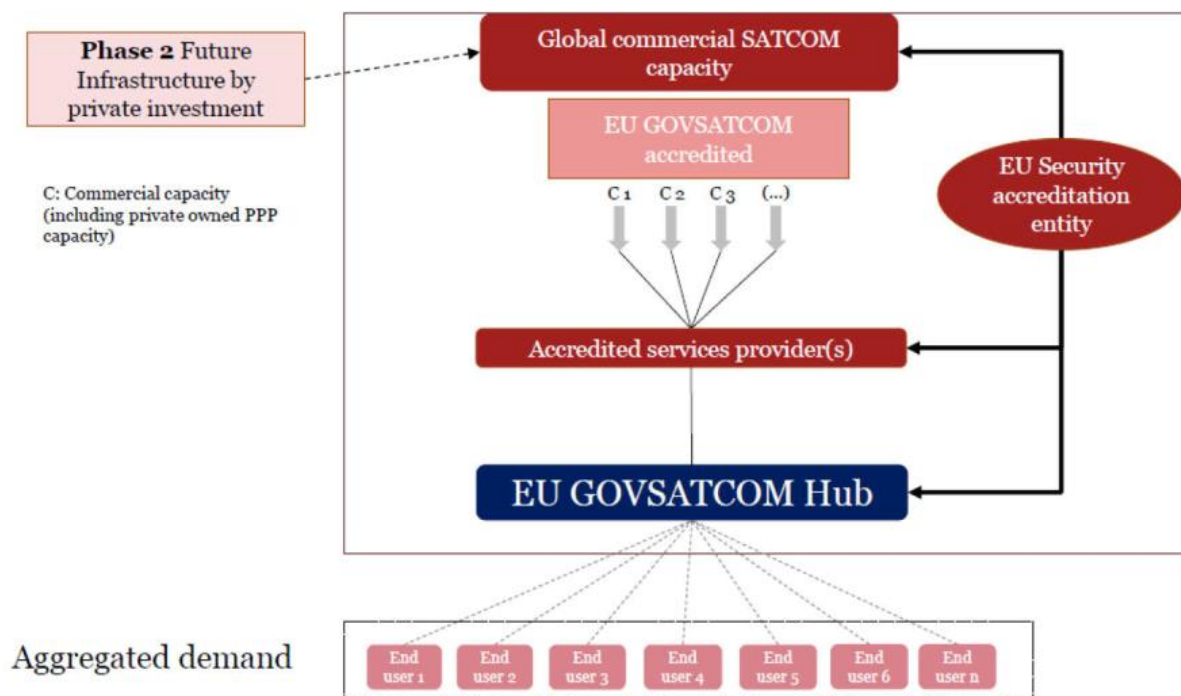


Figure 1: Option 1 - Usage of commercial SatCom services [13]

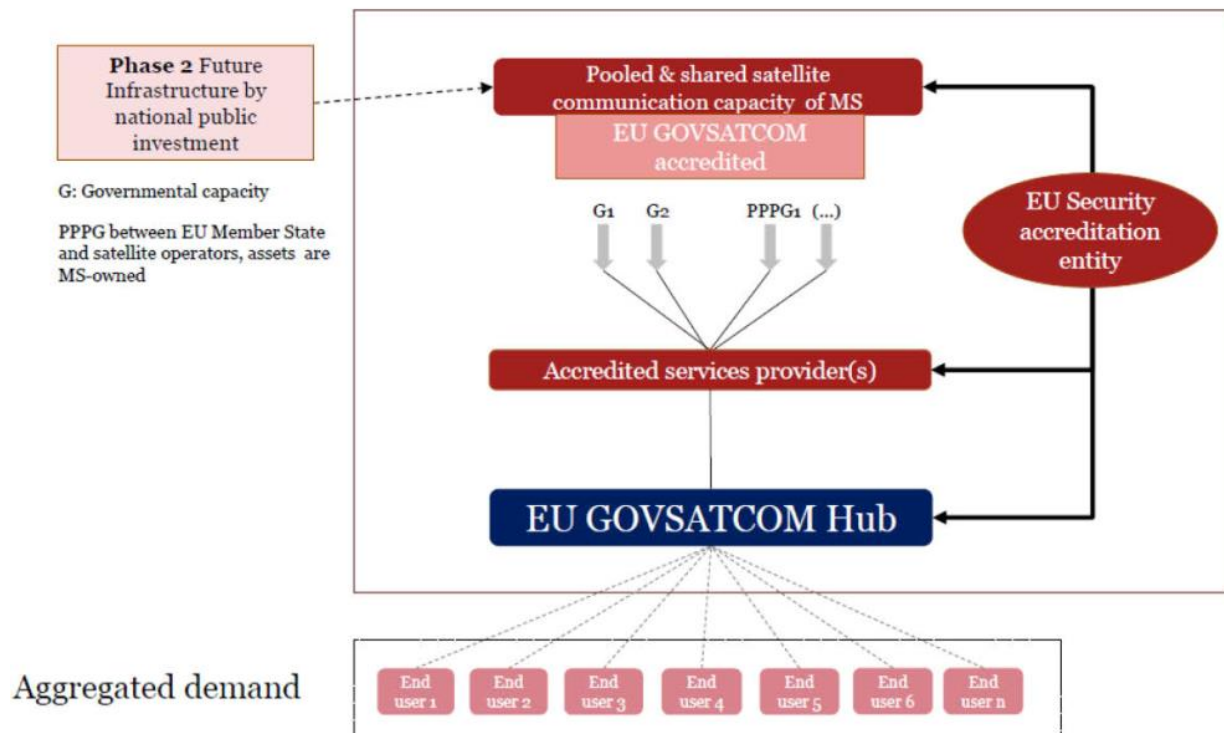


Figure 2: Option 2 - Usage of Member States' space assets [13]

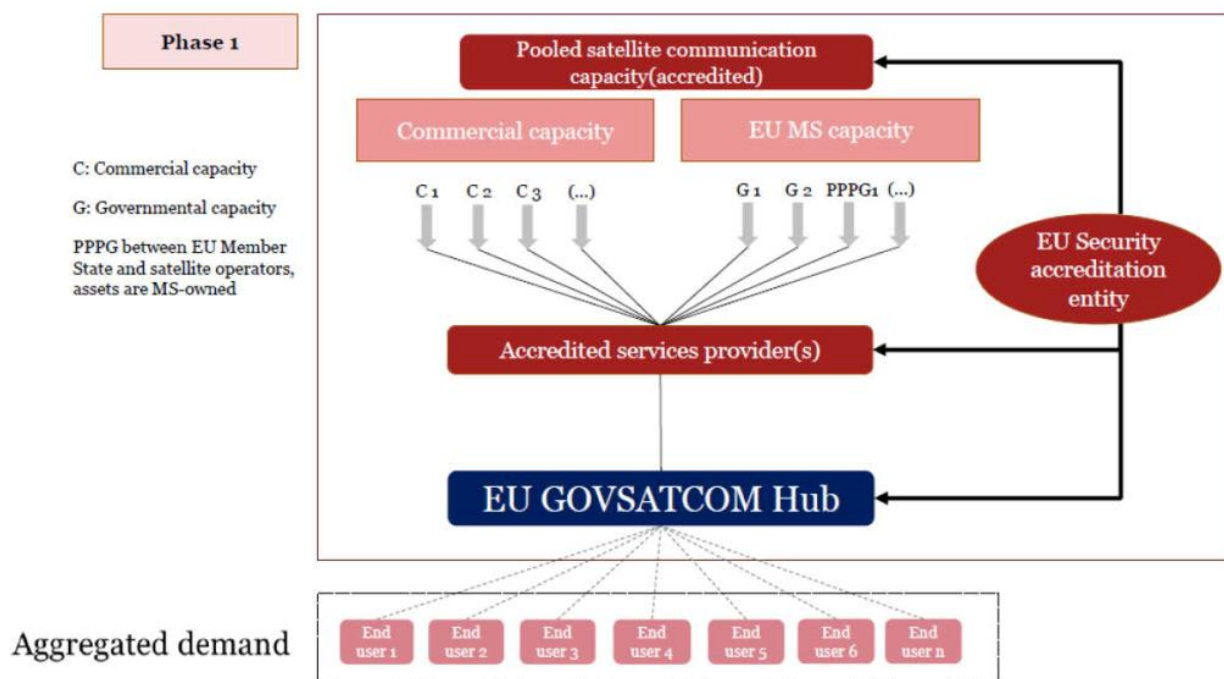


Figure 3: Option 3 - Sharing commercial (Phase 1) [13]

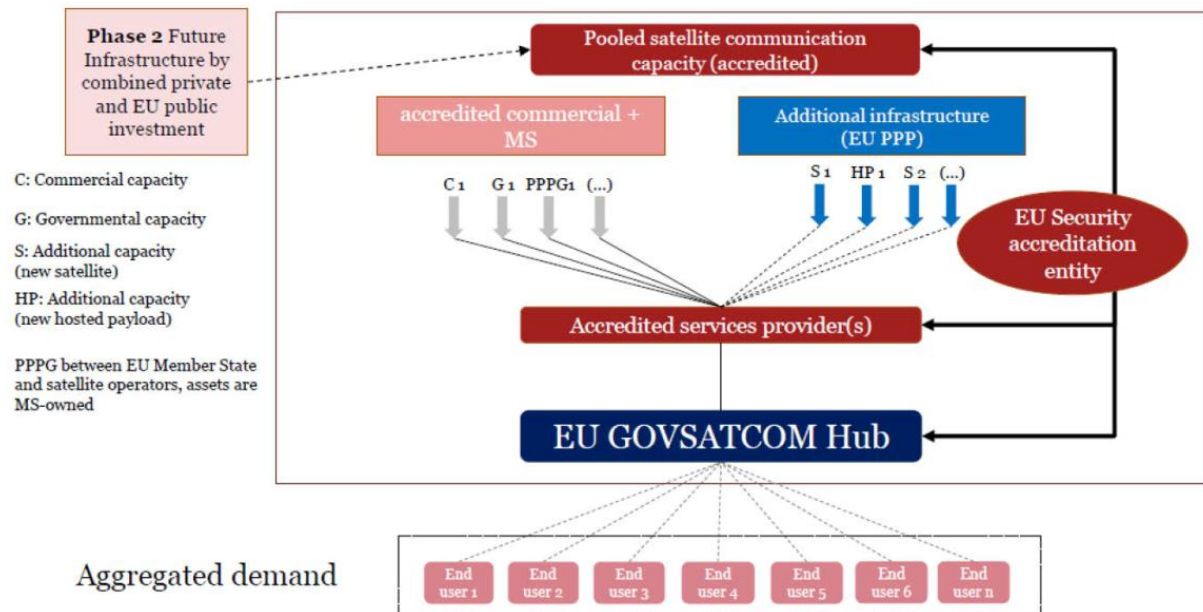


Figure 4: Option 3 - Public-Private Partnerships for future space assets (Phase 2) [13]

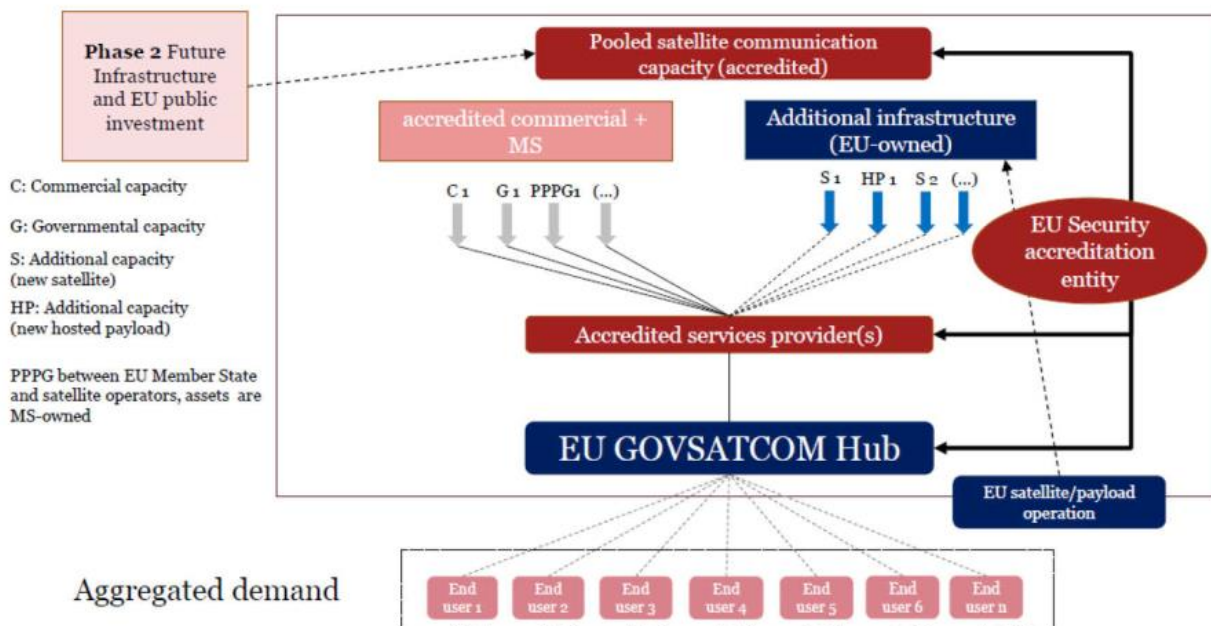


Figure 5: Option 4 - Usage of future EU space assets (Phase 2) [13]

Option	Aggregation of demand (civ/mil, EU/MS)	Security accreditation against joint security requirements	SATCOM capacity provided by	Phase 2 Investment for new space infrastructure	EU ground infrastructure needed
0	No	No	Private (global) National EU MS US WGS	Private (global) National EU MS US WGS	None
1	Yes	Yes	Private (EU accredited)	Private (EU accredited)	EU GOVSATCOM Hub
2	Yes	Yes	MS national	MS national	EU GOVSATCOM Hub
3	Yes	Yes	Private (EU accredited) MS national	Private (EU accredited) MS national EU level PPP	EU GOVSATCOM Hub
4	Yes	Yes	Private (EU accredited) MS national	Private (EU accredited) MS national EU owned	• EU GOVSATCOM Hub • Centre to operate EU-owned satellites

Table 1: Summary of different GovSatCom implementation options' characteristics [13]

Each strategy depended on consolidating user needs at both EU and national scales, ensuring security accreditation, and establishing "GovSatCom Hubs". These operational centers would securely link users with various providers, making the most of available resources and ensuring connectivity, even in unforeseen circumstances. GovSatCom Hubs and potentially other ground components, such as anchoring stations, are required to optimize the available satellite communication resources, to ensure reliable access during unforeseen events like natural disasters, and to maintain operational effectiveness with quick response times [14].

The design of these facilities should be driven by operational needs and security mandates, such as the distribution of GovSatCom Hubs across multiple physical locations to reduce potential risks. As GovSatCom users can be considered public authorities, bodies entrusted with the exercise of public authority, international organisations or natural or legal persons, authorized with responsibilities related to the supervision and management of security-critical missions, operations, and infrastructures. Users of GovSatCom will receive access to service levels that correspond to the risk level of their space missions or operations, considering factors such as the importance of the operation, the type and classification of information being transmitted, and the current level of threat.

During the initial stage of GovSatCom initiative, which is estimated to last until 2025, the defined strategic plan is to utilize existing satellite capabilities. Within this period, the European Commission is expected to procure GovSatCom capacities from Member States that have their own national systems and space capabilities, as well as from private satellite communication or service providers, while taking into consideration the European Union's critical security interests. The deployment of GovSatCom services will follow a gradual implementation process.

However, during the initial stage, in case of a detailed analysis of future supply and demand will demonstrate that the followed gradual implementation process is insufficient

to cover the evolving demand, there may be a decision to proceed to a second phase. This subsequent phase could involve the development of tailored space infrastructure or of additional capabilities, potentially through one or more public-private partnerships, such as collaborations with EU satellite operators. The GovSatCom infrastructure's development will cost up to 100 M€, while in the operational phase the cost is expected to be up to 100 - 150 M€ per year [15]. Additionally, while the fundamental objective is to offer GovSatCom services free of charge to its users in case an analysis identifies that there is a capacity shortfall, the establishment of a pricing policy will be considered as part of the rules for sharing and prioritization, to prevent distortion of the market.

During the implementation phase, the assignment of roles and respective responsibilities amongst specialized entities, including the EDA, European External Action Service (EEAS), ESA, Agency, and other relevant agencies of the Union should be strategically and tactfully performed to avoid conflicts of interests and achieve segregation of duties. Within the context of GovSatCom, the Commission has stated its commitment to collaborate with the EEAS, EDA, which acts as a facilitator, the European Union Satellite Centre (Sat Cen), Member States, and ESA to investigate potential dual-use synergies in the space programs, enabling civil satellites to be utilized for military operations, and reinforcing cooperation at the European Union level on space defense initiatives.

Prior to the existing EU program, the EDA had already been involved in developing a GovSatCom service for EU Member States, with the participation of fifteen (15) countries. In that context, the EDA collected and identified the operational defense requirements and supported the Ministries of Defense as a facilitator. Additionally, the EDA's Pooling and Sharing Demonstration Project to test the pooling and sharing concept of national satellite capabilities for military users entered its execution phase in January 2019 [16].

The designated GovSatCom competent authority plays a critical role in overseeing and monitoring the compliance level of users and other GovSatCom involved entities with the defined rules on sharing and prioritization and security requirements. Any Member State that has not appointed a specific GovSatCom competent authority should, at the very least, appoint a contact point responsible for managing the response to any jamming incidents that impact GovSatCom services. Member States, the Council, the European Commission, and the EEAS can participate to GovSatCom initiative, either via authorizing GovSatCom users or contributing resources, such as space capabilities, sites, or other facilities.

While Member States have the discretion to approve users or offer specific capabilities, they are not required to join as participants of GovSatCom or to house GovSatCom infrastructure. As a result, the creation of the GovSatCom framework acknowledges the right of Member States to abstain from involvement in GovSatCom, consistent with their domestic legislation or constitutional requirements regarding policies of neutrality and non-engagement in military alliances.

The ENTRUSTED (European Networking for satellite Telecommunication Roadmap for the governmental Users requiring Secure, interoperable, innovative, and standardised services) project demonstrated live satellite connectivity use cases, in March 2023, in the context of specific GovSatCom's use cases to highlight the benefits of secure SatCom capabilities and to prove that the concept of pooling and sharing of existing capabilities (e.g., GEO satellites) owned by EU Member States is possible and realistic.

The main objective of the ENTRUSTED demonstrations was the showcasing of pooling and sharing service provision model, of access to telecommunication services in remote areas where terrestrial network is unavailable, of access to secure satellite communications in crisis situations, as well as of secure telecommunication services in

terms of confidentiality, integrity, and availability. More specifically, four (4) demonstrations were performed, one that show cased the assistance in case of disaster and armed conflict, that was executed by Luxembourg / Luxembourg Space Agency (LSA) along with the participation of civil protection actors, another one about secure communications for national diplomacy / EU delegation, that was performed by Greece / Hellenic Ministry of Digital Governance along with the participation of diplomatic staff and EU Agencies, one about the access to GovSatCom services for military users in the context of CSDP, that was executed by the European Defense Agency along with the participation of military actors, as well as one about satellite connectivity in emergency situations, that was performed by Italy / Italian Space Agency (ASI) and Luxembourg / LSA along with the participation of emergency operators [Image 2].



Image 2: ENTRUSTED GovSatCom demonstrations [17]

More specifically, as diplomacy is a governmental activity where secure connectivity is considered as a crucial strategic asset, the secure communications for national diplomacy network demonstration that was conducted by Greece / Hellenic Ministry of Digital Governance [Image 3] included three (3) specific operational scenario assumptions. The first assumption was that the satellite communication between the Ministry of Foreign Affairs and Ministry of Digital Governance was established through Hellas Sat capacity in Ku-band and the GreeCom Satellite Distribution Centre (Hub), with remote terminals installed in embassies in Lisbon (Portugal), Prague (Czech Republic) and Nicosia (Cyprus).

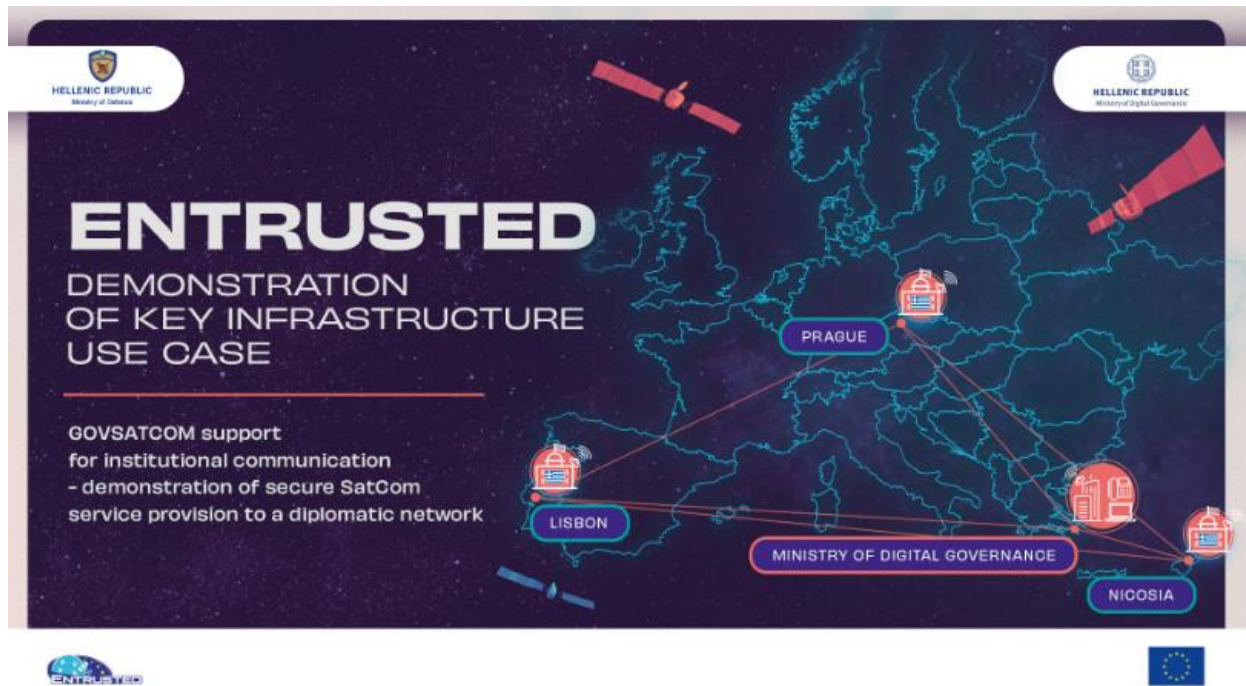


Image 3: ENTRUSTED GovSatCom demonstration by Greece [17]

The second operational assumption was that the communication of the Greek government with its embassies in the EU should be reliable and secure, due to exchange of confidential information, in the event of any interruption or unavailability of services provided through terrestrial telecommunication networks across Europe, while the third assumption was the usage of a secure video-conference application to exchange information between the various users. Upon completion of the demonstration, the Hellenic Ministry of Digital Governance and the Ministry of Defense proved that governmental satellite communications ensure confidentiality, integrity, and availability of transmitted information within a diplomatic network, as well as that GovSatCom services are invaluable when decisions must be taken fast, and the connectivity needs to be reliable and secure [17].

Summarizing, GovSatCom will allow Member States to share the overcapacities of their government-owned (non-military) communication satellites to provide reliable, resilient, secure, with adequate protection against interception, interference, cybersecurity risks, and intrusion, and cost-efficient satellite communication services for EU and national public authorities managing security critical missions and infrastructures. The core of GovSatCom consists of the aggregation of demand, common security requirements and accreditation, as well as pooling and sharing of national and commercial space resources.

2.2 Vision and Strategic Objectives

The space sector, with a special emphasis on satellite communications, is becoming increasingly vital to the EU's security, economic well-being, and competitive edge. Satellite communications are now fundamental components for a range of critical activities, including defense, security, humanitarian aid, emergency services, and diplomatic interactions. Current and future security risks affect the whole EU, and therefore, EU in order to effectively execute the various critical space missions and operations, mitigating and responding to evolving threats, such as pandemics, cybersecurity attacks, and natural disasters, need access to secure means of communication, in cases that the ground-based communication systems are not

available, either due to the fact that they do not entirely exist (e.g., in remote areas) or because they are disrupted or unreliable (e.g., in case of an earthquake or ill-intentioned activities).

Today, there is a misalignment between these risks and needs, as well as the available solutions, which are in many cases inappropriate, fragile, and/or not secure, increasing the attack surface, and creating risks for the key missions and security operations of EU. Consequently, the key drivers for GovSatCom implementation are the fragmented supply and demand for secure satellite communications, the growing security needs of users, and the evolving threat landscape (e.g., cybersecurity) and technology advancements [Image 4].

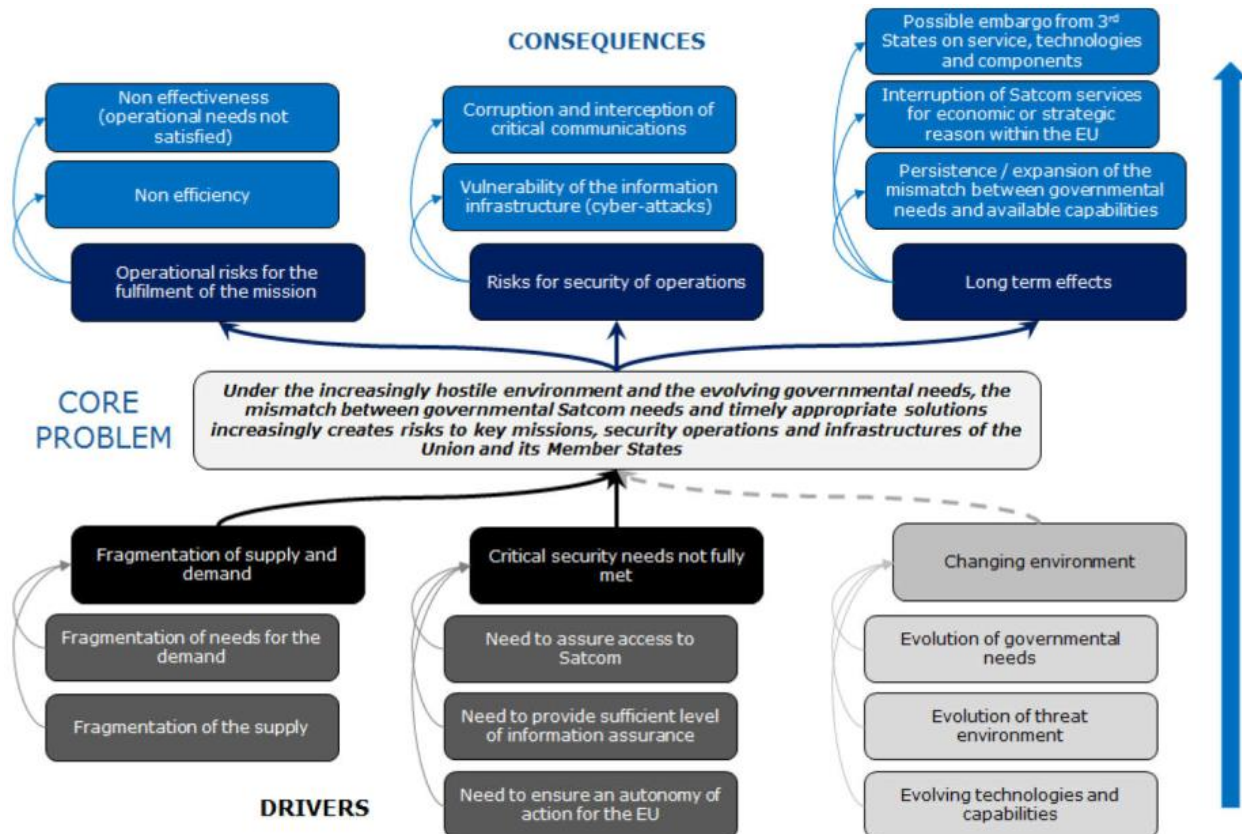


Image 4: EU GovSatCom problem tree [13]

Taking this into consideration, the GovSatCom initiative's vision is to ensure the provision of long-term available, uninterrupted, resilient, reliable, secure, flexible, and cost-effective governmental satellite communications services for EU and Member States' public authorities, natural or legal persons, such as Non-Governmental Organizations (NGOs) acting on behalf of the EU, and other actors, as well as, under certain conditions, third countries and international organizations, supervising and managing critical missions and infrastructures, while also ensuring protection against interference, interception, intrusion, and cybersecurity attacks [18].

Implemented in collaboration with the EU Member States, EUSPA, EEAS, ESA, and with a vast majority of other EU agencies and actors, GovSatCom aims to provide an appropriate level of European technological, asset-based, operational, and services-based non-dependence [19]. By guaranteeing continuous access to robust satellite communications, GovSatCom aims additionally to ensure that users' security needs for their day-to-day operations, including the transmission of sensitive information, are

properly met [20]. More specifically, the following paragraphs define and analyze the strategic objectives of GovSatCom initiative.

One of the strategic objectives of GovSatCom is the enhancement of the European Union's competitiveness in the space sector, emphasizing on satellite communications. In this context, the initiative aims to foster innovation, exploiting a combination of secure SATCOM services, such as Mobile Satellite Service (MSS) and Fixed Satellite Service (FSS), as well as research and development activities across the EU's space industry, which are vital for sustaining technological advancement and economic growth. GovSatCom not only aims to maximize the utilization of existing satellite communication infrastructures, but also to enforce the design and development of new cutting-edge space technologies. Such activities will not only address current and future operational requirements, but will also stimulate the market, creating opportunities for research and development, while also ensuring that Europe remains at the forefront of the global space industry, capable of delivering secure, reliable, and resilient communication services to meet the needs of governmental users, and thus enabling appropriate level of autonomy, and resilience in critical communication infrastructures. This high-level strategic vision can be translated into tangible benefits, such as enhanced emergency response communication systems and secure data links, which are essential for both day-to-day business operations and crisis situations. Therefore, through GovSatCom, the EU will be able to establish a robust foundation for technological advancement and space industry growth, driving towards a more interconnected and secure future.

The achievement of European appropriate level of strategic autonomy, especially in sensitive areas such as defense and security, is a pivotal objective of GovSatCom initiative, addressing the European Union's necessity to reduce dependency on third countries for space-related technologies, assets, operations, and services. In an increasingly interconnected world where space capabilities are critical for national security, this initiative highlights the strategic importance of developing indigenous space capabilities. GovSatCom also highlights the advantages of pooling and sharing model, which not only optimizes resource utilization across the EU, but also leverages collective expertise to enhance the overall space capability. Interoperability of services is also achieved based on pooled and shared capacities from different satellite systems [21].

GovSatCom is strategically designed to encourage and enhance cooperation among Member States, as well as align the different involved EU's institutions and agencies. This collaborative approach aims to establish a harmonized and more efficient environment for implementation of space communication initiatives within Europe, leading to a consolidated and more secure European space infrastructure, reinforcing the EU's position in global space initiatives with greater independence. GovSatCom not only strives to protect the EU's strategic interests but also aims to set the foundations for collaboration in space, resulting to the creation of a robust, interconnected European space network that can ensure uninterrupted services. Therefore, EU will become a self-reliant space power capable of independently fulfilling its space communication needs.

Furthermore, the enhancement of civil protection and humanitarian efforts at the European level is another key strategic objective of GovSatCom, focusing on the effectiveness and responsiveness of these critical services. This initiative recognizes the essential role that reliable and high-capacity satellite communications play in coordinating disaster management efforts, managing emergencies, and delivering aid to affected populations. By equipping civil protection and humanitarian agencies with advanced communication technologies, GovSatCom aims to streamline operations, enabling rapid deployment and more efficient use of resources during crises.

The accessibility of real-time data and secure communication lines is crucial for decision-makers and on-the-ground teams to assess situations accurately, coordinate efforts, and execute life-saving measures with precision and agility, benefiting directly and indirectly the social benefits of European citizens. Direct benefits include the enhanced capability of respective teams and authorities to safeguard lives and properties during disasters, with improved disaster preparedness and response times. Indirectly, the initiative contributes to fostering a sense of security among communities, knowing that robust systems are in place for their protection. The broader social impact of GovSatCom involves facilitating continuity of communication in remote or underserved areas, promoting social inclusion, and supporting the digitization of public services, all of which serve to enhance the quality of European citizens' lives. By emphasizing the enhancement of civil protection and humanitarian interventions, GovSatCom is not merely an investment in technology, it is an investment in the well-being and safety of individuals across the continent, underpinning the EU's commitment to its citizens in times of need.

Furthermore, the aim of GovSatCom towards the defragmentation of governmental satellite communications systems represents a crucial step in unifying space capabilities across Europe. This initiative has the objective to transcend the existing fragmented landscape from both the demand and supply sides by aggregating the continent-wide needs for SatCom and leveraging nationally owned systems into a cohesive network. By cultivating a substantially large pool of space capabilities, GovSatCom intends to achieve enhanced geographical coverage that ensures seamless connectivity across the entirety of Europe, regardless of the location. GovSatCom, also, is intended to be an integrated program leveraging the synergies with services provided by other space programs, such as Galileo, EGNOS, Copernicus, and Space Situational Awareness (SSA). This consolidation will not only unlock more available frequencies, but also enable more efficient utilization of the existing satellite assets, ultimately optimizing the overall investment in space infrastructure.

Furthermore, the defragmentation strategy is designed to foster civil-military synergies, breaking down the silos that traditionally separate civilian and defense space operations. Such a unified approach promises to amplify the strategic value of SatCom resources, enabling dual-use capabilities that cater to a wide spectrum of applications, from supporting emergency services to bolstering national security measures. The civil and military synergies will not only enhance interoperability and flexibility, but also lead to cost efficiencies, and a stronger, more resilient European space communications posture. Through this initiative, Europe aims to solidify its space communications infrastructure, delivering a robust foundation for connectivity and reinforcing its appropriate level of strategic autonomy on the global stage.

An additional GovSatCom's objective is the implementation of cost-effective solutions, to provide free of charge access to robust satellite communication services, capitalizing on economies of scale that emerge from collective European demand. This forward-thinking approach minimizes financial barriers for entities in need of satellite communications, thereby democratizing access to these critical resources. GovSatCom effectively decreases costs through bulk procurement and shared service models, that benefit all users, while to further optimize costs, GovSatCom is designed to leverage the existing satellite communication assets already owned by EU Member States and commercial entities. This utilization of pre-existing infrastructure not only ensures cost-efficiency by avoiding unnecessary expenditure on new systems, but also accelerates the rapid deployment of services. Such a strategy enhances the speed at which satellite communications can be made available, particularly in scenarios requiring immediate action.

Moreover, the integration of diverse asset portfolios from across the EU and commercial spectrum enables GovSatCom to provide a wider range of service offerings, tailored to the distinct needs of its users. This holistic approach ensures that the varying requirements of civil, governmental, and military users are met with a high degree of flexibility and customization. Through this pragmatic combination of cost-saving measures and effective utilization of existing assets, GovSatCom positions itself as an enabler of comprehensive, resilient, and affordable satellite communication solutions critical for Europe's present and future needs.

Finally, the implementation of secure solutions is one of the main objectives of GovSatCom, aiming to establish a secure space communication environment that meets the security requirements of EU's and Member State's governmental users. More specifically, GovSatCom services aim to be resilient against jamming and interference, as well as protected against interception, intrusion, and cybersecurity attacks. GovSatCom is intended to be implemented considering a set of industry standards and best practices to ensure the preservation of high level of confidentiality, integrity, non-repudiation, and authenticity. This comprehensive security approach ensures that governmental entities have secure and reliable access to satellite communications, which is essential for the execution of their critical functions. The importance of such secure communication cannot be overstated, particularly in sensitive operations where the protection of data and communication channels from unauthorized access and cybersecurity threats is paramount.

GovSatCom's security level will indicatively enable the national and EU-level entities to communicate with confidence during the planning and implementation of strategic missions. In alignment with these security goals, GovSatCom is designed to support pivotal EU's missions that highly rely on secure and resilient communication. These missions include a wide range of activities, including but not limited to border protection, maritime surveillance, crisis management, and humanitarian aid operations, each of which require a tailored communication solution that assures privacy and security in potentially hostile or unpredictable environments. GovSatCom's commitment to secure solutions essentially acts as the backbone for various EU-led missions, enabling governmental bodies to perform their duties effectively while safeguarding data and communications against the evolving threat landscape. This not only fortifies Europe's collective security architecture but also enhances its capability to manage and respond to crises with agility and secure communications [22].

2.3 Core Capabilities

Apart from the initiative's strategic objectives, the EU's GovSatCom aims to bridge the gap between the growing needs for secure governmental communications and the capabilities offered both by existing and planned satellite communications systems and infrastructure.

During the first implementation phase that is expected to be running until 2025, as already mentioned, GovSatCom is planned to utilize the existing capabilities and services provided by a pool of commercial and military satellite communication providers, while its services will be accessed only by authorized users by a GovSatCom authority, like Galileo PRS. GovSatCom benefited users will be the national and EU security actors, such as police and homeland security forces, border surveillance authorities, firefighters, military forces, maritime community (including Maritime Safety Agencies and Fisheries Agencies), services in charge of external action, civil protection organizations, providers of humanitarian assistance, operators of essential infrastructure and industrial bodies, encompassing space infrastructure operators, satellite providers, producers of space and

terrestrial infrastructure, providers of space-related services, and transport infrastructure operators (such as entities overseeing air, rail, and road traffic), in addition to EU institutions, and the diplomatic networks of the EU and its Member States (for instance, EU Delegations and Embassies of the Member States) [23].

Users may also include natural or legal persons acting on behalf of the EU with responsibilities relating to the supervision and management of security-critical missions, operations, and infrastructures [23]. GovSatCom users will be duly authorized by a GovSatCom participant to use GovSatCom capacities and services and shall comply with the general security requirements for GovSatCom. Even though the Small to Medium-sized Enterprises (SMEs) and the micro-enterprises will not significantly be affected by the GovSatCom, their contribution is considered beneficial for technological advancement and fostering of innovation purposes, and therefore specific rules to enforce and to facilitate their involvement should be established.

Governmental users will gain access to GovSatCom services, with priority given based on the risk level linked to their missions, such as the critical nature of operations, the type of information being transmitted, the degree of threat, and the urgency of their needs. In more detail, the collective satellite communication capabilities, services, and user equipment will be allocated and prioritized among GovSatCom participants following a thorough evaluation of the safety and security risks associated with the users. This assessment will consider the current communication infrastructure, the reachability and readiness of present resources, and their geographical spread, both across the Union and within individual nations.

The Commission will establish comprehensive rules on the allocation and prioritization of satellite communication capacities, services, and user equipment through implementing acts. These rules will consider the anticipated need for various GovSatCom applications, the security risk assessments pertinent to those applications, and, where relevant, the cost-effectiveness. To ensure an optimal balance between the availability and requirement of GovSatCom services, the Commission is charged with the continual supervision and assessment of the evolving landscape of supply, which includes the existing GovSatCom capacities in space designated for collective use and distribution, as well as the demand for GovSatCom capabilities and services. This will factor in the evolving risks and threats, in addition to technological progress.

The sharing and prioritization of satellite communication services will be authorized by the GovSatCom participants, which are expected to be the Member States, the Council, the Commission, and the EEAS. In instances where the Council, the Commission, or the EEAS grant permission to GovSatCom users, or provide satellite communication capabilities, terrestrial segment sites or segments of terrestrial infrastructure within a Member State's jurisdiction, this action should not breach any stipulations regarding neutrality or non-alignment embedded in the constitutional legislation of the respective Member State. EU Agencies may become GovSatCom participants to the extent that it is essential for the performance of their responsibilities and duties. This participation will adhere to the specific rules outlined in an administrative agreement established between the relevant Agency and the Union institution responsible for its oversight.

Moreover, nations outside the EU and international entities may join the GovSatCom program. Each member must appoint a qualified GovSatCom authority. This authority is responsible for ensuring that service usage adheres to relevant security protocols, user access rights are appropriately assigned and controlled, user devices and related electronic communications and data are managed in line with security standards, and a central contact point is established to aid in reporting security risks and threats, especially in identifying potentially damaging electromagnetic disruptions to the services within this

sector. Institutional and governmental users of GovSatCom will be granted access to these capacities and services at no cost, except in cases where the Commission establishes a pricing policy. The Commission will define a pricing policy to ensure both the non-disruption of the market by the supply of GovSatCom capacities and services, as well as the adequate availability of GovSatCom capacities. Respective implementing acts will also be published.

GovSatCom will apply to a wide range of space operations, having although, three main use cases, one of which is the crisis management, due to both natural and man-made disasters, such as humanitarian crisis and maritime emergencies, including civilian, military security and defense related missions, as both military and civilian responders need guaranteed services for communication and exchange of information with, and between, their rear bases and command and control centers. Another use case of GovSatCom is the surveillance, such as border and maritime surveillance, pre-frontier surveillance, sea-border surveillance, and surveillance of illegal trafficking, as surveillance operators need the collected information by surveillance platforms to be distributed in near real time to the relevant actors to minimize the time lapse between the detection of an event and the intervention of the relevant response team. While the third use case is the key infrastructures support, in domains including, but not limited to, diplomatic networks, police communications, humanitarian aid (e.g., EU missions and delegations around the world), space (e.g., Galileo, EGNOS and Copernicus), aviation (e.g., Air Traffic Management) and land transport (e.g., Intelligent Transport Systems, Rail Traffic Management), digital infrastructure (e.g., data centers and servers), as well as critical infrastructures (e.g., energy, transport and water barriers, dams), as the existence of a secure and available communication link between operational platforms / infrastructures and control centers is a key requirement [Image 5] [24].

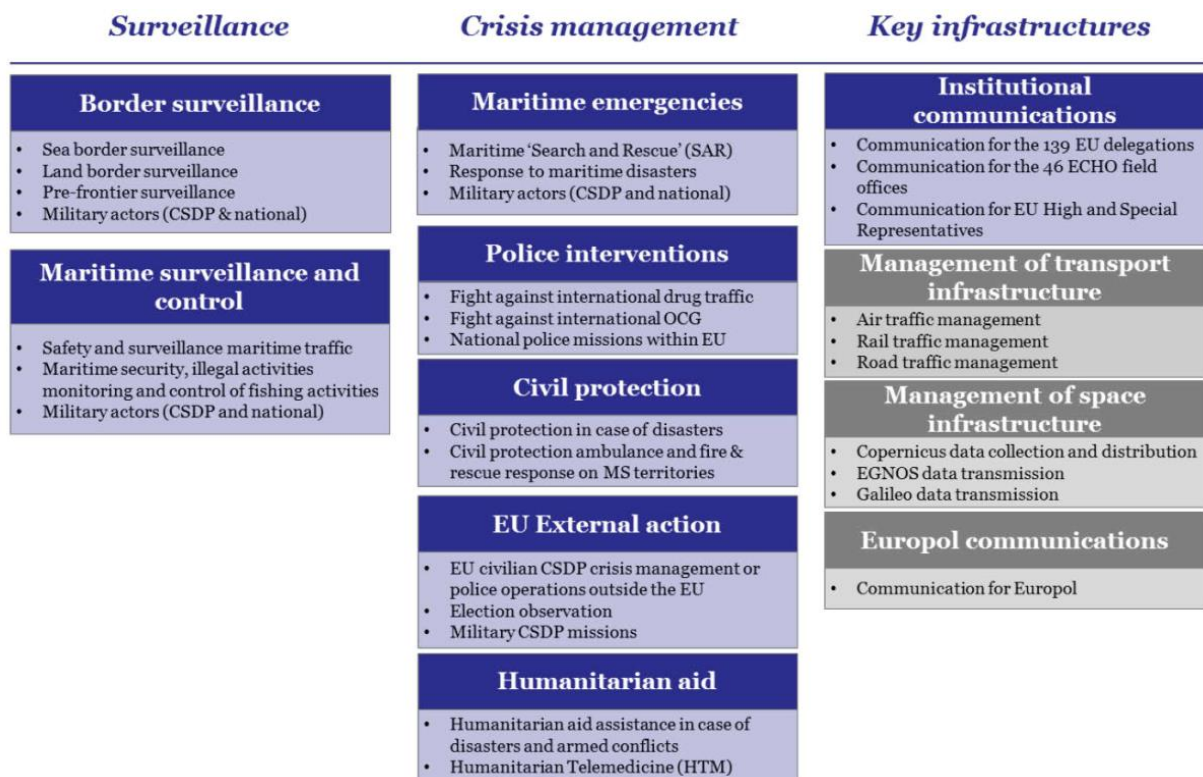


Image 5: EU GovSatCom main use-case families [13]

The European Commission is tasked with establishing the functional specifications for GovSatCom services through implementing acts, which will take the form of technical

guidelines for various GovSatCom applications. These operational specifications will be derived from an in-depth examination of GovSatCom user needs and will consider the necessities arising from current user equipment and networks.

Additionally, three complementary cross-domain use cases have been identified that require secure satellite communications, which are the Arctic region, in which human activities, and in particular maritime traffic, continuously increase but there are not solid terrestrial communication infrastructures, the Remotely Piloted Aircraft Systems (RPAS) along with their acquired data, which are increasingly used in crisis management and surveillance operations, and the applications that utilize Internet of Things (IoT) technology, such as Machine-to-Machine (M2M) applications, in order to monitor other types of key infrastructures (e.g., dams, dykes, bridges, and power plants) which rely on M2M to retrieve information from on-site sensors [25].

Furthermore, to GovSatCom services portfolio are included the communication services, such as voice, images, email, chat, messaging, video conferencing, transmission of high-resolution radar and optical images, broadcast and multicast data services, low data rate transmission and remote and secured access to specific information systems will be supported by GovSatCom [26]. More specifically, GovSatCom will support telemedicine which is crucial for life safety as medical technologies rely on Information Communication and Technology (ICT), such as X-Ray, Computerized Tomography (CT) and Magnetic Resonance Imagery (MRI), logistics/administrative support, being important for managing cargo and asset tracking information, procurement and purchasing of systems, and welfare, which is critical for the provision of communication services (such as email, video conferencing and web browsing) enabling effective, private communication. The delivery of satellite communication capabilities and services under GovSatCom will be performed by GovSatCom participants, as well as by legal persons authorized to offer such capacities and services following the security accreditation process. This must be executed in compliance with the general security requirements for the GovSatCom component [27].

The Commission will issue, via implementing acts, a comprehensive catalog of GovSatCom services, presenting a spectrum of satellite communication capabilities and services along with their detailed features, such as geographic coverage, frequency bands, bandwidth, user equipment, and security features. The formulated service portfolio will consider the existing commercially accessible services to prevent any competitive imbalance within the internal market. These implementing acts will be regularly updated and will be defined in alignment with the operational and security requirements. Furthermore, these services will be prioritized and allocated to users based on their significance and criticality. GovSatCom users will have access to the GovSatCom capacities and services listed in the service portfolio, while the access to these services will be provided through the GovSatCom Hubs.

Satellite communications is resource constrained by the capacity of satellites, available frequencies, and the extent of satellites' geographical coverage. As a result, to achieve cost-effectiveness, benefit from the advantages of large-scale operations, and capitalize on economies of scale, GovSatCom should optimize the balance between its users' requirements and the available resources outlined in contracts for GovSatCom capacities and services. Given that user demand and available supply change over time, ongoing monitoring and adaptability are essential in adjusting GovSatCom services accordingly. Based on equipment's interoperability and compliance with standards of the various user communities, the GovSatCom system will be compatible with most of the existing users' terminals [28].

From an operational perspective, GovSatCom will be able to provide web connectivity, flexibility, and scalability upon demand, as well as integration with fixed and mobile platforms. GovSatCom provided near-real time connectivity services are expected to cover an area of around 1000 km in diameter, primarily the continental Europe and its neighboring regions (e.g., Africa, Mediterranean, Middle East Asia, Arctic, and Atlantic) but secondarily all over the world in order to support crisis management operations, being available in less than forty eight (48) hours or less than twelve (12) hours when first responders are prepositioned with compatible terminals on the mission area [29].

In order GovSatCom to operate effectively, EUSPA has been entrusted with the establishment and management of the network of GovSatCom users, which already includes more than twenty (20) organizations, including Member States and EU Agencies, aiming to identify user needs and use cases for GovSatCom services, through ENTRUSTED (European Networking for satellite Telecommunication Roadmap for the governmental Users requiring Secure, inTeroperable, innovativE, and standardised services) project. ENTRUSTED is a European research project, coordinated by the European GNSS Agency (GSA), leading to a roadmap of activities regarding the enhancement of GovSatCom to meet users' community needs [30].

EUSPA, also, entrusted with the support in the definition of the security controls that should be implemented to ensure the fulfillment of the security requirements, as well as with the definition of the secure architecture principles that should be applied to the ground infrastructure, GovSatCom Hubs, which will incorporate all central functions to organize and manage demand and supply, making GovSatCom services available to the governmental users. Settled on secured and protected from a physical security aspect site, and while aggregating the users' demands, GovSatCom Hubs will combine and link different satellite and ground infrastructures capacities into a system-of-systems approach, monitoring and ensuring the capacity, service planning, and security of the overall system [31].

2.4 Operational Requirements

In order GovSatCom to be able to achieve its strategic objectives, as well as provide its core capabilities should ensure the fulfillment of its operational requirements. The current section defines the primary operational requirements of GovSatCom which play an integral role for its proper functionality, ensuring the provision of secure, reliable, and resilient communication, which is vital for national security, emergency responses, and governmental strategic operations.

The terrestrial architecture of GovSatCom should incorporate the necessary facilities to deliver the satellite communication services to its users, which are the GovSatCom Hubs that should be designed to connect GovSatCom clients and providers of satellite communication capabilities [Image 6].

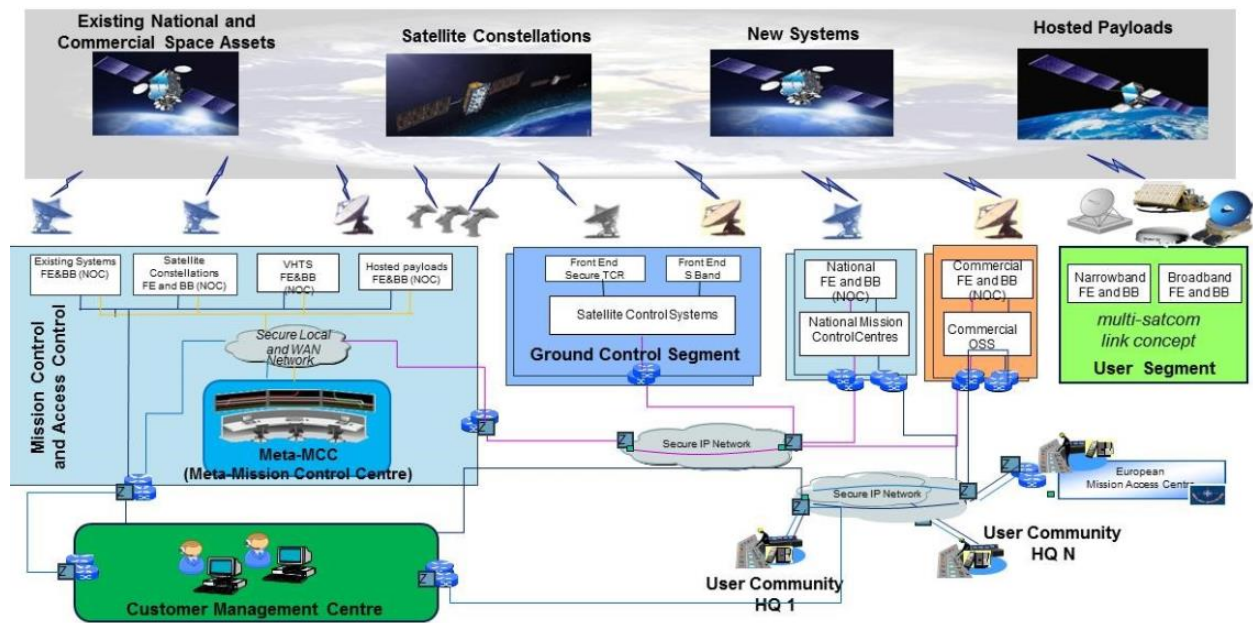


Image 6: EU GovSatCom architecture [32]

The terrestrial operations and their management are expected to align and comply with the appropriate security protocols. The Commission will determine the GovSatCom Hubs locations for the terrestrial infrastructure components, through relevant implementing acts [Image 7]. These acts will take into consideration the scrutiny requirements, while enabling the individual Member States' right to opt-out of hosting this infrastructure.

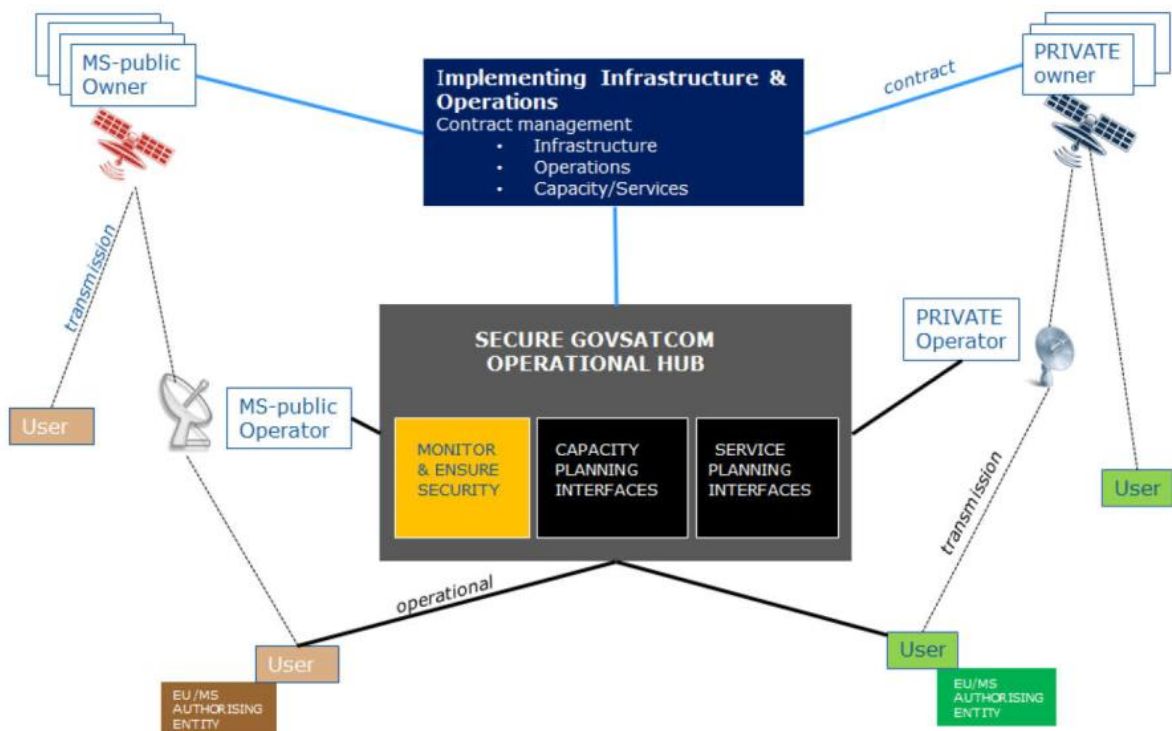


Image 7: EU GovSatCom Hubs architecture [13]

As already explained, the GovSatCom architecture will adopt the principle of pooling and sharing, providing services from a predefined set of current, scheduled, and prospective satellite communication capacities. The pooling and sharing concept will be conducted by the Secure Meta Mission Control Centre (Meta-MCC), which is expected to orchestrate

the SatCom resources to effectively accommodate the requests of the end-users of GovSatCom services. Several existing and emerging SatCom resources have been pinpointed for potential inclusion within the GovSatCom sharing resources, with some of them being still in preliminary design phase to ensure fulfillment of GovSatCom operational and security requirements. These SatCom resources will have diverse frequency bands to meet the various needs of the different services' end-users [32].

During the 2016 Council Meeting at Ministerial Level (CM16), the European Space Agency initiated the GovSatCom Precursor Program. With a funding allocation of eighty-five (85) million euros, this Program was designed to incentivize the space industry to develop innovation-driven digital platforms, known as Pooling and Sharing (PSS) systems, which are another one operational requirement for GovSatCom. The primary objective of these systems was to enable a dynamic and efficient alignment of satellite communication operational and security requirements with available Satcom resources [33]. They were specifically designed to meet the relevant standards of reliability, availability, and security mandated by both institutional and commercial entities. This investment catalyzed the performance of four (4) distinct projects that were executed by satellite operators, collectively referred to as "PACIS", which took place from 2016, and could be beneficial for the achievement of GovSatCom's operational efficiency.

PACIS-1 is the pioneering initiative in the ESA's GovSatCom Precursor Program, marking an essential milestone for secure satellite communications in supporting the European Union's vision for the GovSatCom project. This platform aims to provide access to SatCom services for government sectors and public institutions, meeting critical needs that span from civil protection, border management, humanitarian efforts, and maritime monitoring, while ensuring comprehensive service needs coverage. In a unique public-private partnership, an alliance with SES has the objective to design the foundational architecture and conceptualize the service blueprint.

The consortium offers advanced collective expertise, taking advantage of the strengths of Redu Space Services, GovSat, Newtec, QinetiQ, and Tekever, creating a robust network of space assets and ground facilities. The GovSatCom demonstrator by SES Networks will offer secure communication services to governments and institutions, utilizing a variety of satellites and spanning multiple frequency bands. SES Networks has constructed a specialized Government Mission Operations Centre (GMOC) located in Redu, Belgium, to facilitate the deployment of GovSatCom services. This center is designed for mission control, operations, and service provision. The GMOC will facilitate the integration of space and ground segments from various providers, operating across different frequency bands and incorporating diverse VSAT platform technologies. Focusing on delivery of tailored satellite capacity and bandwidth that adapts to the needs of distinct missions, priority, and location, registered users will witness the agile allocation of resources. The operational agility of the GMOC will provide the ability for response to real-time demands for satellite services, ensuring that critical space and satellite missions are not just supported but empowered. Relying on existing and upcoming assets, the space segment will be sourced from European operators and managed by GMOC.

Initial demonstrations will be performed in the C, X, Ku, and Military Ka frequency bands, utilizing technologically advanced space assets to serve the various user communities, from security forces to humanitarian agencies and Non-Governmental Organizations (NGOs) [34]. Leveraging both current and newly deployed resources at the ESA facility in Redu, the ground segment is enhanced by additional European teleports, such as the SES main office in Luxembourg. Redu plays a crucial role in delivering satellite services to the European Union, as evidenced by the technical operations for Galileo and the European Geostationary Navigation Overlay Service (EGNOS) being situated there. The

site also provides backup telemetry, tracking, and command (TT&C) capabilities for SES, as well as essential ground infrastructure for the European Data Relay System (EDRS). Within this highly secure ecosystem, advanced anti-jamming and stress response mechanisms operating with fine-tuned automation will be deployed, guaranteeing users uninterrupted and resilient communications, from both intentional and incidental disruptions.

The PACIS 2, with Spain's participation, is focused on creating a smart system for managing satellite communication traffic. The project's foundation is built on leveraging the complete potential of satellites, including the flexibility of their antennas and operational processes, to facilitate communication between terrestrial stations and satellites based on diverse user policies and priorities. The aim of the project is to demonstrate the beneficial impacts of the system, particularly in areas such as telemedicine and crisis management [35].

PACIS 3 is another project of the GovSatCom Precursor Program aiming to ensure the provision of secure communications. The primary goals of the PACIS 3 project include the creation and integration of adaptable X-band active antennas capable of both transmission and reception for secure communication, as well as the establishment of a deployable platform equipped with six (6) Ka-band antennas, each of which can be independently directed. This initiative pieces together the intricate puzzle of cutting-edge, reconfigurable X-band active antennas coupled with a pioneering deployable pallet of Ka-band antennas, that can pivot with precision for highly secure communications. The X-band active antennas are the most challenging active antennas developed in Europe, positioning Hisdesat and the Spanish space industry at the forefront of space technology in active antennas. Two (2) Direct Radiating Arrays (DRA) for transmission and reception, beams crafted through software for adaptable coverage, innate on-board geolocation capabilities, and advanced interference cancellation techniques are integrated into PACIS 3.

Additionally, a Ka-band antenna system offers exceptionally accurate ground station orientations, in contrast with conventional mechanisms. Bridging the gap between sophistication and miniaturization, X-band Multichip Control Modules (MCCM) will provide high-performance hybrid circuitry, maintaining the precision of the communication signals. In an environment where temperature plays a critical role, the project will deploy X-band Collecting Heat Pipe Assemblies (CHPAs) and Loop Heat Pipes (LHPs) [36]. These elements will act as conduits, directing excess heat to the spacecraft's wall panels, ensuring the Active Antenna operates within optimal thermal ranges.

Furthermore, the X-band Dual Solid State Power Amplifier (DSSPA) will also be deployed, which is a pioneering addition based on gallium nitride (GaN) technology. Primed for its maiden voyage into space, this amplifier promises high radio frequency power levels, extraordinary resilience, and exemplary performance within the harsh temperature fluctuations characteristic of space. Once the PACIS 3's technological symphony harmonizes in orbit, the door will open for institutional stakeholders to participate in early service demonstrations, utilizing the array of communication assets-from sophisticated links to beam-hopping and geolocation experiments, that this groundbreaking endeavor provides. In essence, PACIS 3 will not just enhance communication capacities, but it will reshape the future of antenna technology and thermal management.

PACIS 4 project, which includes Italy's involvement, is in the process of designing a cutting-edge user terminal for RPAS (Remotely Piloted Aircraft System) that enhances commercial data transmission services. The objective of this project is to showcase the advantages of employing government operated RPAS in executing tasks for national

security agencies by utilizing an updated government user terminal along with government satellite communications.

PACIS 5 was launched in mid-2017 with a life span period over two (2) years, representing a forward leap in the dynamic allocation of satellite capabilities tailored for governmental use. This project is divided into two distinct, yet interrelated components. The initial part is dedicated to establishing an adaptable system designed for the shared use of satellite resources. The core of the ground system is based on the Newtec Dialog technology developed by the Belgian company Newtec and will be installed at the Airbus site in Toulouse, being designed to serve the European governmental agencies, with a particular focus on support for overseas operations. An end-to-end service demonstration highlighted the system's capabilities, showcasing its adaptability and user-friendly interface. The second part of the project concerns a technological development designed to improve the performance of Newtec Dialog platform [37]. The objective was to utilize the pooling capability for next generation of governmental satellites, which present the revolutionary feature of real-time configurable coverage zones.

This innovation enabled mobile users to switch transparently from one satellite beam to another while at the same time protecting the confidentiality of their operations. This development was a natural succession to Airbus's involvement in two foundational design studies conducted between 2015 and 2017, which were orchestrated on behalf of both ESA and the European Defense Agency [38]. These studies laid the groundwork, for the clear definition of European governmental user needs and assessment of the various technologies and architectures in preparation of a future European Commission GovSatCom program, as well as the advantages of the pooling and sharing model. Therefore, PACIS 5 is not just a standalone endeavor but a pivotal connector in the joint efforts of driving Europe toward a new frontier in governmental satcom solutions.

PACIS 6 shaped the future landscape of commercial secure satellite communications with the establishment of an open platform designed for the pooling and sharing of such services. The GovSatCom PACIS 6 consortium, led by Inmarsat, presented expertise of key players, including CGI in cybersecurity and digital transformation, as well as AnsuR and Teamnet, which specialize in government solutions and applications. The inception of PACIS 6 promised to lay the groundwork for a streamlined 'one-stop-shop' in satellite communications procurement tailored to the needs of European governmental bodies and the wider global market. This development aimed to provide customers the flexibility to select from a suite of government-specific terminals, satcom services, and applications, all customized to align with their unique operational requirements and financial constraints.

Throughout 2018 and 2019, PACIS 6 was actively conducting a series of "Sprinter Demonstrations" [39]. These demonstrations were designed to simulate mission scenarios that highlight the effectiveness of SatCom services when leveraged through a pooling and sharing approach. The demonstrations had the objective to reveal the potential advantages this strategy can offer to the missions and operational outcomes of end-users. Moreover, the project leveraged these demonstrations to illustrate the delivery methods for applications and services via the new service delivery platform, to support end-user missions. Application providers were invited to explore collaboration opportunities with PACIS 6 at Inmarsat, establishing how their offerings might be featured within the framework of these Sprinter and/or Mission Demonstrators, taking advantage of the opportunities presented by federated, pooled, and shared SatCom services. This initiative was a transformative catalyst for satellite communication models, echoing a future where collaboration and shared utility are keystones in the evolution of governmental SatCom solutions [40].

In order pooling and sharing capability to operate effectively, the coordination of end users is of paramount importance. Entities such as the European Defense Agency, Frontex, the European Maritime Safety Agency, the European Fisheries Control Agency, Europol, and the joint planners of military and civilian operations alongside the Emergency Response Coordination Centre, could each act as a liaison for distinct user groups, spanning national and civil-military domains. To ensure that user feedback and needs are taken into consideration in the governance of GovSatCom the abovementioned agencies will have coordinating roles for specific user groups, which is a crucial operational requirement for GovSatCom. For civilian-centric user communities in particular, the Agency is proposed to play a central role, orchestrating user-related aspects. This could range from monitoring the actual utility of services to assessing compliance with established requirements, while concurrently keeping a pulse on emerging needs and requirements. By adopting this structured approach, GovSatCom aims to enhance responsiveness to user groups, thereby ensuring that their specific communication demands are met effectively within the GovSatCom's governance.

The tactical and strategic effectiveness of satellite communications relies on the capabilities and compatibility of the user equipment. GovSatCom aims to ensure a seamless transition and robust integration for users by designing a system architecture that supports the continuity of service with the users' pre-existing equipment. This continuity is not only a testament to the forward-thinking approach of GovSatCom, but also to its commitment to user convenience and cost-effectiveness, as it mitigates the need for investments in new hardware.

To further enhance the operational effectiveness and collaborative potential of the various user groups, GovSatCom also prioritizes the interoperability of user equipment. This enables users from different sectors and missions, such as defense, law enforcement, or emergency response, to communicate more effectively during joint operations, which is critical in both national and multinational efforts. By aiming for this level of equipment compatibility, GovSatCom addresses a significant aspect of operational readiness. Reliability in communications during mission-critical operations, training exercises, and response to emergencies become more attainable through user equipment that can operate across different service providers and platforms. Ultimately, the emphasis on using existing equipment and enhancing its interoperability within the GovSatCom initiative resonates with the broader goal of aligning satellite communication capabilities with the dynamic and increasingly complex needs of its users. This approach not only facilitates a smoother operational transition, but also supports the evolution and expansion of satellite communications services to meet future challenges and requirements.

Summarizing, the main operational requirements of GovSatCom are the terrestrial GovSatCom Hubs, the Pooling and Sharing (PSS) systems, that the PACIS projects aim to establish and enhance, the coordination of specific user groups, as well as the compatibility of preexisting users' equipment.

2.5 Limitations and Challenges

Having analyzed the vision, strategic objectives, as well as the main capabilities of GovSatCom, that include but are not limited to the establishment of a framework for secure and resilient satellite communications, enhancing national security level, facilitating disaster management, enabling remote sensing, and supporting various other critical functions, it should also be defined the limitations and challenges of GovSatCom. These challenges, ranging from governance to technical constraints, that will be analyzed to the current section, necessitate good understanding to take advantage of the full

potential of satellite communications for governmental purposes. Through an in-depth analysis of these challenges, this study aims to provide valuable insights into optimizing GovSatCom capabilities and maximizing its benefits.

The governance of GovSatCom initiative, to operate effectively, presents a challenge regarding the coordination among various involved stakeholders, fostering collaboration across diverse parties responsible for managing the initiative's execution. The effective governance of the initiative requires maintenance of balance between ensuring organizational stability and accommodating the divergent perspectives and priorities of Member States and other involved parties on critical issues defining the efficiency and seamless execution of GovSatCom. In this context, another issue is the process of stakeholders' collaboration to define a consolidated set of user and mission requirements, considering the users' needs, cost-effectiveness, timelines, as well as broader European technological and industrial perspectives, which serve as the foundation for deriving GovSatCom services.

Apart from the stakeholders' coordination related challenges, another governance-oriented challenge is about the appropriate risk ownership and management allocation. More specifically, the inherent complexities of satellite communication initiatives necessitate a thorough consideration of risk-sharing mechanisms, encompassing financial and security-related risks, among stakeholders best equipped to manage them. Therefore, the governance-related challenges of GovSatCom to be overcome requires a comprehensive approach that transcends mere administrative coordination, requiring adept negotiation skills, strategic foresight, and a nuanced understanding of the complex interplay between governance structures, policy imperatives, and stakeholder dynamics.

Another challenge and/or limitation is financial-oriented, as the inherent financial risk in GovSatCom exists in the context of insufficient funding from Member States and private sector, which poses a significant threat to the successful implementation of the initiative [41]. The effectiveness of the procurement process is crucial, as it can significantly affect the required budget for the realization of the initiative's objectives, considering and balancing the emerging needs with the available financial resources. Generally, the complexity of financial risk demands scrutiny and strategic foresight, necessitating a proactive approach to risk management that encompasses robust contingency planning and prudent resource allocation strategies. Implications of financial risk can influence on the GovSatCom's long-term sustainability and operational effectiveness. Therefore, to address the challenge of financial risk a robust financial planning framework characterized by transparency, accountability, proactive stakeholders' engagement, and decision making, as well as cost-benefit analysis is required.

Furthermore, among complexities of GovSatCom initiative's implementation, there is a significant challenge related to the timeline of the initiative's execution. The success of GovSatCom depends not only on the efficacy of its strategic vision and technological prowess but also on the timely execution of its implementation roadmap. The realization of timeline risk can disrupt the carefully designed sequence of activities and jeopardize the window of opportunity within which the initiative operates. Any delay in implementation not only undermines the initiative's momentum but also causes a domino effect of cascading impacts, potentially leading to cost overruns, resource misallocation, and diminished operational effectiveness. The interaction between timeline risk and cost dynamics highlights the need for adoption of proactive risk management strategies that prioritize adherence to strict timelines without compromising on quality or operational integrity. To efficiently mitigate the timeline risk, proper planning, robust project management, and agile decision-making are required. Additionally, effective time management mechanisms must be in place to anticipate, identify, and respond to

potential delays promptly, thereby safeguarding the GovSatCom's viability and resilience in unforeseen contingencies, enhancing its operational agility and unlocking the full spectrum of initiative's capabilities.

An additional challenge that threatens the effective implementation of the GovSatCom initiative is the industrial risk, and more specifically the collaboration and coordination of multiple industrial players across diverse geographic locations, being responsible to develop and upgrade the satellite communication related infrastructure components essential for the initiative's successful implementation. The inherent complexity of integrating these disparate entities into a cohesive ecosystem is affected by the transnational nature of industrial collaboration, necessitating balance between harmonizing diverse stakeholder interests, and ensuring adherence to the defined security requirements, as well as commitment to preservation of the desired quality. Mitigation of industrial risk demands a comprehensive approach that spans the entire project lifecycle, from procurement and contracting to implementation and maintenance phases of GovSatCom's implementation. By fostering a collaborative approach, GovSatCom can take advantage of the collective expertise and ingenuity of industrial partners to forge a resilient and future-proof satellite communication infrastructure that underpins its strategic objectives. Therefore, the mitigation of the industrial risk is of paramount importance for the initiative's success, enabling the effective collaboration of various industrial partners, and safeguarding the initiative's execution against potential vulnerabilities inherent in industrial collaboration.

Within the ambitious framework of the GovSatCom initiative, another challenge that arises is in the context of technological aspect, as GovSatCom is designed to operate with cutting-edge technology, the validation of which remains an ongoing and evolving endeavor [42]. The adoption of state-of-the-art technological solutions introduces inherent complexities and uncertainties, requiring attention to detail and a proactive approach towards risk mitigation. Among these technological complexities is the requirement to ensure implementation of robust cybersecurity measures, safeguarding critical satellite communication infrastructure against ever-evolving cybersecurity threats and vulnerabilities.

Moreover, the resilience of GovSatCom against malicious interference, such as jamming and signal disruption, emerges as a critical priority, underscoring the need for implementation of respective controls to mitigate these risks. The dynamic nature of technological innovation necessitates a flexible governance approach that can adapt to emerging threat landscape, while fostering a culture of innovation and collaboration among various stakeholders. To mitigate the existing technological challenges requires a comprehensive methodology that encompasses rigorous testing, validation, and ongoing monitoring of technological solutions, coupled with proactive measures to address emerging cybersecurity threats and vulnerabilities. By addressing this technological challenge, GovSatCom can fortify its technological resilience, enhance its operational effectiveness, and unlock the full potential of satellite communication for governmental purposes in an increasingly complex and interconnected digital landscape.

In conclusion, the successful implementation of the GovSatCom initiative not only represents a significant milestone in advancing the European Union's strategic objectives but also has the potential to elevate the EU as a prominent global player in satellite communications. By harnessing the transformative power of satellite technology, GovSatCom holds the promise of fostering diplomatic relations, enhancing national security, and stimulating economic development across the EU region and beyond. However, realizing these aspirations hinges on effectively navigating the multifaceted governance challenges inherent in the initiative, ranging from technological complexities

to industrial collaboration and cybersecurity concerns. Through proactive risk management, strategic foresight, and collaborative engagement with stakeholders, the EU can position itself at the forefront of innovation and leadership in satellite communication, unlocking new frontiers of opportunity and prosperity in an increasingly interconnected world.

2.6 Implementation Reasons

2.6.1 Technological Advancement and Innovation

Taking into consideration the capabilities, limitations, and challenges of GovSatCom initiative, along with the capabilities and limitations of other existing space communications programs, there are various reasons that support the implementation need of GovSatCom, the most critical of which will be analyzed in detail to the current section.

More specifically, as already mentioned, the implementation of GovSatCom represents a pivotal step towards fortifying the technological advancement and innovation within the European Union. The strategic importance of such initiative cannot be overstated, as it promises to establish a solution for secure and resilient satellite communications for European industry, enhancing its competitive position in the global arena. GovSatCom initiative outlines a comprehensive framework for sustained investment in Research, Development, and Innovation (RDI), crucial for leading-edge advancements. RDI can be performed regarding the foundational elements of GovSatCom initiative, which are indicatively, but are not limited to, the pooling and sharing of satellite resources, the security accreditation mechanism, as well as the terrestrial GovSatCom Hubs [43]. Therefore, this initiative represents a driving force for technological innovation and advancement.

Additionally, as one of the main GovSatCom's objectives is the fostering of EU's appropriate level of autonomy, ensuring the European space industry remains innovative and competitively robust, the efforts for technological excellence are certain both from the public and private sector, as well as from small and big enterprises in EU level, while the Small and Medium Enterprises are recognized as the lifeblood of innovation. To capitalize on the vast potential of SMEs, it is imperative that potential public-private partnerships are structured to foster inclusivity, facilitating access for SMEs. This approach will also accommodate new market entrants, while simultaneously offering the stability required to attract participation from businesses of various scales.

Further evidence of the initiative's commitment to innovation is found in the significant challenge of developing the technologically advanced EU GovSatCom Hubs. Insights from consultations with industry experts and stakeholders, as well as findings from studies conducted by key agencies such as the European Space Agency and the European Defense Agency, emphasize the critical nature of this undertaking [13]. Investment in cutting-edge infrastructure, including the GovSatCom Hubs and future enhancements, such as complementary payloads and satellites, aiming to achieve comprehensive global coverage and introduce novel services, is set to advance the space industry. These investments are deliberate, setting ambitious technological goals that act as a motivation for industry to delve into research and development, fostering innovation, and ultimately augmenting the Union's competitiveness on the global stage.

In conclusion, the implementation of GovSatCom initiative is not merely beneficial, instead it is essential. It encapsulates a strategic vision that converges the technological advancement and continuous innovation, underpinning Europe's commitment to growth and evolution of the European space industry.

2.6.2 Connectivity Across EU

Generally, in the modern era, geographically extended connectivity is a necessary and strategic asset for all nations. In this context, the inception of the Governmental Satellite Communications initiative supports the growing need for the establishment of an intercontinental communications network, enabling connectivity across EU. Current connectivity architectures exhibit disparities in service coverage, resilience, and security, which are challenges that mainly and commonly affect the remote and underserved areas. The fragmented nature of existing satellite communications solutions often results in lack of reliability and accessibility, a difficulty that GovSatCom aims to overcome. Therefore, this initiative represents a strategic investment aiming to unify disparate systems into an integrated EU communications network, thereby ensuring consistent and secure communication channels across various geographical locations.

By establishing a satellite communications network that exceeds terrestrial limitations, this initiative enables the support of various critical functions, from enabling effective disaster management and humanitarian relief, to facilitating secure diplomatic communication channels and robust military communications. Analyzing the enablement of connectivity across EU through GovSatCom from a contributory aspect, is anticipated to serve as a critical enabler for strengthening the European alliances and collaboration. By providing a secure and resilient solution for the exchange of data, GovSatCom is expected to support joint scientific ventures, transnational security operations, and European initiatives. Therefore, the implementation of GovSatCom will enable the existence of robust satellite communications capabilities, as well as the realization and establishment of a comprehensive and harmonious European community.

From a technical perspective, the pursuit of connectivity across EU via GovSatCom aligns with the pursuit of high-capacity and high-availability satellite services with advanced security protocols to mitigate the emerging cybersecurity threats and risks. More specifically, the design and implementation of GovSatCom is performed based on the results of an assessment of the operational needs for satellite communication in various scenarios, ensuring that the appropriate controls are implemented so as the communications infrastructure be resilient to both physical and digital disruptions. Therefore, the GovSatCom will not only enable European connectivity, but also aims to ensure secure connectivity, which is of paramount importance especially when exchanging confidential information during crisis situations.

In conclusion, the implementation of GovSatCom is not only an enhancement to existing communication infrastructure, but also a strategic and critical requirement considering the current landscape characterized by complex socio-political interdependencies and a growing need for information exchange. This initiative paves the way for a paradigm in which connectivity is democratized, secure, and resilient, a foundation upon which European prosperity and cooperation can be benefited. Furthermore, GovSatCom signifies a pivotal shift in strategic orientation, aligning with Europe's endeavors to enforce a new epoch in which communication barriers are overcome, establishing an integrated and cohesive society.

2.6.3 Secure Satellite Communications

The orchestration of the EU GovSatCom initiative is set to revolutionize the paradigm of secure satellite communications across Europe, addressing critical gaps evidenced in the existing communication infrastructures and solutions during crisis situations and performance of security operations. The implementation of this initiative is strategically envisioned to ensure assured access and enhanced level of secure connectivity, in

alignment with the defined security requirements. European security actors, ranging from military stakeholders to humanitarian aid responders, face various communication challenges, as the current SatCom capacities, in many cases, fail in delivering the required security assurance and operational reliability. Therefore, GovSatCom aims to address the identified risks by end users to the existing SatCom capabilities.

This initiative encapsulates the essential need for guaranteed and immediate accessibility to sufficient SatCom capacity, especially during unpredictable, crisis-driven situations. Events such as environmental hazards, geopolitical conflicts and cybersecurity attacks highlight the urgency of this need. Indicatively, forest fires, tsunamis, and earthquakes are prime examples where terrestrial communication infrastructures may be incapacitated, thereby amplifying the criticality of satellite communications for a timely and effective response that could significantly mitigate the impact of such disastrous events. Additionally, the aspect of information security plays an instrumental role in the EU GovSatCom's proposition. The initiative intends to provide to users a robust solution that ensures confidentiality, integrity, non-repudiation, authenticity, and unwavering availability. These dimensions of information security, which currently eclipse from the commercial SatCom capabilities, are paramount for the transmission of sensitive or classified information and for safeguarding operations from the adversarial location tracking and cybersecurity threats [13].

Furthermore, the prohibitive costs and operational impracticability for EU Member States and institutions to maintain reserved SatCom capacity with commercial operators highlight the need for a bespoke EU-driven solution. The EU GovSatCom's emphasis on guaranteed access within a short time window, as stipulated by the security actors' needs, is currently unmet by commercial providers. Therefore, this initiative aims to bridge that gap, serving as a linchpin for reliable and secure communication channels during crisis management and response. GovSatCom, also, has the objective to rectify the prevalent deficiencies within the SatCom environment by addressing the existing various risks, ranging from interoperability issues, prioritization biases, absence of coverage, prolonged service deployment, to susceptibility to jamming, spoofing, and the disruption of operations by third-party actors. By enforcing a comprehensive and robust security accreditation process, this initiative aims to ensure the confidence required for communication of sensitive information, proactively countering the threats of information leaks, and service interruptions. Additionally, GovSatCom is envisioned as a consolidatory force, ensuring autonomous, reliable, and secure SatCom capabilities for Europe. By harnessing the security and appropriate level of autonomy offered by GovSatCom, European actors will possess a useful tool that reinforces operational efficacy, provides a shield against information warfare, and protects the interests of the EU and its Member States.

In conclusion, GovSatCom emerges as an indispensable satellite communications solution, optimizing the security aspect, providing a strategic advantage to EU, and enabling the secure exchange of information, addressing the existing cybersecurity risks.

3. IRIS² INITIATIVE: ENABLING SECURE AND RESILIENT GOVERNMENTAL SATELLITE COMMUNICATIONS

3.1 Overview of Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) Initiative

In the digital age, global society transitions towards an era where economic stability and security are intricately linked to the assurance of secure and resilient connectivity. As we navigate through a decade marked by an increase in the demand for hyper-connectivity, significant technological advancement, and a drive towards digital independence, secure connectivity has emerged as a vital public resource, witnessing an unparalleled rise in the need for satellite communication services. In a geopolitical context, where the cybersecurity threats continuously become more sophisticated, there is an urgent need to enhance the security and resilience of the European Union's governmental SATCOM capabilities. This includes advancing towards solutions that offer greater security, reduced latency, and expanded bandwidth. In response to these evolving challenges and in support of the continent's appropriate level of autonomy and digital sovereignty, the European Union has launched an ambitious initiative to develop the IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite). IRIS² is set to become a foundational space-based component for a digital, resilient, and safer Europe, while also promoting European competitiveness and societal advancement [44].

In the war in Ukraine, satellite technology emerged as a pivotal element in crisis management and support of military operations. The conflict underscored the use of sophisticated technologies and cybersecurity attacks, prompting a reevaluation of defense capabilities and tactics. Space-based assets were key in the preparation and execution phases of the conflict, bolstering the mobility and accuracy of the Ukrainian military against a more formidable enemy. Additionally, the involvement of commercial entities in military endeavors has been noteworthy, with the Starlink satellite network by SpaceX providing substantial support to Ukrainian forces, enabling them to mount an effective defense against Russian forces and extend the duration of the conflict beyond initial projections⁴.

Commonly, in military attacks, incapacitating the adversary's communication centers is a strategic tactic to disrupt the enemy's command-and-control capabilities. This was exemplified by targeting Kiev's main telecommunications tower during the conflict in Ukraine. Cybersecurity attacks have risen as an efficient means to achieve similar disruptions. In contemporary warfare, launching initial offensives via cybersecurity attacks is increasingly prevalent due to its potential effectiveness, which may surpass that of conventional weapons. Prior to the escalation of the crisis, the Ukrainian government was subjected to two significant cybersecurity attacks on January 14 and February 16, 2022. The initial cybersecurity attack left numerous governmental websites nonfunctional, and the subsequent one impacted the defense ministry along with two (2) state banking institutions [45].

⁴ Kolovos, A. Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict. Aerospace Management and Control Laboratory, OCCASIONAL PAPER NO. 3, Automatic Control, Aerospace Technology, Defence Systems and Operations Division, Hellenic Air Force Academy, 2022. https://www.researchgate.net/publication/368806976_Commercial_Satellites_in_Crisis_and_War_The_Case_of_the_Russian-Ukrainian_Conflict

Additionally, before the conflict escalated, the commercial satellite network KA-SAT, managed by the U.S.-based company ViaSat, fell victim to a cybersecurity attack. The network, which delivers high-speed internet from a geostationary position 36,000 km above Earth, experienced extensive malfunctions leading to a partial network shutdown. The outage resulted in communication and service disruptions for a wide range of users, including the Ukrainian government, military forces, and tens of thousands of civilians and critical infrastructure across Ukraine and other European nations like Germany, France, Hungary, Greece, Italy, and Poland. While this incident fits the profile of a traditional anti-satellite activity, it uniquely targeted the terrestrial segment of the system, specifically the modems responsible for data transmission, rather than the space-based satellite components.

Therefore, the conflict in Ukraine has underscored the security weaknesses inherent in satellite systems, emphasizing the importance of ensuring reliable access and enhancing security measures to safeguard against interference and breaches. With satellite technology becoming ever more crucial to military operations, strategies involving anti-satellite measures are becoming a part of modern combat tactics. The impact of cyber-attacks on vital infrastructure has shown their capacity to interfere with communication, navigation, and other essential functions.

In this context, on 24th March 2022, the Council of the EU endorsed the EU's "Strategic Compass" for security and defense policy. Compass considers Russian military aggression against Ukraine on 24th February 2022, "a tectonic shift in European history". Strategic Compass note that "the EU is committed providing associated assets and the necessary strategic enablers, particularly [...] SATCOM" [46]. On 17 November 2022, the "European Security Connectivity project" has been renamed by the Commission to IRIS². On the 17th of November 2022, in a decisive trilogue meeting, the European Parliament, European Council, and European Commission under the Czech Presidency, granted approval to the EU Secure Connectivity Program for 2023-2027, with the goal of rolling out the Infrastructure for Resilience, Interconnectivity, and Security by Satellite (IRIS²) [47]. Shortly thereafter, on the 22nd and 23rd of November, the European Space Agency initiated a new optional program in connection with EU Secure Connectivity Program under its Telecommunications and Integrated Applications Directorate, as part of the ESA Council at the Ministerial Level. The provisional trilogue agreement (European Parliament, European Council, and European Commission) for the EU Secure Connectivity Program was validated by the European Parliament's Committee on Industry, Research and Energy on the 29th of November 2022, and now the stages of the formal adoption process are implemented. The Program's execution is planned to follow a phased approach, initially aiming to provide the initial services by 2024 and achieve full operational capacity by 2027 [Figure 6]. However, this initial timeline is subject to delays for a wide range on reasons.

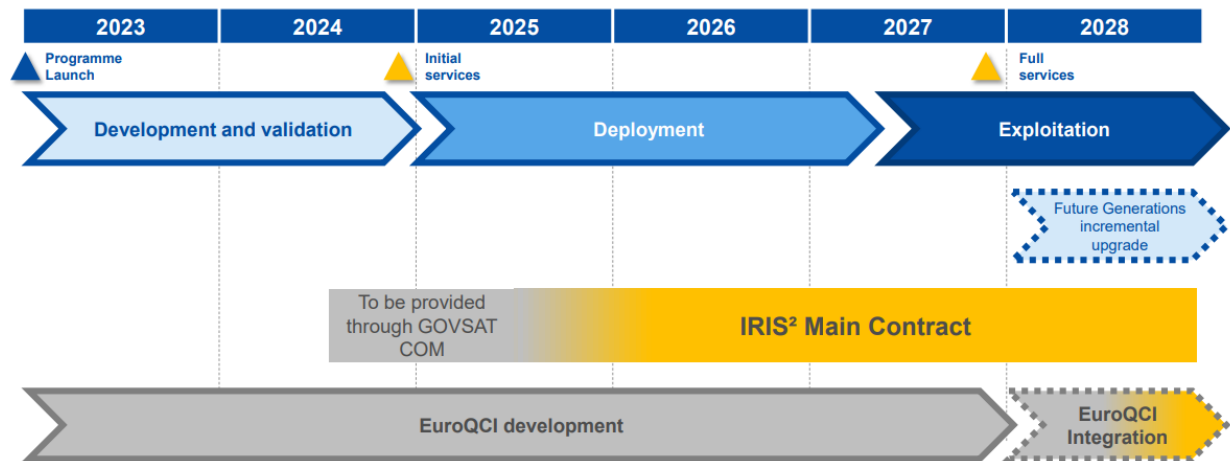


Figure 6: IRIS² initial implementation timeline [48]

Furthermore, given the existing limitations on submitting multiple applications and the rules for obtaining approvals, it is probable that these timeframes will be surpassed. These procedural delays have a knock-on effect on private investment in Europe, which lacks the catalytic boost of public funding that is available in the United States [49]. In preparation for this, the European Commission drafts implementing acts and tender specifications. In this context, on 30 March 2023, the European Commission organized an Industry Information Day on the call for tender for a Concession Contract for the implementation of the EU Secure Connectivity Program [Figure 7] [50].

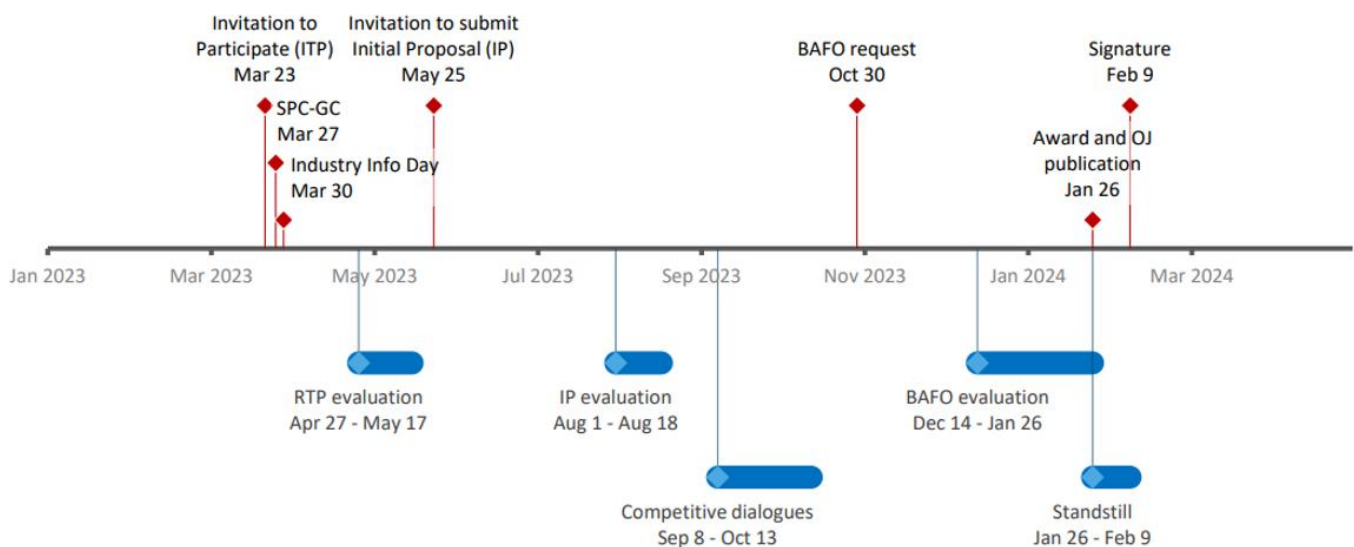


Figure 7: IRIS² initial procurement timeline [48]

In particular, the European Union's IRIS² is the new secure by design multi-orbital satellite constellation designed to meet future's communication needs. By combining the benefits offered from Low Earth Orbit (LEO), Geostationary Orbit (GEO), and Medium Earth Orbit (MEO), this constellation aims to deliver secure communication channels to the EU, its Member States, and beyond. This initiative aims to advance the communication capabilities provided to governmental entities and businesses, while simultaneously addressing the issue of Internet connectivity in areas previously plagued by poor access. Furthermore, this ambitious initiative has the objective not only to eliminate communication dead zones within the EU, fostering greater unity among Member States, but also to extend its reach to strategically important regions outside the Union.

Furthermore, the integration of cutting-edge technologies, including advancements in quantum computing, enables the IRIS² to ensure the long-term availability of reliable, secure, and cost-effective satellite communications services on a worldwide scale, leveraging also the "New Space" ecosystem. It should be highlighted that IRIS² aims to integrate the existing and future capabilities of GovSatCom, while EuroQCI will be an integral part of IRIS² [51].

IRIS² will support a wide array of governmental functions, particularly in areas such as situational awareness, with applications like border surveillance and monitoring, crisis management and response, including humanitarian aid, as well as safeguarding of critical infrastructure, exemplified by secure communication channels for EU diplomatic missions. Concurrently, on the commercial front, this initiative will enable a plethora of mass-market applications, including both mobile and fixed broadband satellite services, Business-to-Business (B2B) satellite trucking, enhanced connectivity for the transportation sector, strengthened satellite-supported networks, and integration of satellite broadband with cloud-based solutions. These applications promise to enhance connectivity and security across both governmental and commercial sectors.

The IRIS² infrastructure is envisioned as an integrated system of systems, including both space-based and terrestrial components necessary to deliver the IRIS² suite of Governmental and Commercial Services. In this context, IRIS² infrastructure is designed to be segmented into a Governmental Infrastructure, including a Shared Infrastructure, alongside a distinct Commercial Infrastructure. The Governmental Infrastructure, which shall be owned by the EU, encompasses all required ground and space assets dedicated to providing Hardgov Services, which are services for government-authorized users that require high level of security. The Shared Infrastructure, that is part of the Governmental Infrastructure, supports the provision of Hardgov, Lightgov, and Commercial Services, with the EU retaining ownership of the infrastructure itself, and the contractor maintaining ownership of payloads and subsystems for Commercial Services. Lastly, the Commercial Infrastructure consists of all space and ground assets that are not included in the Governmental Infrastructure, while it is owned and financed by the contractor. The Lightgov Services refer to those available to government-authorized users but do not require the stringent security measures and utilize both the Shared and Commercial Infrastructures, while the Commercial Services are designed for commercial users and leverage the Shared and Commercial Infrastructures [48].

In the Impact Assessment Report that accompanied the February 2022 proposal for establishing the EU Secure Connectivity Program, the European Commission delineated the financial blueprint for implementing the secure connectivity space infrastructure. The Commission's projections estimated the infrastructure's development and deployment to cost around €6 billion, including a mix of funding through a Public-Private Partnership (PPP), with €4 billion sourced from the public sector, including the EU and its Member States, complemented by €2 billion from private entities [52]. Following negotiations, the European Commission has committed €2.4 billion from the EU Space Program, Horizon Europe, and the Neighborhood Development and International Cooperation Instrument - Global Europe (NDICI) [52]. The Program's execution will occur in partnership with the European Space Agency, which, at CM22, sought €750 million and ultimately secured around €650 million in subscriptions [52]. This includes a pledge of up to €300 million from France, contingent on the eligibility of the consortia for IRIS², and substantial contributions from Germany and Spain, amounting to approximately €145 million and €41.5 million, respectively [52]. The Program also leverages non-EU contributions from Norway and Switzerland.

The impact assessment also forecasts significant economic gains from the new infrastructure, predicting a Gross Value Added (GVA) between €17-24 billion and the creation of additional employment opportunities within the EU's space sector [52]. The ripple effects are expected to extend to the broader economy, particularly through sectors that will utilize the innovative connectivity services. The anticipated Return of Investment (ROI) from the Secure Connectivity Program could potentially quadruple the revenue in terms of GVA.

However, in April Commissioner Bretton stated that the programme, which is considered as the EU alternative to Elon Musk's Starlink space-based communications network, [53] faces delays. These delays are due to the upcoming European elections, which will result in a new Parliament and Commission. The new Parliament's priorities might differ, especially if IRIS² costs increase [54]. Furthermore, it seems that major space powers like Germany and France have different priorities regarding the programme. Specifically, it seems that Germany is not happy with IRIS² being accused of serving mainly the French aerospace interests [55].

Summarizing, IRIS² initiative will ensure the resilient, secure, uninterrupted, and cost-effective provision of satellite communications services through a multi-orbital satellite constellation, which will incorporate the security-by-design principle reducing the probability of realization of cybersecurity threats and risks [56]. Additionally, IRIS² leveraging the robustness of quantum cryptography via the European Quantum Communication Infrastructure (EuroQCI), aims to deliver unparalleled security to its users. Furthermore, by incorporating cutting-edge technologies from both the established space industry and the dynamic "New Space" sector, IRIS² is designed to be scalable, catering to future demands with its versatile multi-orbital (LEO, MEO, and GEO) architecture. Therefore, this strategic initiative fosters an environment conducive to innovation, fostering EU's economic and societal advancement, as well as simultaneously promoting social unity by bridging the digital divide.

3.2 Vision and Strategic Objectives

In an era where economic stability and security are directly linked to robust and secure connectivity, Europe faces the imperative to implement an independent, secure, and resilient infrastructure for connectivity. Additionally, as digital interconnectivity and technological advancements emerge, there is a growing need for satellite communication services to be powered by cutting-edge technologies. In this context, the European Union's IRIS² initiative is designed to address these demands, ensuring access to secure, resilient, cost-effective, and high-quality satellite communications services, while minimizing reliance on non-European entities and bolstering the robustness of Europe's capabilities. Therefore, IRIS² is strategically positioned to fortify security and resilience, which is a crucial consideration for security and safety-sensitive critical missions and operations conducted by the European Union and its Member States.

Taking them into consideration, the overall vision of IRIS² initiative is to establish a multi-orbital satellite communication infrastructure to provide reliable, ultra-secure and resilient satellite communication services to meet the needs of European governmental bodies, while fostering innovation, leveraging the capabilities of "New Space" ecosystem, and integrating advanced technologies, such as quantum communication, to protect Europe's critical information exchanges against emerging cybersecurity threats and to guarantee access to secure satellite communication services without dependence on external entities.

One of the strategic objectives of IRIS² is the fostering of technological advancement and innovation. This strategic objective is designed to be achieved by engaging stakeholders

from the dynamic “New Space” sector, and more specifically engaging both established space industry players and disruptive forces within the “New Space” ecosystem, ensuring infrastructure’s adaptability to future demands through a versatile multi-orbital strategy, encompassing Low, Medium, and Geostationary Orbits. The fresh perspectives and inventive solutions offered by “New Space” participants promise to deliver advanced and innovative services that will benefit a wide range of users. Furthermore, IRIS² supports the active involvement of Small and Medium-sized Enterprises (SMEs) and startups, not only by setting aside a significant portion of contract value for subcontracting, but also by creating opportunities for these entities to contribute their own innovative services, harnessing groundbreaking technologies to their fullest potential [57].

Apart from that, in the realm of disruptive technologies, Europe has a satellite communications industry that has the capacity to make the necessary technological leap and bring Europe to the forefront of technological advancement and innovation. Furthermore, IRIS² aims to initiate the necessary research and development, as well as engineering endeavors, to lay the groundwork for development of later increments of the initiative’s infrastructure. Ultimately, this endeavor aims to provide state-of-the-art satellite communication services within the EU by constructing and managing a versatile multi-orbital connectivity framework. This infrastructure will be designed to flexibly adjust to changing user requirements and to forge new, customized, and pioneering applications and services.

Another strategic objective of IRIS² is the delivery of high quality and cost-effective satellite communication services to authorized governmental users. By enabling access to governmental user terminals compatible with open standards and nonproprietary solutions, including 5G Non-Terrestrial Networks, IRIS² emphasizes on the use of open-source technologies and interoperability to reduce costs associated with the provision of governmental satellite communications services, and more specifically for both Hardgov and Lightgov services. Furthermore, the initiative’s innovative approach regarding multi-orbital architecture will enable the offering of satellite communications services of diverse coverage, bandwidth, and latency options. Integrating capabilities from Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO) will facilitate uninterrupted internet access across the Union, eliminating areas with no communication coverage and enhancing unity within the territories of the Member States. Finally, IRIS² aims to enhance synergies with existing EU Space Programme components like Copernicus, Galileo, and EGNOS, fostering new opportunities for integrated applications with multiple functionalities in crucial areas, such as maritime emergency response and disaster management.

IRIS² is, also, strategically designed to guarantee comprehensive worldwide coverage, as well as the delivery of satellite communication services that meet the performance criteria, system robustness requirements, and service availability demands over Europe. This ambitious goal is achieved through a sophisticated network of satellites positioned in various orbital planes, including Medium Earth Orbit (MEO), Low Earth Orbit (LEO), and Geostationary Orbit (GEO), operating in cooperation to provide uninterrupted global connectivity. The initiative’s infrastructure is engineered to withstand existing challenges, such as good users experience, and high-quality of services even in the most remote regions. By maintaining a resilient infrastructure, IRIS² commits to upholding Europe's communication capabilities at the highest standard, facilitating seamless operations for governmental, commercial, and individual users, regardless of their location. IRIS² will also bolster the EU partnership policy by offering its infrastructure abroad.

Additionally, one of the primary strategic objectives of IRIS² is to provide satellite communications services that are not only secure but also resilient to the evolving

cybersecurity threat landscape. To achieve this high level of security, IRIS² will leverage the cutting-edge capabilities of quantum cryptography provided by the European Quantum Communication Infrastructure. Therefore, the EuroQCI is an integral part of IRIS² [58]. Also, the EuroQCI is part of the European Cybersecurity Strategy and is integrated into IRIS² [59].

The initiative's infrastructure's architecture will be built based on the principle of "security-by-design", ensuring that robust cybersecurity measures are implemented. Additionally, the IRIS² infrastructure will be designed and developed in line with the best practices and industry standards related to cybersecurity, and it will undergo comprehensive security accreditation to certify its robustness. In its commitment to bolstering resilience against cybersecurity related disruptive events, IRIS² plans to integrate the space-based and terrestrial components of EuroQCI, enabling the secure transmission of cryptographic keys. This integration is crucial for safeguarding communications against increasingly sophisticated cybersecurity attacks, thereby ensuring the integrity and confidentiality of data transmitted across the network.

EU asserts that through the establishment of a secure and reliable connectivity network, it will significantly enhance the security of its borders, empower critical infrastructures like smart grids, telemedicine, and institutional communications, and bolster support for crisis management and security operations. This initiative is designed to address the expansive digitization of the economy and society, as well as to counter the growing challenges posed by geopolitical tensions and cybersecurity threats. By ensuring a robust and pervasive communication infrastructure, EU aims to fortify its strategic capabilities in key areas, enabling a more resilient and responsive framework for both everyday operations and emergency situations.

Finally, EU envisions that beyond meeting its strategic and connectivity requirements, there lies a vast potential for commercial mass market ventures. The increasing demand for mobile and fixed broadband, along with cloud-based services, presents a plethora of emerging use cases. With the advent of EuroQCI, IRIS² is poised to extend its reach to the banking sector and other institutional entities that require quantum encryption for their data centers, including smart energy grids, hospitals, and government bodies, ensuring their security in an increasingly digital and interconnected landscape.

3.3 Core Capabilities

IRIS² initiative aims to provide its services to EU's institutions and agencies, such as indicatively the European Commission, European Parliament, Council of the European Union, and European Union Agency for Cybersecurity, ensuring the secure transmission of sensitive data, while also extending its services to EU's Member States to offer satellite communication services to national governments and their respective agencies, supporting public safety, emergency response, and critical infrastructure protection. Furthermore, IRIS² constellation aims to support civil protection and humanitarian aid operators, particularly in response to natural disasters, crises, and emergencies where terrestrial communication infrastructure is compromised. IRIS² also may be used for security and defense purposes, including border control, maritime surveillance, and military operations, ensuring secure communication links for EU Member States, supporting the respective agencies, teams, and users. However, apart from governmental and institutional users, IRIS² will also provide its services to commercial entities, particularly those involved in critical infrastructure and services that require high level of security and resilience.

A standard service model for IRIS² has been developed, including Hardgov Services, Lightgov Services, and Commercial Services, as already mentioned [Image 8].

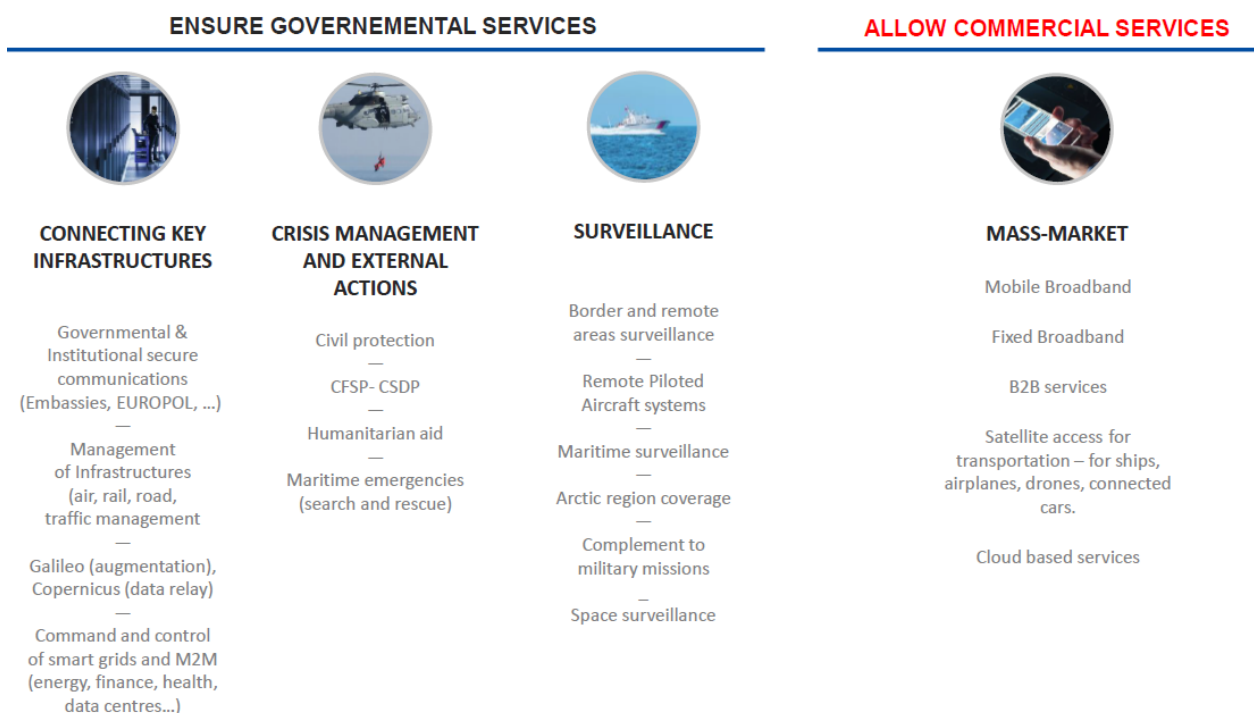


Image 8: EU IRIS² initiative's services [60]

Hardgov Services are restricted to government-authorized users and will be provided by the Governmental Infrastructure, mandating a high level of security for critical applications. Lightgov Services will also be provided to government-authorized users, but through the Shared Infrastructure and Commercial Infrastructure, providing assured worldwide low latency services and worldwide narrowband services, which are essential for seamless global operations, without requiring such strong security measures. Finally, the Commercial Services, leveraging the Shared and Commercial Infrastructure, will provide services to businesses, thereby facilitating a broad range of commercial activities. This service model ensures that IRIS² meets the diverse requirements of its users, from the most sensitive governmental operations to the dynamic needs of the commercial market [Figure 8] [60].

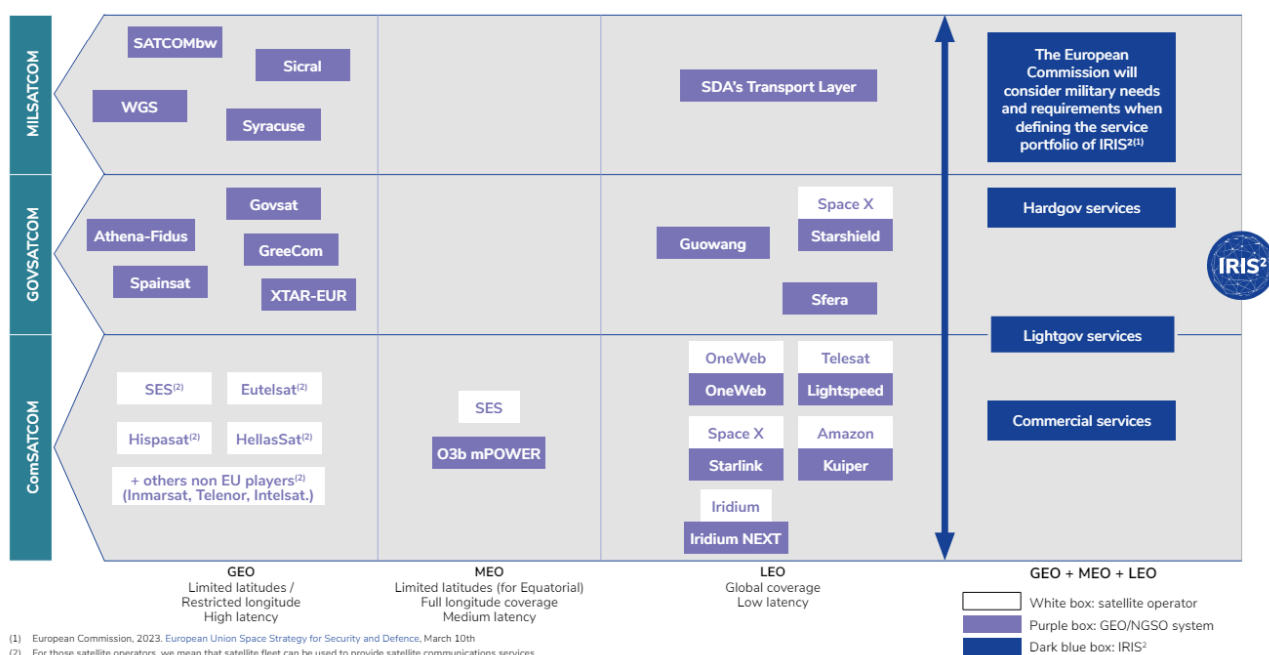


Figure 8: IRIS² SatCom market analysis [61]

Mainly, IRIS² focuses on government's demands, and delivery of governmental services. However, IRIS² applications will cover both governmental and commercial sectors' needs. Regarding surveillance, IRIS² constellation's capabilities will be pivotal in securing the land and maritime borders, offering real-time monitoring, and enabling rapid response to potential threats or illegal activities. This situational awareness is essential for protecting EU's external boundaries and supporting the work of agencies, such as European Border and Coast Guard Agency (Frontex). In crisis management, IRIS² will support the coordination of humanitarian efforts and delivery of aid during natural disasters, conflicts, or other emergencies. The constellation's ability to provide reliable and secure communication links, even when terrestrial networks are compromised, ensures that aid workers, civil protection teams, and first responders can operate effectively in the most challenging conditions. Moreover, the protection of key infrastructures is another area where IRIS² will have a significant impact. The constellation will support external actions by ensuring uninterrupted communication for civil protection operations, such as coordinating responses to maritime emergencies like oil spills or search and rescue missions at sea. Additionally, the secure and resilient connectivity offered by IRIS² will be critical for EU embassies around the world, enabling diplomatic missions to maintain confidential communications and safeguard sensitive information, regardless of the local infrastructure's reliability. By providing these capabilities, IRIS² will not only enhance the security and resilience of the European Union but also bolster its role as a global actor in providing aid and protecting international interests.

The commercial uses of IRIS² extend to providing business-to-business services through satellite trucking, offering satellite connectivity for transportation sectors, and delivering services based on cloud computing, all made possible by the advancement of global high-speed broadband and uninterrupted connectivity [62]. Regarding satellite trucking for B2B services, IRIS² can provide a mobile, on-demand communication infrastructure for media companies, event organizers, and remote construction sites, enabling live broadcasting, real-time data transfer, and efficient coordination of logistics. In the transportation sector, IRIS² can offer satellite access that can revolutionize the way vehicles, ships, and aircraft stay connected, as connectivity is crucial for real-time navigation, fleet management, and constant communication. Particularly, maritime industry can be benefited from enhanced communication for vessel tracking, weather updates, and emergency response. Furthermore, regarding cloud-based services, businesses can leverage satellite communication to access cloud computing resources, ensuring that data-intensive applications run smoothly without the limitations of terrestrial Internet infrastructure. By enabling these commercial applications, IRIS² not only contributes to the economic growth of the European Union but also supports the global digital economy. In time, Starlink and IRIS² might both serve comparable commercial sectors, like consumer broadband since commercial providers will have the opportunity to supply a portion of their capacity to the market.

The upcoming IRIS² services will incorporate the latest 5G non-terrestrial network standards and cutting-edge technologies, including optical intersatellite links, software-defined payloads, and quantum key distribution, to fulfill the specified operational requirements. Additionally, the system will benefit from the integration of advanced technologies from both established space industry veterans with reliable solutions and the transformative "New Space" sector, ensuring the system's scalability for future demands through a multi-orbital strategy. While the specific technologies that will be employed to secure IRIS² services are confidential, the European Commission

emphasizes that the adoption of the most recent advancements in satellite communications and cybersecurity is crucial for the success of this project.

Summarizing, by enabling these capabilities, IRIS² initiative's commitment to providing secure, resilient, and high-speed connectivity is proven, positioning it as a key enabler of the next generation of business services and a driver of competitive advantage in the international market.

3.4 Operational Requirements

In order IRIS² to be able to achieve its strategic objectives, as well as provide its core capabilities should ensure the fulfillment of its operational requirements. The current section defines the primary operational requirements of IRIS² which play an integral role for its proper functionality, ensuring the provision of secure, and resilient satellite communication services.

Firstly, IRIS² ambassadors should be mentioned, as these will play a crucial role in the initiative's adoption, especially as the initiative approaches its operational phase [63]. Tasked with advocacy and outreach, IRIS² ambassadors should actively engage with stakeholders across Europe and the whole world to raise awareness about the constellation's capabilities and benefits. More specifically, they should facilitate workshops, seminars, and conferences to educate potential users on how IRIS² can support their communication needs in various scenarios, including crisis management, defense operations, and critical infrastructure maintenance. By highlighting the constellation's advanced features, such as enhanced encryption and anti-jamming technologies, ambassadors should underscore IRIS² contribution to secure and uninterrupted connectivity. Their efforts are instrumental in fostering partnerships, and reinforcing the strategic importance of IRIS², as well as extending its benefits to neighboring regions.

From a governance perspective, the Commission intends to delegate the oversight of the IRIS² initiative's development and validation activities to ESA, which will then award partnership project contracts to entities selected by Commission. Concurrently, EUSPA is managing the procurement of GovSatCom Hub infrastructure, which will serve as the operational interface connecting GovSatCom Hub to Hardgov and Lightgov services, integrating satellite communication capabilities and services from the Contractor, commercial providers, and national operators. Overall, effective oversight, monitoring, and project management are essential for successful implementation of such a complex and critical initiative [Image 9]. Finally, the Security Accreditation Board established within the Agency shall be the security accreditation authority for the governmental infrastructure of the Programme. EUSPA is also responsible for accrediting the security of all EU Space Programme components.

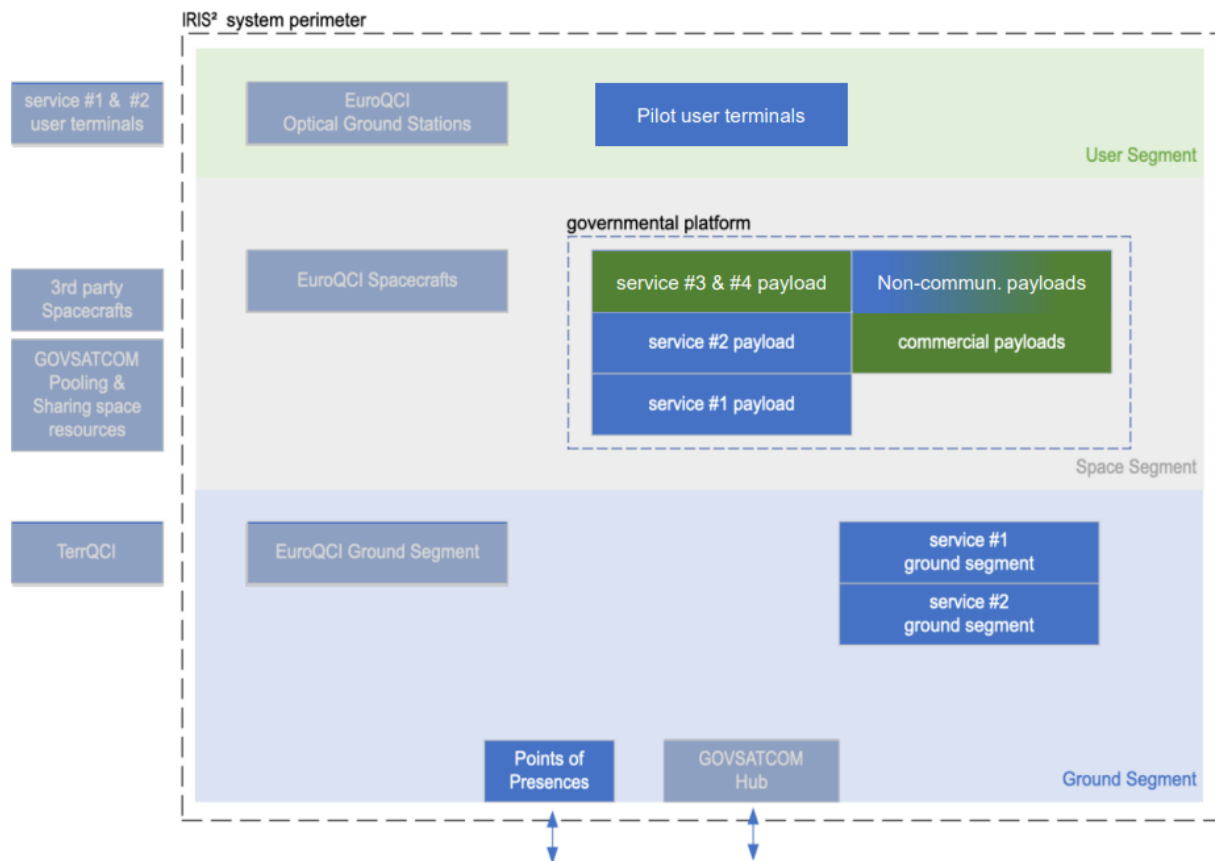


Image 9: Infrastructure and ownership of IRIS² [48]

On the other hand, from an operational perspective, IRIS² initiative will constitute of two (2) segments, the space, and terrestrial segment to operate effectively and efficiently. The space segment will include the constellation's satellites that will operate from GEO, MEO, and LEO orbital positions, while the terrestrial segment will be divided into the Governmental Infrastructure, Common Ground (Shared) Infrastructure, as well as Commercial Infrastructure. More specifically, the Governmental Infrastructure will include the GovSatCom Hubs that will provide satellite communication services to governmental users, which are the Hardgov Services, as well as the Security Monitoring Center that will perform security monitoring activities to ensure the preservation of high level of security. The Governmental Infrastructure will be EU-owned and EU-operated. Furthermore, Governmental Infrastructure's sites will include the Control, Mission, and Service Centers, that are mandated to be located and operated within the EU, the Tracking, Telemetry, and Command (TT&C) ground stations, as well as the Gateways, that both should be established and operated within the EU, and specifically in EU's Outermost Regions and Overseas Countries and Territories, only if it is required. Additionally, the Common Ground (Shared) Infrastructure will be responsible for efficient operation of the constellation, while the Commercial Infrastructure will provide satellite communication services to commercial users, which are the Lightgov and Commercial Services. The Commercial Infrastructure will be privately financed and commercially operated [Image 10] [60].

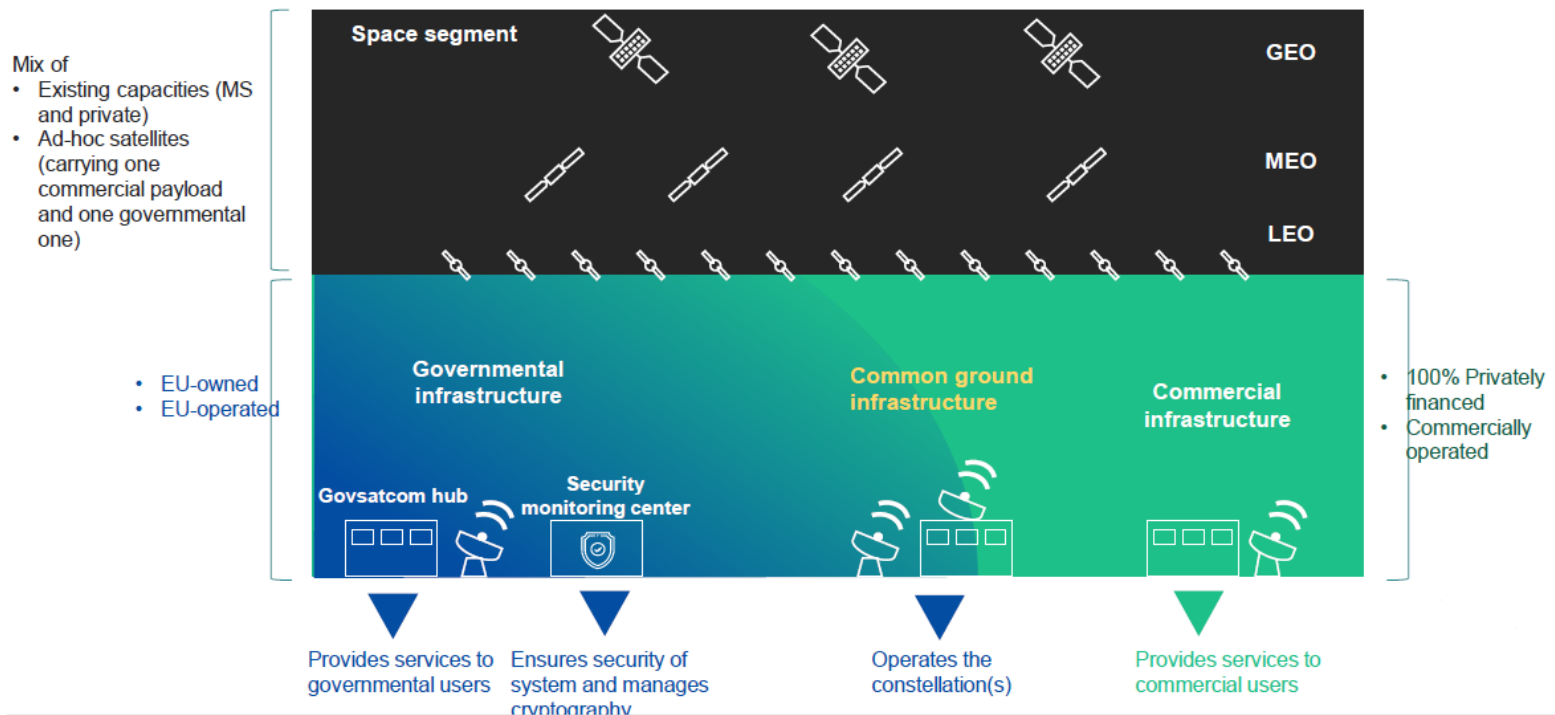


Image 10: Infrastructure of IRIS² [60]

Furthermore, the IRIS² user terminals shall be designed to be open and not based on proprietary solutions, thereby fostering interoperability at both the user and infrastructure levels to the greatest extent feasible. This approach supports the European Union's commitments to international cooperation. To align with global telecommunications advancements, it is planned to be implemented 5G Non-Terrestrial Network (NTN) standards, as defined by the 3rd Generation Partnership Project (3GPP), adopting a gradual approach to integration. Additionally, a range of pilot users' terminals with varying characteristics, such as fixed, on-the-move, and nomadic will be developed to test their functionality and define which of them best meets the end users' needs and requirements. Additionally, to ensure security of users' terminals, endpoint security, terminal authentication, monitoring, and management solutions should be implemented. A test utilizing a generic platform with hardware and software resources is planned to be performed, testing the implemented security solutions, such as device identification and authentication, remote attestation and monitoring for intrusion detection, as well as remote management for secure provisioning and decommissioning, to identify the effectiveness of the endpoint security capabilities [64].

Keeping pace in the global technological race is a universal priority. Therefore, apart from users' terminals security, the security of communication networks is also essential. In this context, Quantum Key Distribution will play a pivotal role in IRIS² initiative, as already mentioned. The European Commission to be proactive in this area, has commissioned a consortium called "Nostradamus", with a budget of some million euros, dedicated to establishing a QKD test infrastructure, enabling the evaluation of European manufacturers' QKD devices. This consortium is led by Deutsche Telekom, with collaboration from Thales, the Austrian Institute of Technology, and other partners across industry and academia. This paves the way for the implementation of EuroQCI, which will be a highly secure pan-European communication network based on quantum technology. The governments of all EU Member States and their citizens will be benefited from ultra secure critical infrastructure and satellite communication services [65].

Also, the mission design for IRIS² should incorporate a multi-faceted approach to sustainability and debris mitigation, ensuring the long-term viability of space activities.

This includes employing advanced techniques for intra-constellation collision avoidance to prevent satellites within the same network from colliding, for prevention of in-orbit collisions with external objects, such as space debris or satellites from other constellations, as well as for prevention of inter-constellation collision avoidance, maintaining safe distances between satellites from different networks. Additionally, to address end-of-life protocols, IRIS² should implement controlled and safe re-entry procedures to ensure that decommissioned satellites do not pose a risk to Earth or other space assets. This could involve deorbiting maneuvers to guide satellites back into the Earth's atmosphere, where they would burn up safely. Alternatively, the disposal of satellites could be conducted using designated "graveyard" orbits for deorbiting [48].

Additionally, IRIS² design should cater for minimization of disruptive visual brightness caused by satellites, which can affect astronomical observations. Techniques, such as anti-reflective coatings or adjusting satellite orientations, could be used to reduce this impact. Furthermore, IRIS² should aim to minimize the greenhouse gas emissions throughout its lifecycle, from manufacturing to launch and operation. This could involve using eco-friendly materials, optimizing launch vehicle efficiency, or selecting low-emission ground operations. To offset any unavoidable emissions, investment should be performed in greenhouse gas offsets, such as funding renewable energy projects or reforestation initiatives. Lastly, by registering with the European Union Space Surveillance and Tracking (EUSST) services, IRIS² will have access to crucial information on space debris and other hazards, enabling it to operate more safely and sustainably within the increasingly crowded space environment [48].

Summarizing, the main operational requirements of IRIS² are its ambassadors, the coordination activities of ESA, the established infrastructures, the interoperability of end users' terminals, the implemented security controls for protection of users' terminals and communications' networks, as well as the integrated techniques for debris mitigation, collision avoidance, satellites' disposal, minimization of disruptive visual brightness, and greenhouse gas emissions minimization.

3.5 Limitations and Challenges

Having analyzed the vision, strategic objectives, as well as the main capabilities of IRIS², that include but are not limited to the provision of secure and resilient satellite communications, it should also be defined the limitations and challenges of this initiative. These challenges, ranging from governance to technical constraints, that will be analyzed to the current section, necessitate good understanding to take advantage of the full potential of IRIS² capabilities. Through an in-depth analysis of these challenges, this study aims to provide valuable insights into optimizing IRIS² capabilities and maximizing its benefits.

The first challenge is the effective governance of IRIS² initiative, and more specifically the coordination among various involved stakeholders, to ensure proper collaboration across diverse parties responsible for managing the initiative's execution. Achieving effective governance demands a balance between organizational consistency and the acknowledgment of differing viewpoints and objectives of Member States and other involved parties. In this context, another issue is the stakeholders' collaboration to define user and mission requirements, considering the users' needs, cost-effectiveness, timelines, as well as broader European goals and objectives. Beyond the difficulties of stakeholders' collaboration, another governance related challenge pertains to the proper allocation of risk ownership. The intricate nature of satellite communication projects demands careful evaluation of how to allocate the management of both financial and security risks among involved stakeholders.

Additionally, as the evolving satellite connectivity market by the deployment of large constellations offering global Internet access has introduced a new era of commercialization in space, inherent risks and challenges have been also emerged. This expansion bridges the digital divide but also raises significant legal challenges, that also applies to IRIS². The shift towards self-regulation by private entities endangers the safety, security, and sustainability of space orbits. The European Commission's efforts to integrate both large and small businesses into the IRIS² program reflect lessons learned from Galileo and Copernicus initiatives, emphasizing the need for a balanced public-private investment approach, particularly in high-risk and capital-intensive space ventures. The inclusion of small businesses and the involvement of small satellites and emerging companies underscore the necessity for a dynamic and inclusive space industry.

However, the current legal landscape, governed by the Outer Space Treaty (OST), is confronted with pressing legal challenges that demand a coordinated international response. These challenges include the licensing and registration of an increasing number of space objects for effective tracking and transparency, the allocation of frequencies to prevent interference and ensure reliable satellite communication, as well as the establishment of robust space traffic management and debris mitigation strategies to maintain the orderly use of near-Earth orbits. Proper registration not only facilitates object identification and tracking but also promotes accountability in space operations. In the absence of adherence to registration protocols, attributing liability in the event of collisions becomes a complex and contentious issue, complicating the resolution of damages and reinforcing the critical need for a comprehensive legal framework to govern the evolving space environment [66].

An additional challenge and/or limitation impeding IRIS² is from a financial perspective, stemming from the potential shortfall in investment from both Member States and private sector. This financial uncertainty poses a considerable risk to the initiative's success. In this context, the procurement process plays a pivotal role, as it directly impacts the budget necessary to achieve the initiative's goals, requiring a careful balance between emerging needs and available financial resources. The intricate nature of financial risk requires strategic planning, adoption of a forward-thinking approach to financial risk management that includes comprehensive contingency measures and wise allocation of resources. The repercussions of financial risk have the potential to affect the long-term viability and efficiency of IRIS². To confront this financial challenge, it is essential to establish a financial planning framework that is marked by active involvement of stakeholders, informed decision-making, and thorough cost-benefit analysis.

Furthermore, among complexities of IRIS² initiative's implementation, there is a significant challenge related to the timeline of initiative's execution. The success of IRIS² depends not only on the efficacy of its strategic vision and technological prowess but also on the timely execution of its implementation roadmap, that is already delayed. The realization of timeline risk can disrupt the carefully designed sequence of activities and jeopardize the window of opportunity within which the initiative operates. Any delay in implementation not only undermines the initiative's momentum but also causes a domino effect of cascading impacts, potentially leading to cost overruns, resource misallocation, and diminished operational effectiveness. Therefore, there is the need for adoption of proactive strategies that prioritize adherence to strict timelines without compromising on quality or operational integrity. To efficiently mitigate the timeline risk, proper planning, robust project management, and agile decision-making are required.

Finally, as part of the IRIS²'s initiative's forward-looking agenda, a notable challenge emerges from the technological domain. IRIS² commitment to leveraging advanced

technological solutions necessitates continuous validation of them, a process that is both dynamic and complex. The integration of the latest technological innovations brings inherent challenges and unpredictability, and requires demanding monitoring, as well as continuous oversight and testing to ensure that they operate as designed and desired and do not introduce any security and/or operational risks. A critical aspect of these technological complexities is the imperative to establish strong cybersecurity protocols to protect vital satellite communication systems from the constantly changing and evolving cybersecurity threats landscape.

In conclusion, the successful implementation of the IRIS² initiative not only represents a significant milestone in advancing European Union's strategic objectives but also has the potential to elevate EU as a prominent global player in satellite communications domain. However, the realization of these objectives requires effective management of existing challenges, ranging from technological complexities to cybersecurity concerns.

3.6 Implementation Reasons

3.6.1 Technological Advancement and Innovation

Taking into consideration the capabilities, limitations, and challenges of IRIS² initiative there are various reasons that support its implementation need, the most critical of which will be analyzed in detail to the current section. In an era where technological innovation is the cornerstone of progress, initiatives like IRIS² are promising to drive innovation and shape the future landscape of secure and resilient communication technology, leveraging satellite capabilities.

As a catalyst for innovation, IRIS² can support experimental communication technologies, such as quantum key distribution (QKD) for satellites, which promises to revolutionize secure communication. More specifically, QKD harnesses the principles of quantum mechanics to create cryptographic keys that are theoretically immune to interception or duplication. This technology has the potential to transform the landscape of secure communication, offering a level of encryption that is impervious to the threats posed by quantum computing and other advanced decryption methods. Researchers and developers can through IRIS² infrastructure conduct extensive testing and validation of QKD systems in the unique environment of space, trying also to overcome the challenges of implementing QKD in space, such as maintaining the integrity of quantum states over long distances and through the Earth's atmosphere. For example, IRIS² can facilitate experiments that test the transmission of entangled photons between a satellite and a ground station. By analyzing the rate of successful key exchanges and the fidelity of the quantum states, researchers can refine the technology to ensure its robustness and reliability. By providing a testing ground for such advanced concepts, IRIS² not only accelerates their development but also demonstrates their practical application.

In the same context, IRIS² can make a significant impact in the development and testing of advanced satellite propulsion systems. These innovative propulsion systems aim to be more efficient, using less fuel and thereby reducing the cost and environmental impact of satellite launches. For example, IRIS² can facilitate the testing of electric propulsion systems, which offer a more sustainable alternative to traditional chemical rockets by providing a longer operational lifespan for satellites while minimizing the release of harmful substances into the atmosphere. Moreover, IRIS² can support the testing of technologies designed for active debris removal. These technologies enable satellites to adjust their orbits to avoid collisions with debris or to deorbit defunct satellites safely. By doing so, IRIS² helps preserve the space environment for future generations of space exploration and satellite deployment. Furthermore, IRIS² can assist in the testing of

advanced radar systems for satellites that improve the accuracy and resolution of topographical mapping. Such systems can monitor glacial movements, sea-level rise, and changes in land use, contributing to our understanding of climate dynamics and the impact of human activities on the planet. Through its support of cutting-edge research and development, IRIS² helps to shape the future of satellite technology and its role in addressing some of the most pressing challenges of our times.

Furthermore, IRIS²'s secure communication channels can be a linchpin for the evolution of advanced cybersecurity technologies. These channels provide an isolated and controlled environment that is crucial for rigorous testing and development of cybersecurity solutions without the inherent risks of exposure associated with the public Internet. Security firms can leverage IRIS²'s satellite network to conduct penetration testing and vulnerability assessments on new software and hardware solutions. This enables them to simulate cybersecurity attacks in a contained setting, allowing for the identification and remediation of security flaws before they are deployed in real-world scenarios. For instance, a company developing a new encryption protocol could use IRIS² to test its resilience against quantum decryption techniques, ensuring that the protocol can withstand future threats.

Additionally, IRIS²'s secure channels are invaluable for the development of communication tools tailored for sensitive government and military applications. These tools require the highest levels of security to protect classified information from interception or tampering. By using IRIS², developers can test secure messaging systems, voice encryption protocols, and secure video conferencing tools under the stringent conditions they will encounter in the field. The satellite network's inherent resistance to traditional network-based attacks provides an additional layer of security during the development and testing phases. By providing a secure and robust platform for the development and deployment of cutting-edge cybersecurity technologies, IRIS² plays a critical role in enhancing the security posture of both private and public sectors. Therefore, its contribution to national and international security is significant, as it enables the creation of tools and systems that protect against the evolving landscape of cybersecurity threats.

IRIS² initiative, also, fosters technological advancement and innovation, as it encourages the deployment of innovative and competitive technologies by leveraging the "New Space" industry, under both the development and operation of the secure connectivity systems, supporting overall the advancement of the EU space sector. More specifically, IRIS² initiative will deliver significant advancements to European economy, as a key goal of is to actively involve private sector participants, especially those within the burgeoning "New Space" sector, to drive innovation. Today, these entities have a more straightforward path to participation in the initiative compared to earlier times, such as when Galileo and Copernicus were initiated, due to the mature commercial market and the established culture of public-private partnerships. Satellite operators are already developing and serving a connectivity market that is forecast to double between 2020 and 2030.

Additionally, IRIS² can leverage the European space industry's renowned expertise and global reputation in the field of telecommunications, harnessing the collective knowledge of seasoned industry giants, including manufacturers, technology providers, and service operators. In a groundbreaking move for such initiatives, IRIS²'s operational program is designed to dedicate EU-funded components to start-ups and Small and Medium-sized Enterprises (SMEs). Therefore, IRIS² sets out specific support for the participation of SMEs, as well as of women innovators achieving equality and inclusion goals.

In conclusion, IRIS²'s impact on technological advancement and innovation is profound, offering a resilient, secure, and versatile platform that not only underpins current technological progress but also inspires and enables the next wave of innovations. With its global reach and commitment to security and connectivity, IRIS² is shaping a future where technological boundaries are constantly expanded, and innovation is a collaborative, inclusive, and continuous journey.

3.6.2 Global Connectivity

Overall, IRIS² is an initiative designed to deliver global connectivity, transcending the limitations of terrestrial networks, and ensuring that high-speed broadband access reaches every corner of the globe. The integration of GovSatCom within IRIS² is a testament to the European Union's commitment to achieving this ambitious goal, aiming to provide seamless connectivity not only throughout the EU but also in critical regions beyond, such as the Arctic and Africa.

The strategic deployment of multi-orbital satellite constellation enables IRIS² to be benefited from the advantages offered from LEO, GEO, and MEO, and provide global connectivity. Specifically, LEO satellites, orbiting at altitudes ranging from 500 to 2,000 kilometers, can offer low-latency communication, making them ideal for time-sensitive data transmission and real-time applications. Their proximity to Earth's surface allows for rapid data exchange, which is essential for applications, such as financial trading, emergency response, and remote control of critical infrastructure. GEO satellites, stationed at approximately 35,786 kilometers above the equator, can provide a stable and persistent line of sight to specific geographic areas, making them well-suited for broadcasting and content delivery services, as well as for maintaining continuous communication links for strategic locations. Their high-altitude vantage point ensures wide coverage areas, enabling a single satellite to serve vast regions. And lastly, MEO satellites, orbiting at altitudes between LEO and GEO, strike a balance between coverage and latency. They can be used for navigation systems like GPS, as their intermediate position allows for precise signal triangulation and reliable coverage. MEO satellites are also beneficial for mobile communications, providing connectivity to aircraft, ships, and vehicles on the move.

Moreover, the deployment of IRIS² is crucial as it promises to deliver high-speed broadband and seamless connectivity across the EU, ensuring sustained global access, including in non-European regions like the Arctic and Africa. It will provide uninterrupted, secure, and cost-efficient satellite communication services, eliminating communication dead zones and facilitating connectivity across strategically important geographical areas. The secure connectivity system's design, with its modular architecture, and the model for implementation and asset ownership (both in space and on the ground) comprise a governmental component within the EU, which will own all tangible and intangible assets of the governmental infrastructure, alongside a supplementary commercial segment. IRIS² is set to enhance the resilience of EU communication services by leveraging a variety of space communication resources.

Beyond aiding governments, IRIS² is set to offer services that facilitate the everyday tasks of individuals in Europe and beyond. The initiative aims to deliver crucial communication services in regions lacking stable terrestrial networks. By providing a secure and robust combination of space and terrestrial systems, IRIS² will eradicate communication "dead zones" across Europe, Africa, and the Arctic, ensuring fast broadband and uninterrupted connectivity. Consequently, IRIS² will propel economic and societal advancement within the EU and promote social unity by contributing to the narrowing of the digital divide.

More specifically, in the Arctic region, the formidable environment presents unique challenges for establishing reliable communication infrastructure. The region's extreme weather conditions, with prolonged periods of darkness and sub-zero temperatures, coupled with its sparse population, have historically impeded the development of ground-based networks. However, IRIS² is a game-changer for this region, offering a robust solution that can withstand the Arctic's harsh conditions. Similarly, IRIS² aims to enable connectivity across the African continent, particularly in rural and remote areas where traditional infrastructure is lacking. Particularly, the African Union stands as one of the most esteemed collaborators in the realm of space, owing to the enduring partnership between Africa and the EU. Through the Global Monitoring for Environment and Security and Africa (GMES & Africa) initiative, the EU and AU work together in the field of Earth observation. Meanwhile, satellite navigation forms the core of the collaboration under the EU-ASECNA Agreement and is further emphasized by the Joint Programme Office for Satellite Navigation in Africa (JPO) [67].

By providing satellite-based Internet access, IRIS² will connect these regions to the global network, unlocking untapped potential and fostering socio-economic development. The implications of this connectivity are far-reaching, indicatively for the scientific community, IRIS² will enable a continuous stream of data from research stations, facilitating groundbreaking research on climate change and arctic ecosystems. Maritime operations will also be benefited significantly from IRIS², as Arctic Sea ice recedes, new shipping lanes are emerging, necessitating reliable navigation and communication systems. Finally, healthcare delivery will be transformed as well, as satellite connectivity will facilitate telehealth services, connecting patients in remote areas with medical professionals around the world.

In conclusion, the IRIS² initiative represents a significant stride towards universal connectivity, adaptable to the diverse needs of the EU and its global partners, by leveraging the combined strengths of LEO, GEO, and MEO satellites. Furthermore, by providing reliable, high-speed broadband access, IRIS² will not only close the digital gap, but also foster a more connected and equitable global community.

3.6.3 Secure Satellite Communications

As we progress into the digital age, the dependence on connectivity for individuals, businesses, and governmental entities has been increased. This connectivity is the backbone of critical systems, such as energy networks and financial services, which rely on digital networks for operation and control. The current trend of hyper-connectivity means that any interruption in these services can have widespread and significant impacts. Reliable, secure, and resilient connectivity is therefore vital to maintain the integrity of global security and economic systems. It is particularly crucial in countering rising cybersecurity threats and ensuring effective communication during emergencies, especially when conventional communication infrastructures are compromised. In response to these challenges, the European Union has embarked on an ambitious initiative to create IRIS², the new space-based system designed to provide secure and resilient connectivity [68].

As cybersecurity is a paramount concern across all sectors and industries in general, the protection of space and ground segment infrastructures, along with the security of governmental communication services, is also of utmost importance. Considering this, the implementation of IRIS² initiative is essential, as it is specifically designed to ensure cyber resilience and operational security. This is achieved through integration of the European Quantum Communication Infrastructure (EuroQCI) initiative, which applies cutting-edge quantum technology to both space and ground segments. By incorporating

Quantum Key Distribution methods, IRIS² aims to create an ultra-secure communications network that is virtually immune to cybersecurity threats, thereby significantly enhancing the security level of data transmission. The incorporation of such advanced technologies not only establishes a secure communications backbone for government and critical national infrastructure, but also elevates the trust of users in the system's integrity. With examples like safeguarding sensitive government communications and protecting the exchange of critical financial data, IRIS² role in ensuring secure and reliable communication channels becomes indispensable in today's interconnected world.

Additionally, in response to the current geopolitical context, there is a pressing need for the European Union and its Member States to significantly upgrade their satellite communication systems in terms of both capacity and quality. The complex threat landscape, encompassing cyberattacks to more subtle hybrid warfare tactics, demands advanced security measures, lower communication delays, and greater data throughput. In this context, the implementation of IRIS² stands as a strategic initiative to affirm European appropriate level of strategic technical autonomy and digital sovereignty, providing a secure and dependable communication network. This network is crucial for government agencies tasked with the protection of vital infrastructure, monitoring of sensitive areas, execution of foreign policy missions, as well as the coordination of responses during emergencies.

More specifically, IRIS² infrastructure is designed to offer ultra-secure connectivity, which is essential for defense and security operations that require rapid and protected communication links. The system's enhanced capabilities will also support other high-priority applications, such as real-time data exchange for disaster response teams, secure transmission of sensitive information between diplomatic entities, and reliable communication for deployed military forces. The incorporation of state-of-the-art encryption and anti-jamming technologies will ensure that communications remain confidential and uninterrupted, even in contested environments. Therefore, by leveraging IRIS², Europe aims to achieve a new, higher level of operational resilience and maintain its sovereignty in the increasingly contested domain of space-based communications.

3.6.4 Resilient Satellite Communications

In an era characterized by evolving security threats, the establishment of reliable and resilient communication infrastructures is paramount for governments worldwide. In this context, the architectural design and deployment of IRIS² initiative has taken into consideration the operational resilience related requirements, to establish a robust and resilient satellite communications network. Therefore, IRIS² initiative emerges as a strategic solution aiming to foster the resilience of satellite communications.

Satellite-based infrastructures have become indispensable for modern governments; however, they face distinct vulnerabilities spanning from cybersecurity to physical security threats and disruptions. In response to these challenges, the IRIS² aims to fortify the resilience of governmental satellite communications networks. This initiative has the objective to safeguard vital communication channels, ensure uninterrupted operations, and uphold national sovereignty. Resilient satellite communications, as envisaged by IRIS², are paramount for ensuring the continuity of essential services, especially during crises or conflicts. By targeting the mitigation of risks associated with single points of failure and bolstering network survivability, IRIS² enhances situational awareness, and facilitates effective emergency response coordination. Ultimately, this initiative not only strengthens national security but also safeguards the well-being of citizens by ensuring the reliability of critical communication infrastructures.

Resilient satellite communications, as supported by IRIS² initiative, serve as a linchpin for fostering interoperability among EU Member States, thereby facilitating seamless collaboration across a spectrum of activities including joint military exercises, and humanitarian aid operations. By implementing standardized protocols and establishing secure communication channels, the initiative not only fosters cohesion among diverse stakeholders but also enhances the speed and efficiency of cross-border cooperation during crisis situations. In the context of joint military operations, for instance, interoperable satellite communication systems enable real-time sharing of information, synchronized command structures, and coordinated logistics, thereby amplifying the collective defense capabilities of participating nations and reinforcing regional stability. Similarly, in humanitarian and disaster relief endeavors, resilient satellite communications enable rapid response coordination, situational awareness, and resource allocation, expediting life-saving interventions and minimizing the impact of natural or man-made disasters. This interoperable communication infrastructure, underpinned by IRIS² initiative, not only strengthens the resilience of satellite networks but also nurtures a culture of collaborative security and crisis management across the European Union.

In conclusion, IRIS² initiative represents a pivotal step towards ensuring the resilience and security of governmental satellite communications in Europe. By harnessing state-of-the-art technologies and fostering collaboration among EU Member States, the initiative offers a comprehensive solution to address emerging threats and challenges in the space domain. Through its focus on resilience, interoperability, and appropriate level of strategic autonomy, the IRIS² initiative reaffirms Europe's commitment to safeguarding its critical infrastructure, protecting its citizens, and promoting international cooperation in the realm of satellite communications.

Overall, considering the advantages of IRIS² in the context of technological advancement and fostering of innovation, global connectivity, as well as enablement of secure and resilient satellite communications, the implementation of this initiative is a necessity to address the challenges derived from the current emerging and evolving operational and threat landscape.

4. EUROQCI INITIATIVE: A PART OF THE EUROPEAN CYBERSECURITY STRATEGY AND A QUANTUM LEAP TOWARDS SECURE COMMUNICATION INFRASTRUCTURE

4.1 The European Cybersecurity Strategy and the European Quantum Communications Infrastructure (EuroQCI)

The efficacy and security of current encryption technologies rely on assumptions about computational complexity. However, with the rapid advancement of computing capabilities and the emergence of increasingly sophisticated threats and attacks, the security of telecommunications and data networks can be potentially breached. As a result, Europe's communication infrastructure is at risk, jeopardizing the confidentiality of transmitted sensitive data. To address these concerns, the Commission, in collaboration with Member States and the European Space Agency, works on the design, development, and deployment of a secure Quantum Communication Infrastructure (QCI) across the EU and its overseas territories, contributing also to meeting the security requirements of the GovSatCom initiative.

In October 2018, the European Commission initiated the first (1st) phase of the Quantum Technologies Flagship, which is a €1 billion, ten-year initiative pooling resources around a commonly agreed technology and science roadmap of activities [69]. A few months later, on 13th of June 2019 at the Digital Assembly, seven (7) Member States signed the European Quantum Communication Infrastructure (EuroQCI) Declaration, while at the end of 2019, Greece signed the Declaration as well, agreeing to collaborate with the Commission and ESA, towards the development of a quantum communication infrastructure for the whole EU, including space and ground infrastructure, integrated into the governmental infrastructure to boost European capabilities in quantum technologies, cybersecurity, and industrial competitiveness. In accordance with the Declaration, EuroQCI has the objective to establish a certified secure end-to-end quantum communication infrastructure facilitating the transmission and storage of sensitive and classified information, as well as the linking of communication assets all over the EU [69]. In response to this commitment, HellasQCI is an EU funded project that intends to build the National QCI of Greece. GRNET has been appointed by the Ministry of Digital Governance as the responsible entity for coordinating the national EuroQCI related proposals [70], [71].

A few years later, on 28th of July 2021, Ireland also signed the EuroQCI Declaration, while gradually all twenty-seven (27) EU Member States signed it. In the period 2021-2027, quantum technologies will be supported by the Digital Europe Program, which will reinforce Europe's strategic digital capacities, as well as by the Commission's Horizon Europe Program, contributing to research on space applications. More specifically, on 10th of November 2021, the Commission approved three (3) work programs for the Digital Europe Program, receiving a funding of €1.98 billion in total. These initial work programs encompass strategic investments crucial for achieving the Commission's vision of transforming this decade into Europe's Digital Decade.

The Digital Europe Program aims to enhance Europe's appropriate level of technological autonomy and facilitate the execution of digital innovations to benefit citizens, public institutions, and enterprises. Several days afterward, on November 17, 2021, the Commission announced the initial set of calls for proposals as part of the Digital Europe Program. Subsequently, on December 16, 2021, the Commission adopted the first Work Program for the digital segment of the Connecting Europe Facility (CEF Digital). This program outlines the scope and objectives of actions supported by the EU, intended to

enhance the digital connectivity infrastructure across Europe over a three-year period. It focuses on fostering cross-border connections among national networks and establishing links with the space component of the EuroQCI.

On 12th of January 2022 the Commission launched the first calls for proposals under the digital part of the Connecting Europe Facility (CEF Digital) program, while on 26th of January 2022, the Commission published the architecture for its proposed satellite broadband constellation. The initial phase of EuroQCI's implementation, funded under the European Commission's Digital Europe Program, started in January 2023. This phase primarily concentrates on a series of industrial projects aiming at advancing the main technological components of EuroQCI, as well as national projects enabling Member States to create and enhance their respective quantum communication networks, which will serve as the foundation for the terrestrial segment.

These projects involve various technologies and protocols, customizing them to meet the specific requirements of each country [72]. Furthermore, these projects aim to make it possible to take the first steps towards offering services utilizing quantum key distribution (QKD), which is a highly secure way of delivering encryption keys. In addition, with the support of the Digital Europe Program, a testing and evaluation infrastructure will be built that will enable QKD-based technologies and services to be assessed and validated, so that users can be confident that they will not be vulnerable to attacks.

The primary objective of the EuroQCI is to bolster the security of critical data and infrastructure by incorporating quantum technology into existing communication networks. This incorporation will provide an added layer of security and a quantum physics-based measure, striving to fortify the defenses of government bodies, data repositories, medical institutions, power grids, and other key elements of essential industries. It is also poised to become a cornerstone of the European Union's Cybersecurity Strategy for the foreseeable future.

The European Cybersecurity Strategy aims to ensure resilience to cybersecurity threats, as well as to ensure that both citizens and businesses benefit from trustworthy digital technologies. The strategy is about harnessing and strengthening all EU tools and resources to be technologically sovereign [73]. Also, the European Cybersecurity Strategy aims to build resilience to cybersecurity threats for its Common Security and Defense Policy (CSDP) [74].

In 2013, the European Union initiated the development of its first comprehensive strategy for cybersecurity⁵. This move came during an era referred to as the 'cyber awakening' between 2012 and 2013, a time when many leading global economies, including the EU, became sharply conscious of the significant repercussions that cybersecurity issues posed to their national security and economic stability. Meanwhile, the EU's approach came somewhat later than NATO's, which had already established its first cyber-defense strategy in 2008 and implemented a subsequent policy by 2011. However, NATO's cyber-

⁵ The European Parliament, "P7_TA (2013)0376 EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace. European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606 (RSP))," Official Journal of the European Union, 12 September 2013.

policy efforts were mainly concentrated on safeguarding its own communication and information systems⁶.

Although the EU's cybersecurity strategy emerged after NATO's, it was more expansive in its scope [Figure 9]. During its formulation in 2012-2013, the EU's strategy encompassed all significant domains under its jurisdiction, resulting in a wide-ranging, government-wide cyber policy. This all-inclusive strategy set the EU's approach to cybersecurity apart from NATO's.

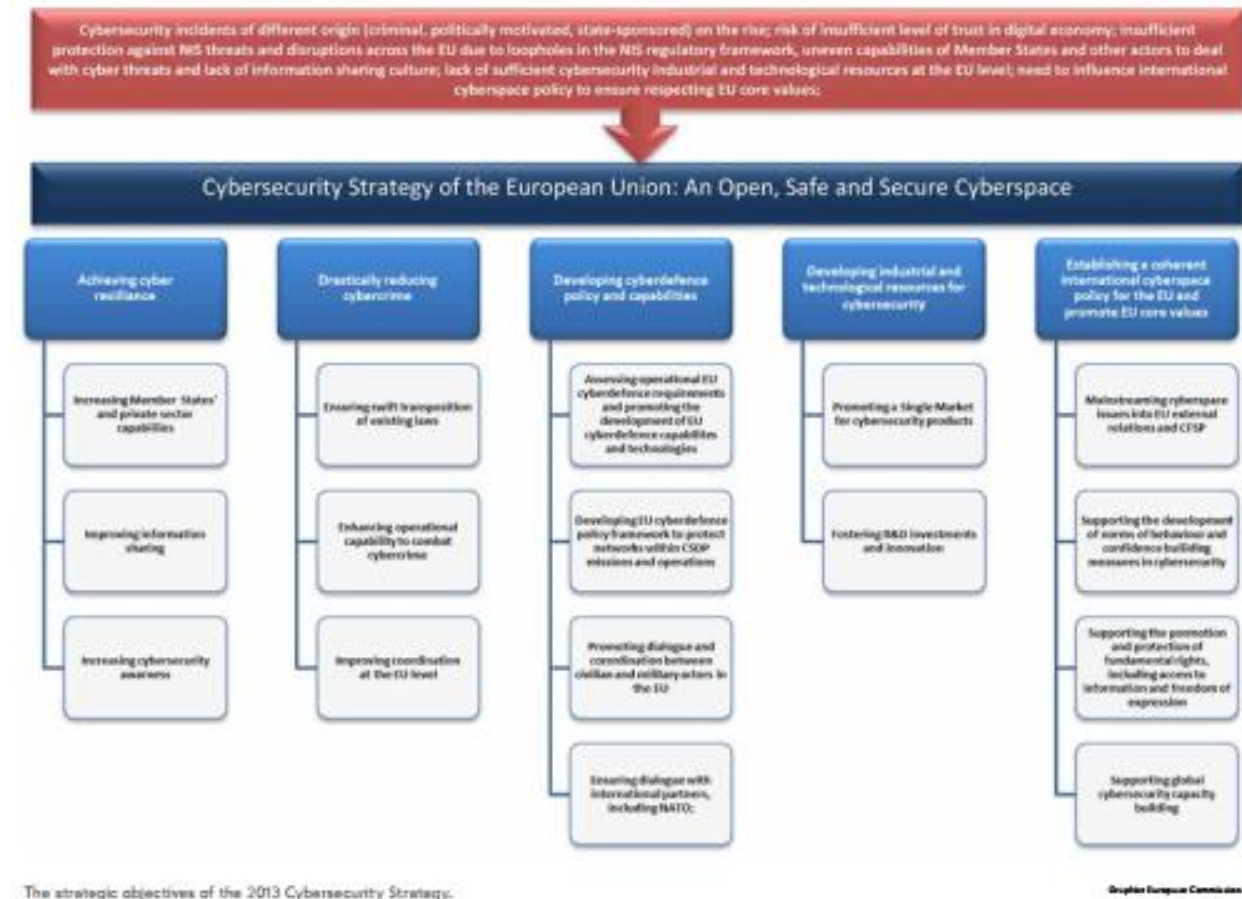


Figure 9: Strategic objectives of 2013 Cybersecurity Strategy [75]

The 2013 cybersecurity strategy was accompanied by a legislative initiative from the Commission, which led to the creation of the Network and Information Security (NIS) Directive. The execution of the 2013 Cybersecurity Strategy involved a joint effort across different departments. Directorate-General for Communications Networks, Content and Technology (DG CNECT) was responsible for new cyber legislation, industrial policies, research and development, and initiatives to raise awareness. Directorate-General for Migration and Home Affairs (DG HOME) revised EU cybercrime policies and promoted collaboration among national cybercrime units. A notable advancement in the EU's efforts to tackle cyber threats was the establishment of the European Cybercrime Centre (EC3)

⁶ Rehrl Jochen, Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union, Armed Forces Printing Centre, Vienna/Austria, 2019 (18-01988)

within Europol in 2013, which significantly improved police coordination, strengthened operational connections, and enhanced the EU's capabilities in fighting cybercrime.

Adopted in 2014, the EU Cyber-Defence Policy Framework was designed to bolster the cyber-defense capacities of Member States in relation to the Common Security and Defence Policy (CSDP), ensure the security of communication networks utilized by EU bodies within the CSDP context, encourage collaboration and the sharing of benefits between civil and military sectors as well as with broader EU cyber policies and the private industry, enhance the availability of training and educational programs, and intensify collaborative efforts with global allies, particularly NATO.

In September 2017, the European Union embraced an updated Cybersecurity Strategy, centering on the advancement of technological capabilities via research, innovation, and skill development, as well as fostering enhanced cooperation at the EU level. This strategy included the creation of the EU Network of Cybersecurity Research and Competence Centers. The announcement of ENISA, the European Union Agency for Network, and Information Security, was made, along with a proposal to introduce a certification framework to evaluate the cybersecurity of information and communication technology (ICT) products, a move that could significantly influence the cybersecurity landscape across Europe. Furthermore, the strategy gave precedence to the development of a cyber-defense training and education platform to mitigate the cyber defense skills shortage among Member States.

The EU's updated Cybersecurity Strategy, introduced in September 2017, is structured around three main components. The first component is the Joint Communication to the European Parliament and the Council, titled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", which serves as the strategy's foundational element [76]. The second component is the legislative proposal for a regulation concerning ENISA, also known as the "EU Cybersecurity Agency," and the establishment of a certification framework for Information and Communication Technology cybersecurity, referred to as the "Cybersecurity Act." The third component is the "Commission Recommendation (EU) 2017/1584," which outlines a coordinated approach for responding to significant cybersecurity incidents and crises. Together, these three components are designed to enhance the security of Europe's vital infrastructure and strengthen the EU's autonomy in the digital realm.

Subsequently, as a countermeasure to the escalating cyber threats during the pandemic, the European Union introduced a fresh cybersecurity strategy on December 16, 2020. This updated strategy of the EU addresses four main security concerns: the hazards linked to the growing interconnectedness of digital infrastructures, the changing nature of threats in the context of geopolitical strife, the attacks on vital infrastructure that jeopardize crucial services, and the surge in cybercriminal activities aimed at data and monetary theft [77].

This strategy outlines the EU's perspective on cybersecurity, focusing on a range of key priorities, including the formulation of a cyber defense policy and the enhancement of capabilities linked to the Common Security and Defense Policy (CSDP). The strategy also pinpoints critical areas for CSDP cyber defense and delineates the roles of various European entities, ensuring adherence to the distinct responsibilities and competences of Union actors and Member States. Additionally, it upholds the EU's institutional structure and its sovereign capacity for decision-making. The collaborative execution of this strategy will aid in establishing a decade of digital security for the EU, advancing the realization of a European Union, and bolstering the EU's stance on the international stage.

The EuroQCI is a key component of the EU's Cybersecurity Strategy of 2020, in the context of an ultra-secure communication infrastructure. It will constitute a secure quantum communication network that covers the entire EU and its overseas regions. By incorporating quantum technology into current communication networks, it will enhance the security of sensitive information and vital infrastructure, offering a supplementary layer of defense based on quantum physics. This infrastructure will bolster the security of European governmental bodies, data centers, hospitals, energy networks, and other critical areas, establishing itself as a central element of the EU's Cybersecurity Strategy for the future years [58]. Leveraging satellite communications and quantum communications infrastructure, the initiative will merge state-of-the-art technologies, including quantum computing, 5G, AI, and edge computing, adhering to the stringent cybersecurity framework. This integration aims to support secure-by-design services that offer dependable, protected, and economical connectivity, as well as encrypted communication channels essential for critical government operations [77].

The EuroQCI will leverage cutting-edge quantum communication technologies, including those developed by researchers under the EU-funded Quantum Technologies Flagship, and particularly upon the advancements made within the Horizon 2020 OPENQKD project.

The Quantum Technologies Flagship is an initiative that aims to propel Europe to the forefront of the second quantum revolution by supporting hundreds of quantum researchers over a decade. Launched in 2018 following the Quantum Manifesto of 2016, it serves as a collaborative platform uniting research institution, industry players, and public funders, aiming to enhance Europe's scientific leadership in quantum technologies. Focused on translating European quantum research into practical applications, the Flagship funds projects in quantum computing, simulation, communication, and sensing, alongside foundational research, education initiatives, and international collaborations. Its ramp-up phase from 2018 to 2022 allocated €152 million to twenty-four (24) projects involving over 1,600 researchers, while its ongoing phase under Horizon Europe, backed by a budget exceeding €400 million, aims to consolidate Europe's research leadership and accelerate the commercialization of quantum technologies. Complemented by funding from the Digital Europe Program, the Flagship's Strategic Research Agenda envisions the development of a "quantum internet" in Europe, interconnecting quantum computers, simulators, and sensors via quantum communication networks, marking a significant milestone towards Europe's quantum-enabled future [78]. The OPENQKD project aims to raise awareness of the maturity of QKD and its seamless integration into existing infrastructure and networks for a wide range of use-cases [79].

Involving European industry partners and SMEs is vital to ensuring that EuroQCI's critical components are based on European technologies. This approach aims to enhance Europe's scientific, technological, and industrial prowess in cybersecurity and quantum technologies. Consequently, the EuroQCI initiative will contribute to bolstering European digital sovereignty and industrial competitiveness, aligning with the goal of positioning Europe at the forefront of quantum capabilities by 2030, as outlined in Europe's Digital Decade agenda. The EuroQCI will consist of a ground component that utilizes current fiber optic communication networks to connect strategic locations both within and between nations, and a space-based component that employs satellites. This space component will be a crucial aspect of IRIS², the EU's new secure communication system that operates from space. The EuroQCI is developed, under the supervision of the Commission and implemented by the Member States and with the support of PETRUS project in the case of the terrestrial segment, and by ESA in the case of the space segment [58].

The PETRUS project serves as a collaborative and supportive initiative for the establishment of national Quantum Communication Infrastructures across EU Member States in the upcoming years. It also helps the Digital Europe Program projects, which are instrumental in creating a robust European industrial ecosystem centered around secure quantum technologies. By uniting previous consortium leaders from significant studies and projects related to EuroQCI, the PETRUS project consolidates their collective knowledge and skills, and incorporates contributions from specialists in both the industrial and academic sectors of the quantum field [80]. The development of the EuroQCI's space, ground, and terrestrial infrastructure will be organized into two (2) primary phases. The initial phase will focus on preliminary validation, which could encompass the development and validation of various technologies and communication protocols. Following this, the full-deployment phase will ensue, incorporating suitable solutions for inter-satellite connectivity and data relay among satellites, ground stations, and terrestrial infrastructure.

Through a collaborative effort involving ESA, the European Commission, and European space enterprises, the Eagle-1 satellite is set to pioneer the development of the first space-based quantum key distribution system. That mission is co-funded by Horizon Europe and is a precursor of the EuroQCI initiative, which will be at a later stage integrated [81]. This innovative project aims to establish an exceptionally secure network by utilizing quantum key distribution, exploiting the fundamental principles of physics to distribute encryption keys, thereby swiftly detecting any potential eavesdropping activities, and ensuring information security. Eagle-1 will demonstrate the feasibility of quantum key distribution technology within the EU using a satellite-based platform, capitalizing on advancements from ESA's Scylight program and validating crucial components procured domestically within the EU.

By showcasing and validating quantum key distribution technologies across low Earth orbit and ground, it will provide invaluable mission data for the development and rollout of EuroQCI, seamlessly integrating into Europe's secure connectivity architecture, thus empowering the EU to ready itself for an independent, cross-border quantum secure communications network. Led by SES, a satellite company based in Luxembourg, and supported by a consortium of more than twenty (20) European entities, the project will leverage an upgraded optical ground terminal from the German Aerospace Centre (DLR) and a newly developed terminal by a Dutch team. Manufactured by Italian firm Sitael, the Eagle-1 satellite will carry a quantum-key payload engineered by Tesat Spacecom of Germany and will be managed by SES. Additionally, several other ESA Member States, including Austria, Belgium, the Czech Republic, Italy, and Switzerland, are actively engaged in the initiative. With a launch scheduled between late 2025 and early 2026, the Eagle-1 satellite will undergo three years of in-orbit validation, supported by the European Commission, representing a significant milestone in Europe's pursuit of quantum-enabled security and communication capabilities [82].

Summarizing, the EuroQCI initiative aims to protect Europe's critical infrastructure and sensitive data, safeguarding them against cybersecurity threats and ensuring the preservation of information security of vital systems, such as smart energy grids, air traffic control, financial institutions, and healthcare facilities. Furthermore, EuroQCI has the objective to enable secure data storage and exchange within various data centers, while ensuring data protection and privacy of governmental processed data. Overall, the vision regarding the EuroQCI infrastructure is to evolve into the backbone of Europe's Quantum Internet.

4.2 Vision and Strategic Objectives

The Internet's emergence has transformed humans' daily lives, enabling instant global connectivity with millions of messages being exchanged per minute. Amidst this convenience, the risk of potential financial transactions', emails', and private data breaches is often not taken into consideration. To enhance security level, currently utilized encryption mechanisms, though conceptually simple, present formidable decryption challenges, requiring very high computational power for decryption. However, there are various cybersecurity incidents that indicated codes being cracked before detection, as well as computational advancements being able to trigger the realization of cybersecurity risks. Considering these challenges, quantum technologies should be widely adopted and utilized to achieve higher security level, leveraging quantum physics principles. As we navigate the information and big data age, and as communications' security becomes increasingly complex, major world's powers, as well as the European Union, invest in quantum physics. In this context, the vision of EuroQCI initiative is to protect Europe's critical infrastructure and sensitive data, providing an additional security layer based on quantum physics, and safeguarding them against cybersecurity attacks. In respect to this vision, the EuroQCI initiative presents various strategic objectives.

The first strategic objective of EuroQCI is the enhancement of Europe's digital appropriate level of autonomy. More specifically, EuroQCI is a pivotal initiative aiming at fortifying Europe's appropriate level of digital autonomy and technological sovereignty, marking a strategic leap towards self-reliance in the digital realm. As EU presents strong commitment towards technological advancement and innovation, EuroQCI aims to enhance the collaboration of subject matter experts both from public and private sector to develop high-quality and competitive European cybersecurity and quantum technologies, mechanisms, and systems. Moreover, by leveraging European researchers and fostering collaboration across academia, industry, and government, the EuroQCI ensures that quantum technologies, mechanisms, and systems are developed and managed taking into consideration the European interests and general objectives. In this context, EuroQCI not only drives innovation but also fosters a robust ecosystem of digital capabilities within Europe. Through seamless integration of quantum communication infrastructure into the existing communication infrastructure, this initiative has the objective to strengthen Europe's digital infrastructure, reducing reliance on external entities and bolstering resilience against emerging cybersecurity threats, vulnerabilities, and attacks. Furthermore, EuroQCI not only aims to safeguard Europe's digital sovereignty but also to position the EU as a global leader in the quantum era. Summarizing, the EuroQCI represents a major step towards a future where Europe controls its digital destiny, ensuring its prosperity and security in an increasingly interconnected world.

Another strategic objective of EuroQCI initiative is the EU's space related industrial ecosystem advancement and development. By utilizing and harnessing Europe's quantum related expertise, the EuroQCI aims not only to foster innovation but also drive the EU's quantum industry towards new frontiers of ingenuity. Additionally, considering that EU has in place extended research capabilities, this initiative serves as a launchpad for the development of new and innovative industrial and commercial applications, thus fostering a dynamic interplay between supply and demand within the EU's industries. Through its emphasis on fostering innovation, the EuroQCI initiative creates a substantial market pull, driving the evolution of the EU's quantum industry and bolstering its competitive edge on the global stage. Furthermore, as already mentioned, this initiative goes beyond mere technological advancement, as it strategically aims to develop critical quantum technologies, mechanisms, and systems for maintaining European appropriate

level of strategic autonomy and digital sovereignty. In summary, the EuroQCI is not just a technological endeavor, it is a cornerstone of the EU's vision for industrial resilience and leadership in the quantum era, aligning with broader strategic objectives to ensure Europe's continued success and prosperity [83].

An additional strategic objective of EuroQCI is the development and establishment of Europe's Quantum Internet [Image 11].

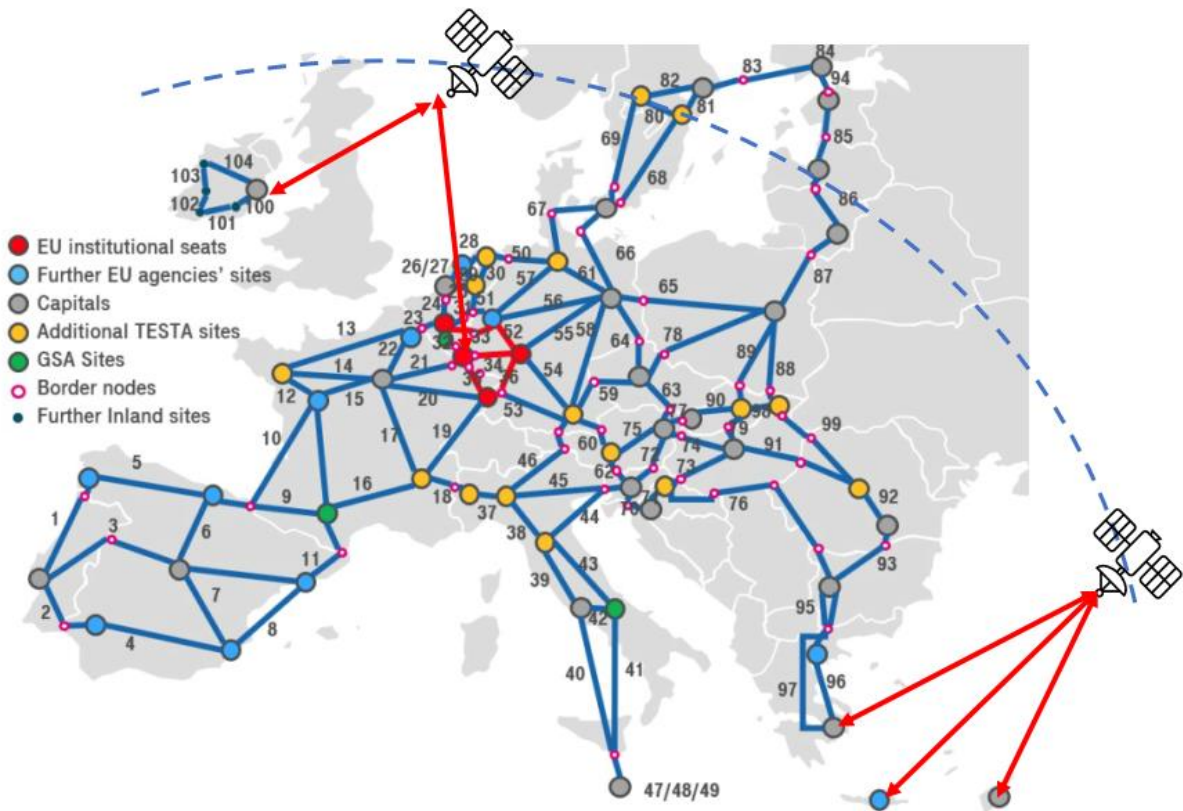


Image 11: EU Quantum Technologies Flagship and the quantum internet [84]

More specifically, the EuroQCI represents a strategic endeavor aiming at establishing Europe's Quantum Internet, as a transformative force in the digital landscape. With a comprehensive long-term plan, the EuroQCI aims to position the quantum communication infrastructure as the backbone for Europe's Quantum Internet, envisioning a network that connects quantum computers, simulators, and sensors via quantum networks to distribute information and resources securely and efficiently across the EU. This ambitious vision promises to revolutionize communication and connectivity, offering high level of security and privacy by enforcing the principles of quantum mechanics. Furthermore, the EuroQCI is designed to enable innovation and collaboration across a wide range of sectors, from cybersecurity to scientific research, by laying the foundation for a robust quantum ecosystem within Europe. By fostering partnerships between academia, industry, and government, the EuroQCI aims to propel Europe to the forefront of the global quantum race, positioning the EU as a leader in unlocking the full potential of quantum technology for societal benefit. Summarizing, the EuroQCI represents a step towards a future where Europe's Quantum Internet serves as a catalyst for progress, driving innovation, fostering collaboration, and shaping the digital landscape for the coming generations.

The final objective of EuroQCI initiative is the enhancement of information security maturity level of existing communications infrastructure. Specifically, the EuroQCI initiative aims at securing Europe's communications infrastructure through the deployment of advanced quantum communication technologies. This ambitious endeavor

aims to address the pressing need for the implementation of robust information security measures across critical infrastructure and government communication networks. By harnessing the power of quantum communication, the EuroQCI aims to offer an advanced level of protection against cybersecurity threats, ensuring the integrity and privacy of sensitive data exchanged within Europe's digital ecosystem. Furthermore, the EuroQCI can serve as a vital tool for securing data centers, enabling safe storage and exchange of information and government data. Beyond its immediate applications, this initiative represents a paradigm shift in information security, supplementing conventional systems with robust information security measures that leverage the latest advancements in quantum technology. By securing Europe's public communication assets and encryption systems against cybersecurity threats, the EuroQCI plays a crucial role in safeguarding the EU's digital sovereignty and bolstering its resilience in the face of evolving security challenges. In summary, the EuroQCI embodies Europe's commitment to ensuring the information security and integrity of its communications infrastructure, laying the foundation for a more secure and resilient digital future [85].

Summarizing, the EuroQCI stands as a transformative initiative aiming to fortify Europe's security landscape through the deployment of advanced quantum communication technologies. Through the quantum communication infrastructure, this ambitious endeavor aims to enhance Europe's appropriate level of digital autonomy, to advance the space related industrial ecosystem, to establish the Europe's Quantum Internet, as well as to address the evolving need for robust information security measures across critical infrastructure and government communication networks. In essence, the EuroQCI embodies Europe's commitment to ensuring the information security of its communications infrastructure, laying the foundation for a more secure and resilient digital ecosystem.

4.3 Core Capabilities

Apart from the initiative's strategic objectives, the EU's EuroQCI aims to bridge the gap between the growing needs for secure governmental communications and the capabilities offered by existing and planned cryptographic systems. One of the main services of EuroQCI will be the Quantum Key Distribution (QKD), which is an ultra-secure form of symmetric encrypted communication as it utilizes the principles of quantum mechanics to provide the sender and recipient of an encrypted message with an intrinsically secure random key in such a way that an attacker cannot eavesdrop or control the whole system [84] [Figure 10].

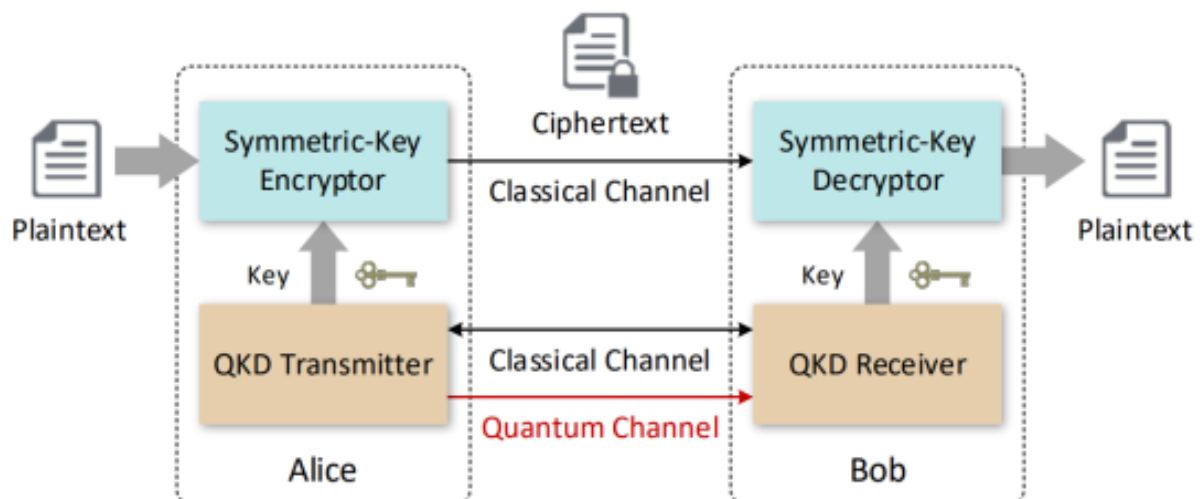


Figure 10: Quantum Key Distribution - QKD [84]

Quantum Key Distribution employs the fundamentals of quantum mechanics to secure and protect communications. It transmits the decryption keys through individual photons, which are particles of light at the quantum level. If an interception is attempted, it alters the photons' physical condition, leaving detectable signs. This mechanism serves as a warning of potential interception, thereby providing a fundamentally secure method for exchanging data. The QKD service will transmit the encryption keys through quantum communication channels on both terrestrial fibre optic and space laser links. The usage of quantum photon states, in quantum superposition states, makes the key distribution infrastructure immune to vulnerabilities unlike the current forms of mathematical function-based encryption methods, as well as inviolable even to quantum computers, securing in such way the confidential data, power grids, government communications, digital transactions and distribution of pins and passwords, even against crypto codebreaking by the quantum computers [84].

More specifically, data is encoded on individual photons. Alice has the option to encode them into a "bit sequence" using one of two polarizations, such as vertical (V) or horizontal (H), or she can opt for two different polarizations, typically denoted as $+45^\circ$ and -45° . Bob then selects one of two bases for measurement, either he measures H, V, or he measures $+45^\circ$, -45° . If he measures in a different base from the one Alice used for preparation, his response will be random and disregarded. However, if they both choose the same base, their results will be perfectly correlated. For instance, if Alice sends H and Bob detects H, these outcomes are retained. The final step involves Alice and Bob communicating about the base used, without disclosing the outcome, which becomes the secret key [86]. While this is one method, there are numerous variations. This approach solely generates a secret key, which must then be integrated into cryptographic protocols to ensure security across various applications. What makes this solution remarkable is that any attempt by a spy or hacker to intercept the key generation process will introduce errors, thus exposing their presence. Crucially, this occurs before any information is encoded or communicated.

Furthermore, a QKD link represents a logical bond between two distant QKD nodes, which are linked via a quantum channel for photon transmission and a public channel for subsequent processing of the shared information. While fiber remains a commonly used choice for qubit transmission, setting up a dedicated optical channel solely for Quantum Key Distribution is not always feasible. Alternatively, a free space link can be utilized, despite that this method relies on favorable atmospheric conditions, a clear path for visible light, and a sufficient signal-to-noise ratio (SNR). QKD networks serve to expand the reach of QKD systems and are comprised of fixed nodes acting as secure access points, assumed to possess unlimited processing capabilities and power supply. The point-to-point nature of interconnecting links between nodes has been demonstrated in past testbeds, revealing the feasibility of transmitting secure keys within QKD networks either hop-by-hop or via a key repeater model. In both scenarios, there is a fundamental presumption that all nodes within the network are trustworthy. A QKD network employs a quantum layer to create a secure symmetric key, a key management layer for the verification and administration of the key, and a communication layer that utilizes the established key to safeguard data transmission [Image 12] [87].

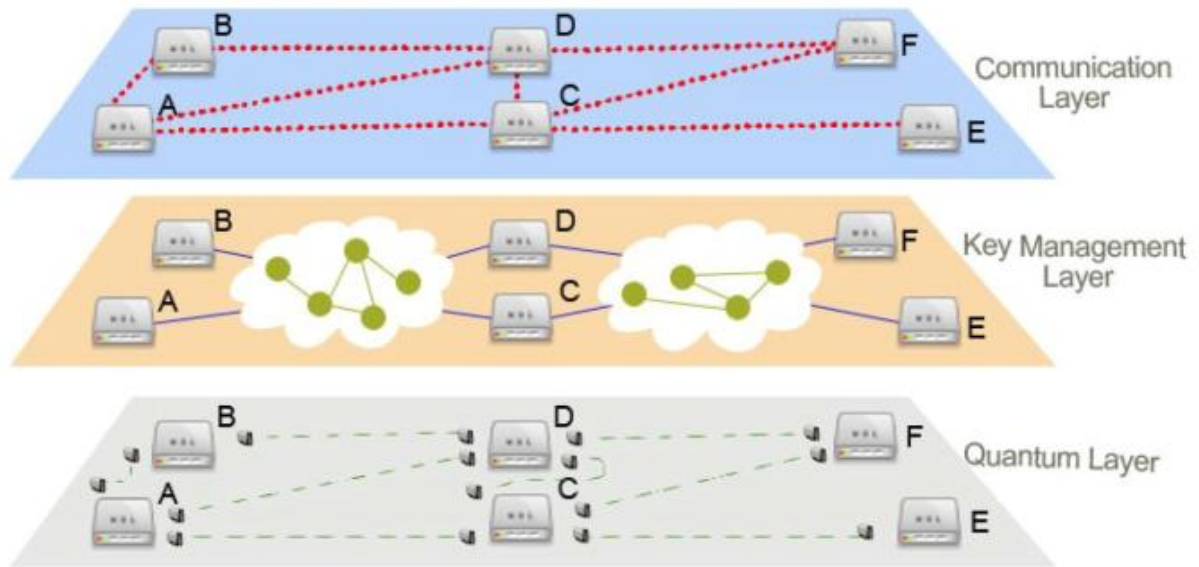
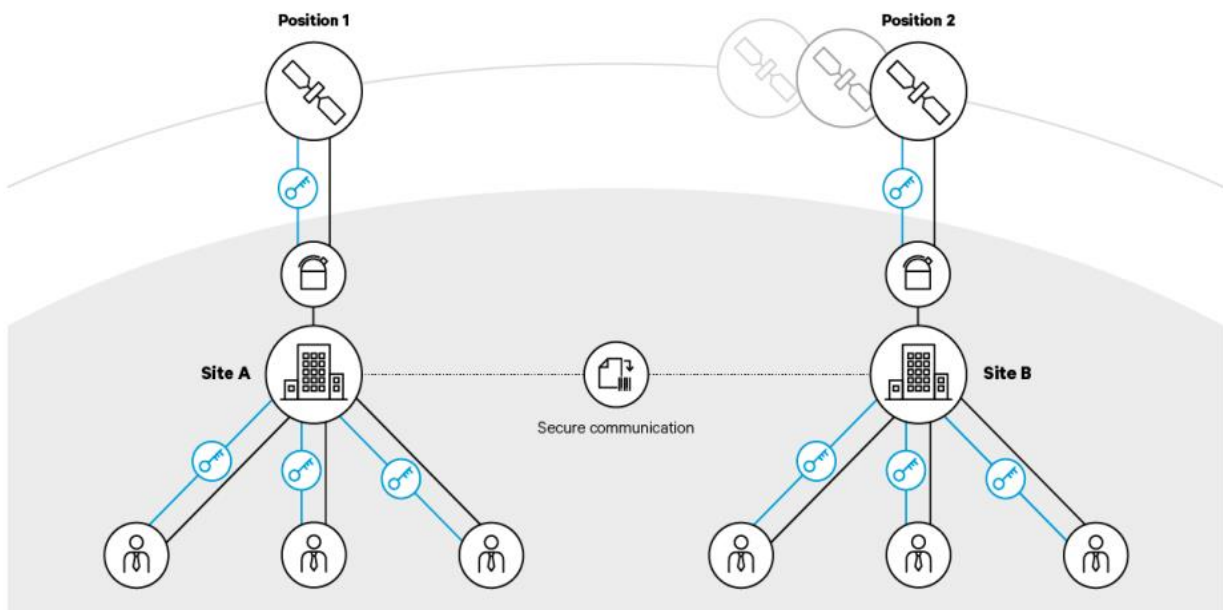


Image 12: QKD network hierarchy layers [87]

Secret keys are established between any pair of QKD nodes and subsequently disseminated to multiple users across diverse locations to ensure long-term protection and forward secrecy [88].

Therefore, EuroQCI is an infrastructure established by the European Commission to provide to European Union entities a service facilitating the generation of cryptographic keys and the transmission of cryptographic key material through the QKD system. Thereafter, this infrastructure could progress into a fully operational quantum communication network. As already mentioned, EuroQCI is an interconnected system including Space Quantum Communication Infrastructure (SpaceQCI), ground, and Terrestrial Quantum Communication Infrastructure (TerrQCI) components utilizing quantum technology [Figure 11].



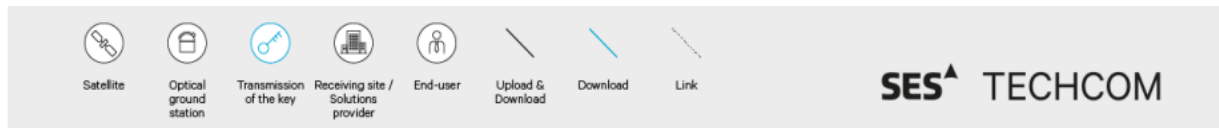


Figure 11: EuroQCI space and terrestrial segments [84]

The SpaceQCI, constituting of one or more satellites, serves as a shared infrastructure under EU ownership, while the TerrQCI comprises interconnected National Quantum Communication Infrastructures (NatQCI) owned individually by each Member State. The SpaceQCI produces and delivers data products (shared key material) to pairs of Quantum Secure Interconnect Points (QSIPs) linked to SpaceQCI User Equipment (SUE), enabling distribution to end-users, particularly over long distances. QSIPs associated with SpaceQCI SUEs can transmit key material to any user within TerrQCI interconnected with SpaceQCI if necessary. The SpaceQCI User Equipment encompasses the apparatus at user sites (typically Optical Ground Stations, Optical Ground Terminals, and User End Points) essential for delivering data products to QSIPs. SpaceQCI and NatQCIs are independent domains that are interconnected by the Quantum Hub, upon request and through bilateral agreements between domain owners. Acting as the orchestrator of the QCI system, the Quantum Hub manages service requests and resource allocation based on established governance, serving as the entry point for users into the QCI system. Interconnection requests between NatQCI domains via SpaceQCI are channeled through the Quantum Hub, allowing for independent operation of domains while facilitating key requests and delivery across interconnected domains. NatQCIs can establish connections via SpaceQCI or TerrQCI. In the event of a compromised NatQCI domain, the Quantum Hub is notified and, in conjunction with relevant Member State authorities, halts connections to/from the affected NatQCI. The concerned Member State may also initiate disconnection [89].

An indicative EuroQCI's business case is the management of sensitive and classified information systems. The preservation of confidentiality of sensitive and classified information systems relies primarily on three (3) key strategies. Firstly, the establishment of a secure perimeter for these systems, adhering to policies and guidelines set by respective bodies, such as the Council for Classified Information Systems, and the receipt of relevant accreditation. Secondly, the deployment of cryptographic solutions at the perimeter's boundaries to facilitate secure exchange of sensitive or classified data over untrusted networks. And finally, the implementation of a robust key management system capable of delivering required cryptographic parameters while ensuring the confidential delivery of key material.

More specifically, HellasQCI presents diverse use cases spanning various sectors. For national security, it encompasses QKD implementation for securing sensitive information, enhancing QKD resilience for critical national security links, and extending satellite QKD connectivity to remote national security nodes. For public health, it offers secure communication solutions for public safety applications, leverages quantum secure technologies for cloud-based health applications and ensures the secure transmission of medical imaging data for public hospitals. For industry and critical infrastructures, HellasQCI employs quantum cryptography to secure communication links vital for critical infrastructures, ensures secure storage in cloud data centers within the ICT sector, and explores applications like QKD over 5G and Next Generation Quantum Secured FTTH services. Additionally, it facilitates the development of quantum encrypted software applications and enables secure connectivity to supercomputing infrastructure through QKD. Finally, in the domain of research, HellasQCI contributes to the preparation for the quantum internet, advances the quantum network controls, and explores hybrid authentication approaches utilizing physically unclonable functions (PUFs) for switched

QKD. Overall, the Quantum Key Distribution service is an integral part of governmental services, complementing the GovSatCom's service portfolio.

Oversight of user access to EuroQCI falls under the jurisdiction of the Secure Connectivity Competent Authority (SCCA), ensuring that proper management and authorization procedures are in place. While the EuroQCI's Concept of Operations (ConOps) simplifies access rights management by attributing it to the SCCA, this responsibility could potentially be delegated to another entity. Authorization for any user seeking access to the SpaceQCI service must be explicitly granted by the SCCA, emphasizing the importance of stringent security measures. The prioritization of users from a Member State's service is determined autonomously by the respective Member State, allowing for tailored access protocols.

Furthermore, the delivery of governmental services to authorized users is entrusted to the European Union Agency for the Space Programme (EUSPA), particularly through the operation of GovSatCom Hubs. Lastly, the ownership and administration of National Quantum Communication Infrastructures (NatQCIs) remain under the control of individual Member States, ensuring national sovereignty over critical communication assets. Furthermore, each NatQCI domain falls entirely under the jurisdiction of a Member State, which oversees, with the endorsement of its corresponding National Security Authority (NSA) or National Cybersecurity Agency (NCSA), the exchange and utilization of cryptographic keys within the domain. A NatQCI represents a distinct segment of the TerrQCI network, owned by either a Member State or a European Union institution, body, or agency. It is possible for Member States or the EU to possess multiple NatQCIs, illustrating the decentralized nature of control and ownership within the network.

Considering the unique capabilities of EuroQCI that were outlined, a set of key performance indicators (KPIs) is established to comprehensively measure and monitor the provided services' efficiency for the respective governmental users. Specifically, concerning SpaceQCI operations, one crucial KPI is the aggregate volume of key material disseminated to pairs of Quantum Secure Interconnect Points (QSIPs) over a specified timeframe, such as one year. On the other hand, for TerrQCI, two primary KPIs are identified. Firstly, the maximum throughput rate of key material between any pair of users within the same National Quantum Communication Infrastructure, aiming to ensure efficient communication within a single domain, and secondly, the maximum throughput rate of key material between pairs of users situated in different NatQCIs, signifying seamless connectivity and effective data transmission across distinct national domains. These KPIs serve as vital metrics in assessing the overall performance and functionality of the EuroQCI services, aligning with the diverse operational requirements inherent in both space and terrestrial quantum communication infrastructures. Based on the measurement and analysis of KPIs' results, the respective improvement activities are performed, when it is deemed necessary, to enhance the EuroQCI's operational efficiency, and security level, meeting the defined security requirements as well as the users' needs.

4.4 Operational Requirements

In order EuroQCI to be able to achieve its strategic objectives, as well as provide its core capabilities should ensure the fulfillment of its operational requirements. The current section defines the primary operational requirements of EuroQCI which play an integral role for its proper functionality, ensuring the provision of secure communication, which is vital for national security, emergency responses, and governmental strategic operations.

To ensure the effective operation of EuroQCI, it is composed of SpaceQCI and TerrQCI components [Image 13].

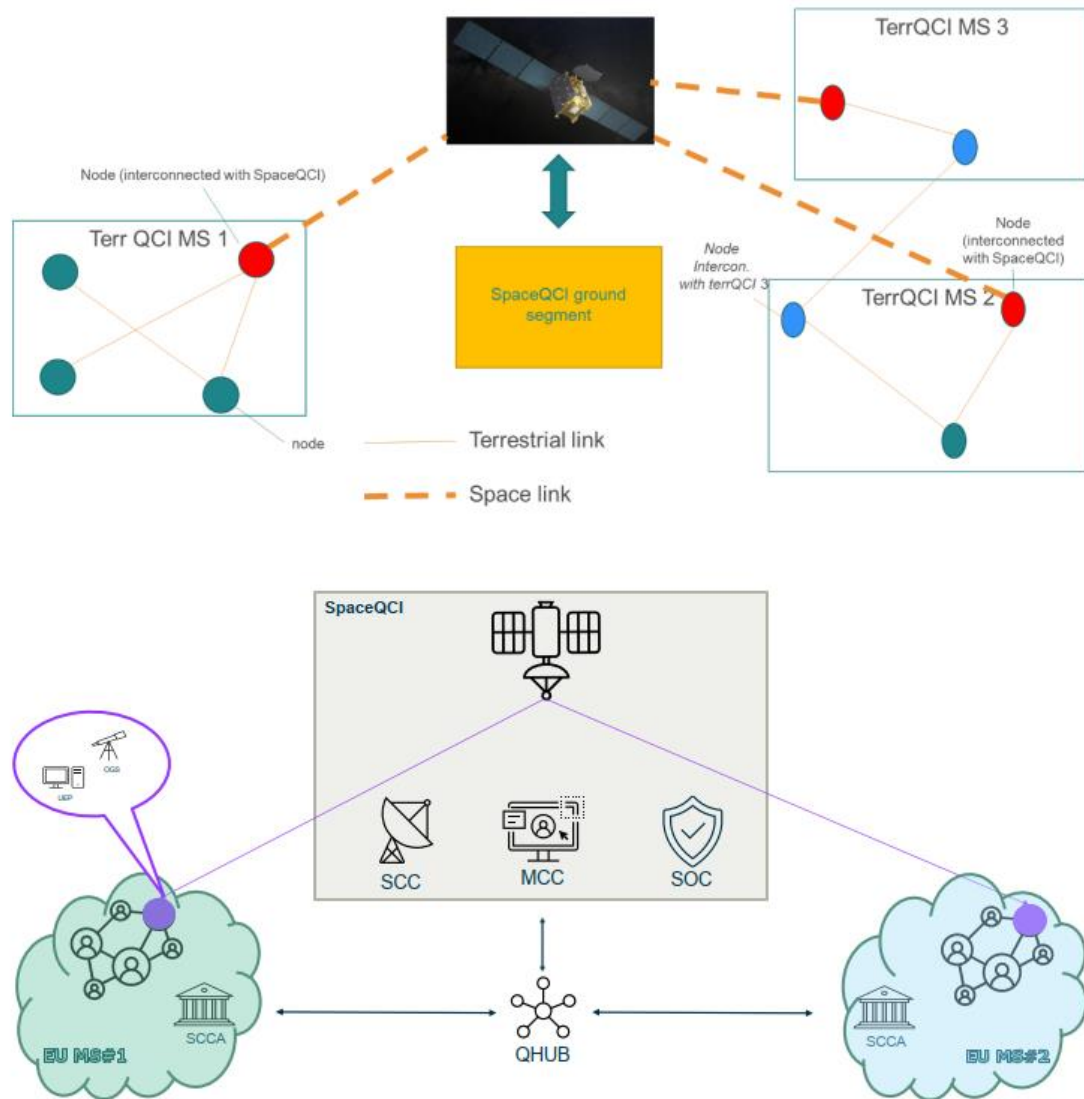


Image 13: Overview of EuroQCI and its main components [89]

More specifically, the SpaceQCI includes the space infrastructure alongside its ground segment, being pivotal for providing the capacity for the whole system to generate the cryptographic keys. Its core elements include the satellites orbiting in space, a Satellite Control Centre (SCC), a Mission Control Centre (MCC), a Security Operations Centre (SOC), and the SpaceQCI User Equipment (SUE). More specifically, in the context of EuroQCI, the Satellite Control Centre serves as the main center for satellite operations, overseeing their functionality, trajectory adjustments, and overall performance in space. The Mission Control Centre acts as the central command hub for coordinating and monitoring mission activities, including satellite deployments, data collection, and task execution, while the Security Operations Centre plays a pivotal role in safeguarding the EuroQCI system against cybersecurity threats, ensuring the integrity and confidentiality of data transmitted and received by employing robust security protocols and monitoring mechanisms.

Lastly, the SpaceQCI User Equipment includes the hardware and software components utilized by users to access and interact with the EuroQCI system, enabling them to utilize its capabilities for various applications. On the other hand, the TerrQCI, which is the terrestrial infrastructure, includes the infrastructures owned by the respective Member States and the EU (NatQCIs), linked to SpaceQCI. The Member States may possess multiple interconnected or standalone NatQCI networks. Several nodes, such as the QCI

Space Interface Point (QSIP) facilitating SpaceQCI and TerrQCI integration, and gateway nodes connecting NatQCIs of different Member States, play vital role to the efficient operation of EuroQCI. Finally, the Quantum Hub (QH) serves as the orchestrator, managing service requests and resource allocation according to established governance, acting as the user interface for the QCI system, resolving conflicts and prioritizing services effectively [89].

From a governance perspective, various roles have been defined, and Authorities have been established, some of which, along with their respective responsibilities are analyzed to this section, to effectively manage and oversee the execution of EuroQCI, as well as to address any issues collectively and tactfully. In the EuroQCI initiative, the European Commission owns the role of Programme Manager, being responsible, jointly with the Member States for TerrQCI, and specifically for the preparation and operational management of the infrastructure's and services' operation. Furthermore, the High Representative (HR), in collaboration with the European External Action Service (EEAS), undertakes the responsibility of identifying and addressing security threats to the Union or its Member States stemming from the EuroQCI's deployment, operation, or usage. Specifically, the HR should recommend instructions to the Council or issue provisional instructions promptly in urgent situations to mitigate potential harm to the Union's essential interests, while the Council is responsible to decide on these instructions or when relevant to confirm the provisional instructions provided by the HR.

Moreover, each Member State and organisation with EuroQCI users or nodes shall have a Secure Connectivity Competent Authority (SCCA) to ensure the adherence to the defined security requirements related to EuroQCI usage. These authorities should monitor the compliance of governmental services with the security requirements, manage access rights, supervise the usage of SpaceQCI User Equipment, and establish a central reporting mechanism for security risks, including electromagnetic/optical interference, under the Secure Connectivity programme. While this Concept of Operations (ConOps) assumes the SCCA's direct management of authorizations, individual Member States retain the flexibility to designate specific entities for this purpose.

Furthermore, a SpaceQCI Operator should be established to be responsible for the daily management of SpaceQCI operations, ensuring the platform's smooth operation and appropriate configuration, ensuring also that connections between QSIPs are created in accordance with the mission configuration requests defined by the Quantum Hub, the management of necessary functions of SUEs, the guaranteeing coordination between SpaceQCI and the SUE, the monitoring of the service's quality related indicators, the evaluation of feasibility of new connection requests, as well as the incorporation of new SUEs or satellites as requested by the Quantum Hub.

Similarly, a Terrestrial Network Operator should be established and be responsible for the management and configuration of the terrestrial network, ensuring the deployment and maintenance of quantum infrastructure, the distribution of the secrets received from the Quantum Hub to SUEs allowing them to access the SpaceQCI services, as well as the management of connections within the national infrastructure as per relevant requests. Additionally, the EuroQCI Security Monitoring Entity should oversee the compliance with security standards within the Quantum Hub and SpaceQCI, continuously assessing their operations and promptly notifying HR/EEAS if deviations occur, offering expertise on definition of security incidents' impact and recommendation of mitigation activities, ensuring the cybersecurity readiness and appropriate response to cybersecurity attacks. Although, it does not monitor the NatQCIs' adherence to security requirements [89].

Additionally, the National Security Monitoring Entity should be established, operating under the authority of the relevant Secure Connectivity Competent Authority, and being responsible to ensure the compliance with security protocols within NatQCI. Specifically, the National Security Monitoring Entity should monitor the adherence to applicable security requirements, promptly reporting any deviations to the SCCA, and instructing operators to mitigate associated risks. In cases where security risks in a NatQCI may affect other Member States or the Union, the respective National Security Monitoring Entity should promptly notify the EuroQCI security monitoring entity for intervention. On the other hand, the Quantum Hub plays a pivotal role as the exclusive liaison with SCCAs for QKD service requests [Image 14].

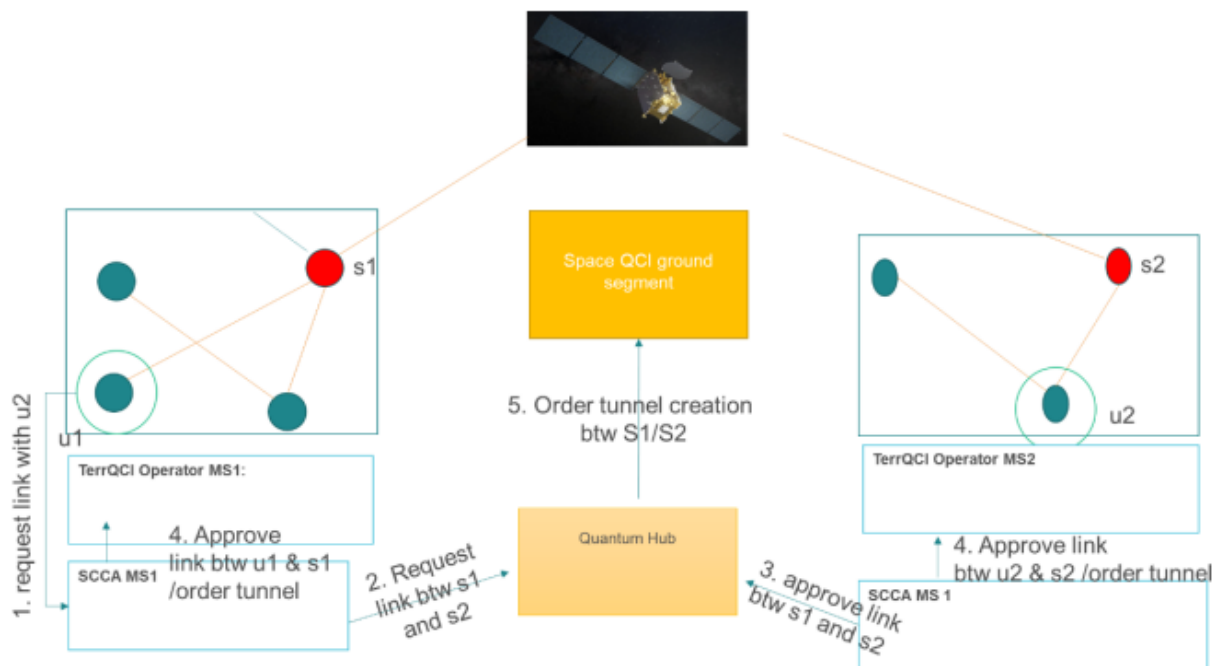


Image 14: Delivery of key material to EuroQCI users via SpaceQCI [89]

Its responsibilities encompass requesting the addition of new SpaceQCI User Equipment and satellites, distributing initial secrets for access to Quantum Key Distribution services, and facilitating connections between QSIPs as per relevant requests. Additionally, the Quantum Hub should verify the system capabilities, propose alternatives, if necessary, manage priorities, and resolve conflicts among service requests, ensuring efficient SpaceQCI operations and promptly informing the respective authorities of any service provision challenges.

From an operational and technical perspective, EuroQCI's Quantum Key Distribution service aims to deliver the cryptographic keys to the respective pairs of users. Then, the EuroQCI's users shall be able to use the cryptographic keys either directly in their cryptographic products or in combination with cryptographic keys delivered by other cryptographic Key Management Systems (KMSs), like those relying on Post-Quantum Cryptography (PQC) algorithms.

Additionally, the QKD service is designed to interconnect various information systems, and therefore the QKD service should generate keys for information of various classification levels, from non-classified to sensitive and secret or equivalent national classification levels. Access to cryptographic keys should be strictly managed, meaning that the QKD service should be designed to provide them only to pairs of users that are authorized to receive them, by their respective authorities. Furthermore, scalability is a key consideration, while the production capacity of cryptographic keys should be fully

aligned with users' demand for receipt of keys. To manage peak loads exceeding service capacity, a prioritization mechanism should be enforced and implemented by the respective Competent Authorities to ensure the right allocation and prioritization of keys distribution. As the data protection and privacy is always a crucial concern, the whole infrastructure and system should be designed and implemented in such a way to ensure that the user's identity that request the QKD service is protected. The QKD service shall rely only on quantum communication, symmetric cryptographic algorithms, and hash algorithms, to reach this objective [89].

Another operational requirement of EuroQCI is the establishment of a testing and evaluation framework and methodology for assessing the compatibility of existing communication technologies with the new quantum communication infrastructure, as well as the security certification and validation of the new quantum communication technologies, with a view to possible integration of existing communication infrastructure with the quantum systems.

More specifically, the establishment of a testing and evaluation framework and methodology is crucial to ensure the robustness and security of QKD-based technologies and services developed within the EU, through assessment and certification of these technologies, providing users the required assurance that they will not be vulnerable to cybersecurity attacks. The testing and evaluation framework and methodology should include both security and non-security aspects. Security aspects should aim to create a "product security baseline for EuroQCI components" which will involve collaboration with relevant national security authorities coordinated by Commission, as well as to develop and establish a testing methodology capable of evaluating security products incorporating quantum cryptography, in line with common criteria. On the other hand, non-security aspects should encompass functional and non-functional attributes, including safety measures. The primary objective is to evaluate EU technologies for their adherence to standards (e.g., architectures, protocols, etc.), security requirements (e.g., security certification or accreditation), as well as product specifications (e.g., features, performance, reliability, etc.), ultimately accrediting them at the European level to be used to initiatives like EuroQCI, as well as to ensure interoperability with EuroQCI and GovSatCom services.

An additional objective of such endeavor is the deployment of a flexible large-scale approach capable of testing and certifying the QKD devices, technologies, systems, and operational processes, benefiting stakeholders across Member States. The testing and evaluation framework and methodology will be particularly valuable for industries manufacturing EU QKD devices and technologies, as well as for projects implementing advanced quantum systems and networks within and between EU Member States [90]. The design, development, and implementation of such testing framework and methodology require preliminary studies on the subject, available funding, experienced and competent human resources, as well as the establishment of security certification schemes that would be needed for the QCI to deploy technologies that process sensitive and classified information.

Summarizing, the EuroQCI has various operational requirements from a governance, operational, and technical perspective that should be taken into consideration to ensure proper functionality and maintenance of appropriate level of information security.

4.5 Limitations and Challenges

Having analyzed the vision, strategic objectives, as well as the main capabilities of EuroQCI, that include but are not limited to the enhancement of Europe's appropriate level of digital autonomy, the EU's space related industrial ecosystem advancement and

development, the development and establishment of Europe's Quantum Internet, as well as the enhancement of information security maturity level of existing communications infrastructure, it should also be defined the limitations and challenges of EuroQCI. These challenges, ranging from governance to technical constraints, that will be analyzed to the current section, necessitate good understanding to take advantage of the full potential of quantum communication for governmental purposes. Through an in-depth analysis of these challenges, this study aims to provide valuable insights into optimizing EuroQCI capabilities and maximizing its benefits.

Within the European Union, several Member States have embarked on ambitious projects to establish quantum communications networks at local and national levels. These endeavors are critical steps toward harnessing the transformative potential of quantum technologies. Yet, the fragmented nature of these initiatives underscores the necessity for a more unified approach at the European level. By pooling resources and expertise, the EU can effectively compete with the rapid progress in quantum communication observed in other global regions. Quantum communication promises unparalleled security and efficiency in data transmission, making it a strategic asset in the modern digital landscape.

However, the expertise and industrial strength in this cutting-edge field are not uniformly distributed across the EU, which is the first challenged that should be addressed. Some Member States are at the forefront, pioneering quantum technologies, while others lag, lacking the necessary infrastructure and technical prowess. The disparity in capabilities among Member States could lead to an uneven playing field, where only a few benefits from the quantum leap in communication technology. To avoid this, a coordinated EU-wide strategy is imperative. Such a strategy would not only foster collaboration and knowledge sharing but also ensure that all Member States have equitable access to the benefits of quantum advancements. By aligning their efforts, EU nations can create a robust and secure quantum communication network that spans the continent. This network would serve as a backbone for future technologies and position the EU as a formidable player in the global quantum race. It would also stimulate innovation, attract investments, and potentially lead to breakthroughs that could spill over into various sectors, from cybersecurity to finance.

Additionally, as already mentioned, unlike traditional encryption methods that rely on mathematical complexity for security, QKD's strength is derived from the laws of physics, which dictate that any attempt at eavesdropping can be detected. This high level of security necessitates the use of bespoke equipment designed to handle the quantum properties of particles like photons, which is another challenge. More specifically, implementing QKD is not a trivial matter, as it demands dedicated fiber optic lines or the careful alignment and maintenance of free-space optical systems for line-of-sight communications. This is because QKD signals are delicate and can be easily disrupted by noise or interference, making the integrity of the physical transmission medium a critical factor. The requirement for specialized infrastructure means that QKD cannot be retrofitted into existing networks through software upgrades or delivered as a cloud-based service. The hardware dependency of QKD also introduces constraints in terms of scalability and futureproofing.

In a digital landscape where threats evolve quickly and technology advances at an unprecedented pace, the inability to update or patch QKD systems without physical intervention is a notable limitation. This rigidity contrasts with the agility of software-based security solutions, which can be continuously improved and adapted to counter new vulnerabilities. Moreover, the cost and complexity of setting up and maintaining a QKD infrastructure may be prohibitive, potentially limiting its adoption to those with significant

resources or specific high-security needs. As such, while QKD offers a theoretically unbreakable form of encryption, practical considerations around its deployment and maintenance must be carefully weighed against the security benefits it provides. The future of QKD may depend on advancements that allow for greater compatibility with existing network architectures and more flexible upgrade paths, ensuring that this cutting-edge technology can be effectively integrated into the broader ecosystem of cybersecurity defenses.

The adoption of Quantum Key Distribution to enhance cryptographic security comes with a significant uptick in both infrastructural investment and the spectrum of internal security threats. The nature of QKD networks, which often necessitates the establishment of intermediary trusted nodes, leads to a substantial increase in operational costs. These nodes, essential for maintaining the integrity of the quantum keys over extended distances, require the construction and maintenance of highly secure facilities, which in turn incurs a financial cost. Beyond the monetary implications, these trusted nodes introduce an augmented security risk, particularly from insider threats. Since these relays are pivotal in the QKD process, individuals with access to them hold considerable power and, if their intentions are malicious, there is the potential to compromise the entire network. The human element thus becomes a critical point of concern, and the need for rigorous vetting, continuous monitoring, and stringent access controls becomes paramount, adding layers of complexity and cost [91].

An additional challenge in the context of EuroQCI initiative is that the current landscape reveals that QKD technologies and products have not yet reached a level of maturity necessary for the security of EU classified information (EUCI). Several critical challenges impede the full-scale deployment of QKD for this purpose, including the need for standardized QKD protocols, comprehensive side channel analysis, and robust evaluation methodologies. As a result, the program supporting EuroQCI is tasked with fostering the development of these areas and integrating approved cryptographic products into the infrastructure as they become available. Given the nascent state of QKD and the looming threat of quantum computing, which could potentially compromise traditional encryption methods, the program advocates for a multifaceted approach to protect EUCI.

This approach would blend conventional cryptographic solutions with emerging post-quantum cryptography and, where feasible, QKD in a hybrid model. Such a strategy aims to leverage the strengths of each method to ensure the highest level of security and key distribution efficiency. The security that QKD systems offer in practice diverges from the theoretical ideal of unconditional security promised by the laws of quantum physics. The actual security level is contingent upon the precision of hardware and engineering designs, which are far more prone to vulnerabilities than the theoretical models suggest. The stringent requirements for cryptographic security, which demand an exceedingly low tolerance for error, pose a formidable challenge in validating the efficacy of QKD systems. This is exacerbated by the fact that the specialized hardware intrinsic to QKD can inadvertently introduce weaknesses, as evidenced by several high-profile breaches in commercial QKD systems [92].

Moreover, the inherent sensitivity of QKD to eavesdropping attempts, while a cornerstone of its theoretical security premise, also renders it susceptible to denial-of-service attacks. Such attacks could disrupt the quantum key distribution process, thereby undermining the reliability of QKD as a secure communication method. As the EuroQCI moves forward, addressing these multifaceted challenges will be crucial in realizing a secure and resilient infrastructure capable of protecting the EU's sensitive information against the quantum threats.

While QKD excels at generating secure cryptographic keys that can be employed by encryption algorithms to ensure message confidentiality, it does not inherently address all facets of secure communication, which is a challenge and potential information security risk. For instance, the cryptographic keys produced by QKD could be integrated with symmetric key cryptographic algorithms to bolster integrity and authentication measures, but this hinges on the critical assumption that the QKD transmission's origin is verifiable and trusted, a function QKD itself does not fulfill. To bridge this gap, additional measures such as asymmetric cryptography or pre-shared keys are necessary to authenticate the source of a QKD transmission, ensuring that the keys are indeed exchanged between legitimate parties. This is a crucial step in preventing man-in-the-middle attacks where an adversary could masquerade as a legitimate entity to intercept or manipulate the key exchange.

Furthermore, the confidentiality that QKD aims to provide can also be achieved through quantum-resistant cryptography, which is designed to withstand the potential future threats posed by quantum computing. Quantum-resistant algorithms often come with the advantage of being less costly and having a risk profile that is more thoroughly understood and easier to manage compared to the relatively uncharted territory of QKD. Therefore, QKD may be seen as a specialized tool with unique advantages, but it is not a standalone solution. A comprehensive security strategy, particularly one that aims to protect sensitive information at the level of the EuroQCI, must consider a blend of technologies and approaches, including both QKD and quantum-resistant cryptography, to create a robust and multi-layered defense against the evolving landscape of cybersecurity threats.

The Space Quantum Communication Infrastructure component of the EuroQCI initiative operates having space system limitations, such as the cyclical nature of satellite orbits, the agility with which satellites can be reoriented, and the impact of atmospheric conditions and daylight on communication capabilities. Consequently, the Quantum Security Infrastructure Point must implement a buffering strategy to store the quantum cryptographic keys received from SpaceQCI at the Satellite User Equipment. The duration for which these cryptographic keys are buffered is determined by the service level requested by the user, with SpaceQCI periodically replenishing the QSIP's reserves in accordance with a pre-established average delivery rate. This ensures a steady supply of cryptographic keys to meet user demands over time.

In contrast, the Terrestrial Quantum Communication Infrastructure is not encumbered by these space-based constraints and can supply cryptographic keys on demand. However, the rate at which TerrQCI can deliver them is influenced by the physical properties and configuration of the network, such as the photon transmission capacity of fiber optic cables and the intricacies involved in interconnecting multiple National Quantum Communication Infrastructures. These factors collectively dictate the volume of cryptographic keys that can be transmitted through TerrQCI, shaping its operational capabilities. By harmonizing the capabilities of space-based and terrestrial systems, the EuroQCI can offer a comprehensive and resilient infrastructure, ensuring that users have access to quantum keys when and where they are needed, despite the inherent limitations of each individual component.

The EuroQCI's ambition to establish secure quantum communication links is tempered by the inherent limitations of the quantum channel key generation rate, which is a function of the direct optical fiber or free line-of-sight connections that facilitate point-to-point (P2P) Quantum Key Distribution. The security of the keys generated through these links is linked to the constraints of the medium over which they are transmitted. Presently, commercial optical fiber systems that support QKD are typically restricted to distances around 100

kilometers, with key generation rates capped at several tens to hundreds of kilobits per second. While free space links offer an alternative medium, they come with their own set of challenges, including the necessity for clear atmospheric conditions, an unobstructed path of visible light, and a signal-to-noise ratio conducive to effective communication, all of which limit operational windows.

The reach of QKD via optical fibers or terrestrial free space is further constrained by channel losses that exponentially diminish the photon transmission rate, effectively capping the distance for effective QKD at a few hundred kilometers. In contrast, satellite based QKD emerges as a promising solution to transcend these terrestrial limitations, leveraging the minimal photon loss and decoherence found in the vacuum of space. This approach holds the potential to extend the reach of QKD to a global scale, offering a pathway to a worldwide quantum network. The EuroQCI's pursuit of such satellite based QKD endeavors is a testament to the innovative strategies being employed to overcome the physical constraints of earthbound systems and to realize the vision of a secure, interconnected quantum communication infrastructure spanning the globe [93].

In conclusion, the EuroQCI initiative, while a groundbreaking step towards a pan-European quantum communication infrastructure, presents challenges and limitations. Throughout this section, the multifaceted constraints that accompany the ambitious goals of the initiative, from the technical intricacies of Quantum Key Distribution to the logistical hurdles of integrating space-based and terrestrial networks were analyzed. Inherent limitations of current QKD technologies, such as the restricted key generation rates and the physical bounds of transmission distances, pose significant obstacles to the initiative's implementation. Moreover, the reliance on secure and authenticated channels, the need for robust standardization, and the potential vulnerabilities to insider threats further complicate the landscape. Despite these challenges, the EuroQCI stands as a testament to the collaborative spirit and innovative drive of the European Union, forging a path towards a more secure future in the quantum era.

4.6 Implementation Reasons

4.6.1 Technological Advancement and Innovation

Taking into consideration the capabilities, limitations, and challenges of EuroQCI initiative there are various reasons that support its implementation need, the most critical of which will be analyzed in detail to the current section. In an era where technological innovation is the cornerstone of progress, initiatives like the EuroQCI are really promising. As the world increasingly relies on secure and resilient communication networks, the EuroQCI emerges as a beacon of technological advancement, driving innovation and shaping the future landscape of communication technology.

EuroQCI represents a pioneering effort to apply the principles of quantum mechanics for communication purposes. Unlike conventional communication systems, which rely on classic bits for encoding information, quantum communication utilizes qubits, exploiting the unique properties of quantum entanglement and superposition. By leveraging these quantum capabilities, EuroQCI promises high level of security and speed in data transmission, laying the foundation for transformative advancements in various domains. One of the most compelling reasons to implement EuroQCI lies in its ability to bolster cybersecurity. Traditional communication channels are susceptible to interception and hacking. EuroQCI addresses this challenge by employing Quantum Key Distribution (QKD) protocols, enabling high level of security based on the laws of quantum mechanics, not only to safeguard critical information but also to enhance trust in communication networks, essential for fostering innovation in sectors, such as finance, healthcare, and

government. Quantum communication holds the potential to revolutionize fields, such as quantum computing, quantum sensing, and quantum metrology. By establishing a robust infrastructure for quantum communication, EuroQCI provides researchers with the tools necessary to push the boundaries of scientific knowledge, paving the way for groundbreaking discoveries and technological advancement.

Furthermore, EuroQCI serves as a catalyst for innovation, driving collaboration between academia, industry, and governmental entities. The development and deployment of quantum communication technologies require multidisciplinary expertise, fostering research and development. As stakeholders converge to harness the potential of EuroQCI, new opportunities emerge for startups, SMEs, and established industry enterprises to pioneer new technologically advanced applications and services, leading to economic growth and advancement of EU's competitiveness on a global scale. Illustrating the transformative potential of EuroQCI, various case studies highlight real-world scenarios, that quantum communication technologies drive innovation. Examples include but are not limited to secure communication networks for autonomous vehicles, quantum-resistant cryptography for financial transactions, and quantum-enhanced imaging for medical diagnostics. These case studies underscore the diverse applications of EuroQCI across different sectors and emphasize its role as a driver of technological advancement.

In conclusion, the implementation of EuroQCI is not merely a matter of technological progress but a strategic imperative for shaping the future of communication technology. By utilizing the power of quantum mechanics, EuroQCI offers security, facilitates scientific exploration, and catalyzes innovation ecosystems. As the quantum revolution has begun, EuroQCI is a testament to EU's commitment to pushing the boundaries of what is possible in the realm of communication technology, building a secure, interconnected, and innovative future.

4.6.2 Secure Satellite Communications

The EuroQCI initiative can be considered as an innovative initiative aiming to address the growing need for secure satellite communications, to be protected against evolving security threats while fostering innovation and technological advancement. Satellite communications play a pivotal role in enabling global connectivity, supporting vital services ranging from telecommunications and navigation to weather forecasting and disaster management. However, traditional satellite communication networks are vulnerable to interception, hacking, and spoofing, posing significant risks to sensitive data and critical infrastructure. EuroQCI aims to secure satellite communications by leveraging the principles of quantum mechanics, to establish inherently secure communication channels.

One of the primary advantages of EuroQCI lies in its ability to secure data transmission between satellites, ground stations, and terrestrial networks. Conventional encryption methods, while effective, are susceptible to brute-force attacks and advances in quantum computing. EuroQCI mitigates these risks by employing QKD protocols, which enable the generation of cryptographic keys with provable security based on the laws of quantum mechanics. This ensures that satellite data remains confidential and tamper-proof, safeguarding against unauthorized access and manipulation. Satellite communications support critical infrastructure systems, including banking, energy distribution, and transportation networks. Any disruption or compromise of satellite communications can have disastrous consequences, leading to possible financial losses, service outages, and even threats to national security. In this context, EuroQCI enhances the resilience of critical infrastructure by providing secure and resilient communication links that are

impervious to interception and cyberattacks, thereby bolstering societal resilience and continuity of critical operations.

In the realm of defense and national security, secure satellite communications are indispensable for command and control, information gathering, and tactical operations. EuroQCI offers a quantum leap in securing military and government communications by ensuring the confidentiality, integrity, and authenticity of sensitive information exchanged over satellite communication networks. Whether facilitating secure communications or safeguarding diplomatic exchanges, EuroQCI enhances the operational effectiveness providing a strategic advantage to various defense agencies. Beyond its security benefits, EuroQCI serves as a catalyst for technological innovation and economic growth. The development and deployment of quantum communication technologies enhance collaboration between academia, industry, and governmental entities, fostering research and development. By investing in EuroQCI, Europe can position itself at the forefront of quantum technology innovation, creating new opportunities for startups, SMEs, and established to the space industry enterprises to pioneer novel applications and services in satellite communications.

In conclusion, the implementation of EuroQCI represents a pivotal step towards fortifying satellite communications security and resilience in an increasingly interconnected world. By harnessing the power of quantum mechanics, EuroQCI offers a robust framework for establishing secure communication channels that are immune to present and future cybersecurity threats. Embracing EuroQCI is not only essential for safeguarding critical infrastructure and national security but also for driving innovation and prosperity in the digital age. As Europe moves towards a quantum-secure future, EuroQCI is an opportunity for progress in satellite communications domain.

4.6.3 Enhanced Users' Trust

Trust is necessary in fostering users' confidence in the utilization of satellite communication networks, ranging from telecommunications and internet services to financial transactions and critical space operations. However, conventional communication systems are susceptible to cybersecurity threats, data breaches, and privacy violations, eroding users' trust. EuroQCI aims to enhance users' trust by leveraging the principles of quantum mechanics to establish inherently secure and resilient communication channels.

One of the primary drivers for implementing EuroQCI lies in its ability to secure sensitive data exchanged over communication networks, as already mentioned to the previous sub-sections. In various sectors, including but not limited to government, financial, and e-commerce, trust is paramount for both customers and businesses. EuroQCI enhances trust by safeguarding communication against data breaches, identity theft, and fraudulent activities through quantum-resistant encryption protocols. By ensuring the confidentiality, integrity, and authenticity of information, EuroQCI fosters trust and reliability in operations, driving economic growth and consumer confidence. Privacy concerns are increasing nowadays, with users continuously worrying of unauthorized data processing, and access to their personal information. EuroQCI addresses these concerns by offering end-to-end encryption that is immune to quantum-enabled attacks, preserving user privacy and ensuring data protection.

Whether communicating sensitive messages or sharing confidential documents users can trust EuroQCI to safeguard their privacy and protect their data from malicious actors. Trust in communication networks is particularly critical for supporting essential services and critical infrastructure systems, including emergency response mechanisms. EuroQCI enhances trust in critical infrastructure by providing secure and resilient communication

links that are impervious to cybersecurity threats. Whether ensuring the reliability and coordination of emergency responses, or safeguarding national security communications, EuroQCI ensures confidence in the resilience and continuity of vital services. Beyond its security benefits, EuroQCI empowers users by offering greater control over their communications. By providing secure and privacy-preserving communication channels, EuroQCI enables users to utilize satellite communications capabilities with confidence.

In conclusion, the implementation of EuroQCI promises the enhancement of users' trust in communication networks. By leveraging the power of quantum mechanics, EuroQCI offers a secure, resilient, and privacy-preserving framework for communication, fostering trust across various sectors' stakeholders. Implementing EuroQCI is not only essential for safeguarding sensitive data and critical infrastructure but also for empowering users and driving innovation in the digital age.

Overall, considering the advantages of EuroQCI in the context of technological advancement and fostering of innovation, enablement of secure and resilient satellite communications, as well as the enhancement of users' trust, the implementation of this initiative is a necessity to address the challenges derived from the current emerging and evolving operational and threat landscape.

5. SYNERGIES BETWEEN GOVSATCOM, IRIS² AND EUROQCI INITIATIVES

5.1 Comparative Analysis of GovSatCom, IRIS² and EuroQCI Main Differential Aspects

Having analyzed the vision and strategic objectives, core capabilities, operational requirements, as well as limitations and challenges of GovSatCom, IRIS², and EuroQCI initiatives it should be outlined both their main differences and interdependencies. In this context, the current section aims to perform a comparative analysis of these three pivotal European satellite communication initiatives. Each of these initiatives plays a significant role in shaping the continent's strategic satellite communication infrastructure, however they present distinct differences, indicatively as part of their operational status and timeline, target of users that could utilize their provided services, geographical coverage, available technological resources, as well as objectives [Table 2].

	GovSatCom	IRIS ²	EuroQCI
Operational Status	Operational	Not Operational	Not Operational
Targeted Users	Governmental	Governmental & Commercial	Governmental & Commercial
Geographical Coverage	EU	Worldwide	EU
Technological Resources	Existing Satellites	Multi-Orbital Constellation	Quantum Key Distribution Network
Services Objective	Secure Satellite Communication Services	Secure & Resilient Satellite Communication Services	Secure Data Transmission Services

Table 2: Main differences of GovSatCom, IRIS², and EuroQCI initiatives

In this context, firstly, one main difference of these three initiatives is as part of their operational status and implementation timeline. More specifically, GovSatCom is already operational since 2013, providing dedicated satellite communication capabilities to several European Union's Member States and countries, primarily for defense and security purposes. This initiative, as already mentioned, is a strategic asset for Europe, ensuring that EU countries have access to secure and reliable satellite communication services for military operations, crisis management, and other critical missions that require robust and protected connectivity. In contrast, IRIS² is in the planning and development phases, having already faced delays based on the initial implementation timeline. This initiative aims to develop a state-of-the-art satellite communication network,

integrating innovative technologies to deliver secure, resilient, and continuous interconnectivity even in the most adverse conditions. Similarly, EuroQCI is also currently in the stage of planning and development, aiming to create a highly secure and resilient quantum communication network that would be virtually impervious to cybersecurity threats and attacks, leveraging the principles of quantum mechanics.

Another difference among these initiatives is their targeted user groups. More specifically, GovSatCom already provides in some countries, and generally aims to provide satellite communication services to governmental users, such as EU security actors, operators of key infrastructure and industry entities, as well as EU Agencies to support critical missions and operations undertaken by military forces, agencies, and civil protection authorities. Contradictory, IRIS² is strategically designed to provide services to a wider spectrum of users, including both governmental and commercial users, thereby having a broader potential customer target in comparison to the more narrowly focused GovSatCom initiative. Specifically, IRIS² will provide satellite communication services to EU's institutions and agencies, as well as commercial entities, particularly those involved in critical infrastructure and services that require high level of security and resilience. Similarly, EuroQCI is expected to serve both governmental and commercial users, such as governmental institutions, defense and security agencies, space and satellite operators, research and academic institutions, and indicatively financial institutions, reflecting a wide range of applications for quantum-secure communications.

Furthermore, another crucial difference is about geographical coverage. GovSatCom is primarily focused on delivering satellite communication services across the entire European Union, with the purpose of ensuring comprehensive coverage that meets the specific needs of all Member States. In contradiction, IRIS² ambitiously aims to establish a global satellite communication network that extend beyond the borders of the European Union, aiming to connect users around the world. The initiative's global scope is significant for ensuring connectivity in remote locations, and during international humanitarian efforts where conventional communication systems may be nonexistent or compromised. Similarly to GovSatCom, the geographical coverage of EuroQCI is designed to cover the entire European Union, providing a secure quantum communication network that connects all EU Member States, linking critical infrastructures and government institutions within and potentially even beyond the EU's borders.

Additionally, these three initiatives differ in the aspect of technological / satellite resources that will be utilized for the provision of their services. More specifically, GovSatCom aims to strategically utilize both commercial and governmental satellite assets and services through the pooling and sharing capability, enabling a flexible and robust service offering tailored to the diverse needs of its users. IRIS² aims to deploy a multi-orbital constellation, which includes the strategic operation of satellites from various orbital positions, including GEO, MEO, and LEO, to achieve comprehensive coverage and enhanced service resilience. By leveraging these diverse orbital positions, IRIS² constellation has the objective to deliver a robust satellite communication network with multiple layers of redundancy, ensuring that in the event of a satellite failure or service degradation in one orbital layer, other satellites can compensate to maintain uninterrupted service. Additionally, the multi-orbital approach allows for optimized coverage across different latitudes. In this context, EuroQCI initiative aims to develop a terrestrial Quantum Key Distribution (QKD) network, consisting of a ground-based infrastructure of fiber-optic cables and QKD stations, supplemented by satellite QKD links, utilizing quantum-enabled payloads to distribute encryption keys from space, to bridge the gap in areas where traditional fiber-optic networks are impractical or too costly to deploy.

Finally, another difference of these initiatives is the objective of their provided services. Specifically, GovSatCom aims to deliver reliable, secure, immediate, and continuous satellite communication services, ensuring that users have uninterrupted access to communication channels even in challenging circumstances, such as natural disasters, conflict zones, or areas where terrestrial networks have been compromised or are non-existent. In the same context, but focusing on different objectives, IRIS² aims to provide highly secure and resilient satellite communication services, focusing on reliability and continuity, ensuring that communities and governments have the communication tools they need to respond effectively to crises and maintain essential services under all circumstances. Lastly, EuroQCI initiative aims to enable an ultra-secure data transmission network, theoretically immune to interception or compromise, across the EU by leveraging the capabilities of quantum technology, safeguarding the transmission of classified information between government agencies, ensuring the privacy of citizens' data, and protecting the integrity of critical sectors' data, such as financial, healthcare, and energy.

In summary, the role of supporting governments aligns with the ongoing mission of GovSatCom. However, IRIS² distinguishes itself by incorporating advanced technologies such as cryptography and utilizing EuroQCI's capabilities. Its modular design, which includes multi-orbital features, and its commercial objectives aim to enhance the competitive nature of the current market, indicating an evolution from the traditional GovSatCom framework. While these programs share synergies and bear resemblances, their unique differences underscore their importance and the need for their deployment.

5.2 Analysis of Potential Benefits of GovSatCom and EuroQCI to IRIS²

Having presented and explained the results of the comparative analysis of GovSatCom, IRIS² and EuroQCI main differential aspects, and considering that these initiatives present similarities, as well as can have various synergies, the current section aims to define the potential benefits of GovSatCom and EuroQCI to IRIS² initiative's functionalities and capabilities.

The evolution of digital age has brought numerous challenges and opportunities in the realm of secure satellite communications. Recognizing the strategic importance of robust and resilient satellite communication networks, the European Union has initiated IRIS², which is a visionary initiative aiming to reinforce Europe's satellite communications infrastructure for governmental and commercial use. IRIS² aims to utilize the capabilities of GovSatCom initiative of the Union Space Programme, and gradually integrate the innovative EuroQCI initiative. The synergy between these two initiatives within IRIS² is set to establish a secure, satellite-based, multi-orbital satellite communication system capable of quantum key distribution (QKD), offering an unprecedented level of encryption and therefore security. More specifically, this section will provide a comprehensive analysis of the potential benefits and practical applications of GovSatCom and EuroQCI within the IRIS² framework, underpinning the transformative impact these integrations will have on secure satellite communications.

GovSatCom is designed to provide reliable and secure satellite communication services tailored to the needs of European governmental bodies. By integrating GovSatCom's capabilities into IRIS², the EU aims to create a robust satellite communication network that can withstand both natural and man-made disasters. More specifically, by integrating GovSatCom's capabilities into IRIS² involves a strategic combination of satellite communication assets and services to enhance the resilience, interconnectivity, and security of the European Union's satellite communication infrastructure. Furthermore, IRIS² terrestrial infrastructure can incorporate the GovSatCom Hubs to provide the

requested satellite communication services to the respective users. Indicatively, during natural disasters, such as floods or earthquakes, terrestrial communication infrastructure may be severely damaged or destroyed. GovSatCom's satellite links can serve as a critical lifeline, ensuring that emergency services, humanitarian aid, and crisis management teams can coordinate effectively, even in the most affected areas. Moreover, IRIS² multi-orbital approach, utilizing GEO, MEO, and LEO based satellites, ensures comprehensive coverage and low-latency communication across Europe and beyond. By combining these capabilities, it is particularly beneficial for border surveillance and maritime security operations, where real-time data transmission is crucial for tracking and responding to illegal activities. More specifically, GEO satellites offer wide coverage and persistent visibility over a region, which is ideal for monitoring large-scale activities such as migration patterns or environmental changes, while LEO and MEO satellites, on the other hand, provide faster data throughput and lower latency, which are essential for time-sensitive operations like defense communications and real-time command and control.

IRIS², also, will leverage the capabilities of EuroQCI, representing a forward-thinking approach to safeguarding Europe's governmental satellite communications against the rising threat of quantum computing. EuroQCI's quantum key distribution technology enables the transmission of cryptographic keys with a level of security that is theoretically immune to any computational attack, including those from quantum computers. This quantum advantage ensures that sensitive information, ranging from diplomatic correspondence to military operations, remains confidential and tamper-proof. An example of EuroQCI's application within IRIS² could be the secure transmission of electoral data during national elections, where the integrity of the information is of utmost importance. By employing QKD, electoral commissions can guarantee that the results are transmitted without the risk of interception or manipulation, thus upholding the democratic process.

The strategic integration of GovSatCom and EuroQCI within the IRIS² framework is a clear demonstration of the EU's commitment to securing its communication networks against both current and future threats. By leveraging the strengths of both initiatives, IRIS² is positioned to deliver a satellite communication infrastructure that is not only resilient to physical and cybersecurity threats but also equipped with the most advanced encryption technologies available. This dual-layered approach creates a comprehensive security solution that addresses the full spectrum of risks, as well as ensuring that governmental communications, which are often targeted by sophisticated cybersecurity attacks, are protected by the most advanced technologies available.

Summarizing, the IRIS² initiative is a beacon of European innovation, symbolizing a unified effort to protect and enhance governmental communications through state-of-the-art satellite and quantum technologies. The integration of GovSatCom and EuroQCI within IRIS² is a strategic move that will provide Europe with a multi-orbital, quantum-secured network that is well-equipped to handle the complexities of modern-day communications. The benefits of this integration extend beyond mere technological advancement, but they encapsulate the EU's commitment to safeguarding its institutions and citizens against a wide array of threats. As we move towards an increasingly interconnected and data-driven future, the successful implementation of IRIS² will be critical in ensuring that Europe remains at the forefront of secure governmental communications.

6. COMPREHENSIVE SECURITY REQUIREMENTS ACROSS THE GOVSATCOM LIFECYCLE

6.1 Enforcement of Security by Design Principle

Space has become indispensable for Earth's economic and societal advancement, and satellites play a key role not only as critical infrastructures, but also in supporting the operation of other critical infrastructures, representing a single point of failure for various industries. Because of their complexity, space systems often lack high cybersecurity standards. Furthermore, there are not plenty of comprehensive international industry standards and guidelines to define the best practices that should be followed. Given the commercialization of space, malicious actors consider space infrastructure as an attractive target. Therefore, it is critical to intensify cybersecurity measures for space infrastructures. Priority must be given on securing the ground and user segments, which are recognized as the most vulnerable targets for cybersecurity threats. In evaluating space infrastructure components, it is essential to view space systems as unified and interconnected entities. Key aspects like launch capabilities, ground control stations, and satellite production are vital parts that demand focused protection because of their central roles in the operation of space systems. Hence, the implementation of technical and organizational cybersecurity related controls is required, such as indicatively access control, network segmentation, encryption, as well as development of policies, procedures, and guidelines tailored to managing cybersecurity threats and risks.

Moreover, the European Union Agency for Cybersecurity (ENISA) categorizes space as a sensitive area and has emphasized that the absence of formally defined cybersecurity standards in the industry has resulted in substantial security risks. Managing a satellite is akin to overseeing a computer network, since satellite communications frequently depend on IP-based links in space. Nonetheless, in contrast to servers, IP-based space systems are exposed to the public, which means they must confront a range of threats. These can vary from basic attacks such as Denial of Service (DoS) and jamming to more complex attempts to gain root access. Consequently, cybersecurity controls must be implemented during the lifecycle of space systems development, and more specifically during the design phase of new space systems. This also requires a cultural shift for space companies to a security by design approach, to take into consideration confidentiality, authentication, integrity, and availability principles [94].

Now more than ever, it is crucial to adopt the security by design approach for the design and development of space infrastructure. Firstly, every manufacturer should develop their products in a way that incorporates the security by design practices. Secure by design means that space products are developed in a way that are protected against malicious cybersecurity threat actors. To achieve this objective, indicatively a risk assessment should be performed to identify possible existing cybersecurity risks, and then apply appropriate protective and preventive measures to the space product. Secure practices and multiple layers of defense, known as defense-in-depth, are also recommended to prevent realization of malicious activities from compromising space systems or obtaining unauthorized access to processed sensitive data. Additionally, manufacturers should follow a tailored threat model during the space product's design and development phase to address all potential threats. A formally defined and documented set of security controls should be developed by manufacturers, enforcing its implementation to achieve the security by design, ensuring that there will be deviations only in exceptional situations. Finally, a shift to the current approach is needed to consider security as a business priority, and not as just a technical feature. However, at this point, it should be highlighted that there is no single solution to diminish the existing cybersecurity threats and risks

arising from the malicious threat actors, as well as space products that are secure by design will continue to have vulnerabilities. Nonetheless, a large set of vulnerabilities are due to a relatively small subset of root causes and thus, an appropriate level of protection can be achieved through implementation of robust cybersecurity measures during the design and development phases of space infrastructure [95].

More specifically, through an indicative use case scenario, incorporating the security by design principle into space infrastructure, such as a satellite communication system, begins with comprehensive threat modeling during the design phase to proactively identify and prioritize potential security threats, like jamming, eavesdropping, and physical security attacks. The satellite communication system should be indicatively architected with state-of-the-art encryption to secure data in transit, as well as with secure boot mechanisms and authenticated firmware updates to ensure the integrity of onboard systems. Physical security can be achieved using tamper-resistant components, and the communication system's resilience can be enhanced by designing redundancy into its architecture, allowing it to withstand and recover from incidents such as denial-of-service attacks. Rigorous access control measures, including multi-factor authentication and role-based access, should be implemented to permit only authorized interactions with the satellite, and a comprehensive monitoring system should be deployed to detect and respond to abnormal activities in real-time. Regular technical assessments and security audits should also be performed to ensure compliance with defined security principles and applicable industry standards and best practices, as well as identify areas for improvement. By embedding these multifaceted security measures from the design phase, the satellite communication system will be protected against a wide range of cybersecurity threats, ensuring the protection and continuity of critical space-based operations.

The NIST IR 8270 highlights the necessity of developing and implementing a cybersecurity program tailored for space operations to ensure that the security by design principle is effectively implemented. A Cybersecurity Framework (CSF) facilitates the effective execution of such a program through a seven-step process. Initially, it is essential to define the scope and priorities of the cybersecurity program, ensuring that risk mitigation strategies are integrated from the inception of space architecture development and space systems design, aligning with the defined business goals and strategic objectives. The next phase involves the compliance with regulatory obligations, and defined risk management approach, while also identifying potential threats and vulnerabilities. Subsequently, the third phase involves the definition of the current cybersecurity posture, as well as an assessment of how the CSF is implemented by listing the activities that are currently being executed. A risk assessment exercise should follow to evaluate the operational environment, and identify the existing risks, leveraging cybersecurity threat intelligence information to assess the probability and potential impact of realization of the identified cybersecurity risks. The fifth step involves the establishment of a target profile that reflects the preferred cybersecurity posture. Then, the discrepancies must be identified, and prioritized by comparing the current and target profiles, which, when combined with a threat analysis, enables the creation of a risk-based action plan. The final step is the execution of this action plan [94].

The Framework's application should be a cyclical process that requires regular repetition, especially when there are changes in the space systems / architecture or the cybersecurity threat environment. Furthermore, in this context, as recommended by NIST and MITRE frameworks, the security profiles and assessments' results should be regularly and consistently reviewed, as well as the defined action plans should be reviewed and updated when it is required. These reviews should take place at least annually or following significant cybersecurity events or industry developments.

Summarizing, a common, baseline security control framework should be established and implemented during the design phase of space infrastructure, as well as the misconception that security is solely the responsibility of one of the parties involved in the design and implementation of space systems should change.

6.2 Enablement of Secure Command and Control for Satellites

Satellites are increasingly at risk as potential adversaries demonstrate both the intent and capability to disrupt and disable space operations. These threats are prompting a shift in space strategies, necessitating greater level of cybersecurity, robustness, flexibility, and rapid response to predict and prevent the expanding array of such threats and vulnerabilities. Among the considered countermeasures is the implementation of cybersecurity controls to command and control (C2) links of satellite operations. The telemetry, tracking, and commanding functions are essential components of satellites' missions, facilitated by the command and control (C2) links.

While the data transmitted is often encrypted, ensuring confidentiality and authentication, the signal waveforms do not hide the pattern of the data flow, being clear when commands are sent. Also, the telemetry varies in modes based on the satellite's operational status, such as changes in data rates, which can be identified by analyzing the signal characteristics. This means that an external observer might deduce certain activities within the systems, potentially leading to either passive or active exploitation. Furthermore, the signal waveforms are not particularly resilient to the reception of false signals. Although cryptographic measures are in place to prevent the most common unauthorized activities, such as unauthorized satellite commands, these are not the only concerns [96].

Therefore, applying advanced encryption mechanisms to satellite C2 links is a main cybersecurity control that ensures data confidentiality. By using robust encryption algorithms, such as AES-256-, or 128-bit Advanced Encryption Standard (AES) that is most suitable for securing small satellite telemetry/telecommand channel [97], communications between ground stations and satellites can be secured against eavesdropping and interception. Key management practices, including the regular rotation of cryptographic keys and the use of Public Key Infrastructure (PKI), further enhance security by making it difficult for attackers to decrypt the data without the proper authorization. For example, a satellite might employ a secure handshake protocol that verifies the identity of the ground station before initiating data transfer, akin to how HTTPS secures web transactions [98].

Additionally, to protect satellite C2 links from jamming attacks, which aim to disrupt communications by flooding the frequency with noise, anti-jamming techniques such as spread spectrum technology should be employed. By spreading the signal across a wider bandwidth, it becomes more difficult for an attacker to target the specific frequency being used for satellite communications. Frequency hopping, where the signal rapidly switches between different frequencies, is another example that makes it challenging for an attacker to jam the signal continuously.

Another security control is the implementation of Intrusion Detection Systems (IDS) on satellite C2 links that can help in the early detection of unauthorized access attempts or anomalies in the communication patterns. An IDS can monitor the network traffic for signs of malicious activity and raise alerts when suspicious behavior is detected. For instance, if an IDS identifies an unusual increase in command signals or telemetry data that deviates from normal operational patterns, it could indicate an attempt at unauthorized control or data exfiltration.

Furthermore, enhancing the physical layer of satellite communications can prevent attackers from gaining access to the satellite signal. Techniques such as beamforming focus the transmission power towards a specific geographic area, reducing the likelihood of interception by unintended recipients. Additionally, using low probability of intercept and low probability of detection technologies minimizes the chances that an adversary can detect or intercept the signal. For example, a military satellite might use directional antennas that concentrate the signal beam towards a secure ground station, limiting the potential for adversaries to tap into the communication link.

Building redundancy into the satellite C2 infrastructure ensures continuity of operations even if one link is compromised. This can involve setting up multiple ground stations, alternative communication paths, and on-board processing capabilities to handle commands and data without relying on a single point of failure. For example, a satellite system might have a primary ground station for routine operations and a secondary, geographically distant station that can take over in case the primary is compromised or suffers from a denial-of-service attack.

Also, strict access control measures and multi-factor authentication can restrict access to satellite C2 systems to only authorized personnel. By requiring something the user knows (a password), something the user has (a security token), and something the user is (biometric verification), the risk of unauthorized access is significantly reduced. For instance, operators may need to provide a password, a smart card, and a fingerprint scan before being granted access to the satellite control console.

Conducting regular security audits and penetration testing of the satellite C2 links can identify vulnerabilities before they are exploited by attackers. Security professionals can simulate cyber-attacks on the system to test the effectiveness of current security measures and recommend improvements. For example, a simulated attack on the satellite's communication protocols might reveal a weakness that could be exploited by an adversary, prompting the implementation of additional security layers or protocol enhancements [99].

Furthermore, having a well-defined incident response plan in place ensures that any security breaches can be effectively handled. This plan should outline the steps to be taken in the event of a cyber-attack, including containment, eradication, recovery, and post-incident analysis. For example, if a satellite C2 link is compromised, the response team should follow the plan to quickly isolate the affected systems, remove the threat, restore operations, and analyze the breach to prevent future incidents.

Finally, educating users about cybersecurity best practices and specific threats to satellite C2 systems can help prevent accidental or intentional insider threats, as human factor is the weakest link in many cases. Regular training and awareness sessions, as well as cyber-attacks simulation exercises can keep users informed about how to recognize and respond to cybersecurity incidents. For example, satellite operators can perform training on how to identify phishing attempts that could compromise their login credentials.

It should be noted that the most suitable combination of these controls should be implemented to ensure the highest level of security. Indicatively, to secure satellite C2 links from satellite-to-satellite cyber-attacks, a combination of cybersecurity controls is essential, such advanced encryption and key management, intrusion detection system implementation, physical security measures, and strong access control with robust authentication protocols. Furthermore, anomaly detection algorithms will help identify unusual behavior indicative of an attack, network segmentation will prevent the spread of breaches, a comprehensive incident response plan will enable quick mitigation and recovery from attacks, while diligent configuration and patch management will keep

satellite systems updated against known threats [100]. Collectively, these cybersecurity measures form a multi-layered defense strategy that enhances the security and resilience of satellite C2 links against potential cybersecurity threats, vulnerabilities, and attacks.

6.3 In-Orbit Security Monitoring and Threat Detection

The economic growth of commercial space markets, such as those involving satellites, are threatened by the continuously evolving cybersecurity threat landscape that target the space-based assets along with their associated terrestrial infrastructure, making space missions operating in an inherently risky environment. These threats mainly concern the satellites' manufacturers, owners, as well as operators, establishing the necessity of mitigating such threats and relevant risks, the most challenging of which being the cybersecurity related.

Upon the satellite is placed into orbit, the satellite is required to initiate a signal and set up a communication channel with the ground-based command and control system. Then, the satellite is usually subjected to multiple verifications to confirm that its systems are operational. Following these verifications, the satellite transitions to the active phase [Image 15].

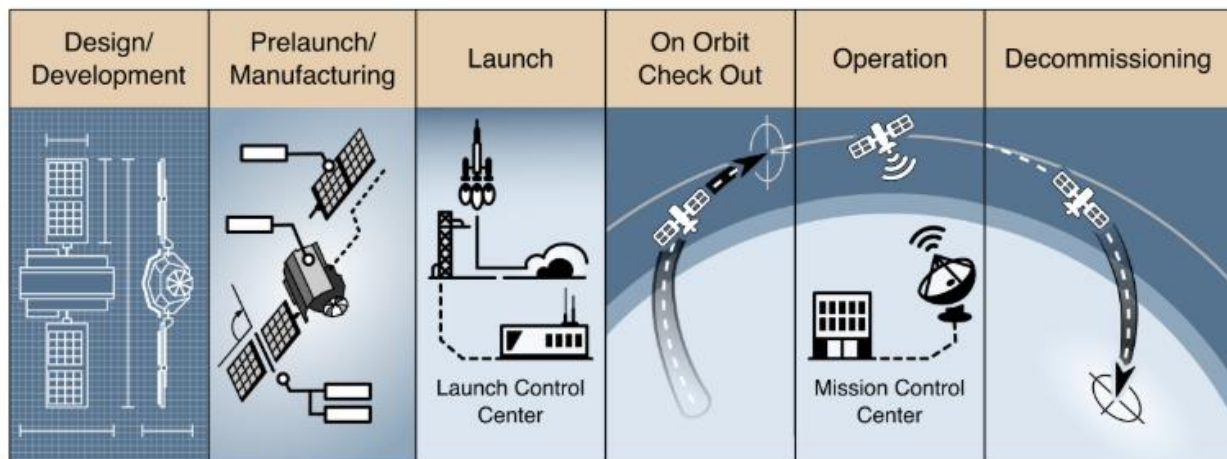


Image 15: Phases of satellites' operations [101]

A pivotal process during this phase is the handover of satellite's command and control from the team responsible for its development to the team responsible for its operation. From a cybersecurity perspective, this transition requires close monitoring due to the change in responsibility, as it could potentially be acquired by adversaries if the process is not performed with a formally defined and structured approach. Furthermore, as far as cybersecurity is concerned, upon normal operation of the satellite a continuous security monitoring with threat detection capabilities should take place to timely identify any malicious activities. Generally, this can be achieved by integrating internal vehicle cybersecurity measures.

Internal vehicle cybersecurity pertains to the satellite's inherent, by-design security controls, encompassing its defenses against cybersecurity threats, its capabilities to identify malicious activities, its resilience to cybersecurity attacks, as well as its ability to restore its functionality, when it is compromised. These cybersecurity measures should be incorporated into the design phase and embedded from the early stages of the satellite's design and development. Typically, the responsibility for ensuring the satellite's internal cybersecurity state falls under the satellite's owners and operators, while they frequently delegate it to specialized and competent third-party service providers [101].

After the satellite reaching its operational orbit, the human interaction is minimal, however this does not eliminate the risk of cybersecurity incidents. The satellite's software and hardware may have vulnerabilities and flaws that once exploited could affect the satellite's functionality. For instance, in case of inadequate validation of radio frame processing or transmission of corrupted data from the digital signal processing software that is used for radio functionality, this could potentially lead to memory buffer overflows, denial-of-service, and/or jamming. This form of jamming is stealthier because it can be activated by transmitting just a few data packets, rather than requiring a persistent radio frequency interference signal. Given that satellites are engaged in missions where reliability is crucial, they should be equipped with robust operating systems designed to offer substantial protection against cybersecurity attacks [102].

In this context, ongoing security monitoring of the satellite's systems is essential for detecting new threats and vulnerabilities to ensure satellite's provided services' reliability. More specifically, security monitoring for a satellite can be performed through a comprehensive system, such as a SIEM solution, that should continuously monitor the satellite's operational data / logs for any signs of unauthorized access, or malfunction. To support this solution's functionality and to feed it with the most appropriate data, ensuring effective monitoring, real-time monitoring capabilities should be in place, intrusion detection systems that analyze communication patterns and flag irregularities should be deployed, as well as abnormal operation detection algorithms should be utilized to compare current behavior against established baselines of normal operation. Furthermore, periodic integrity checks of the satellite's software and hardware components should be performed to ensure they remain uncompromised. In the event of a detected possible cybersecurity incident, the SIEM solution should trigger alerts, as well as automated response activities to isolate any compromised systems or satellite's components should be initiated, enabling the protection of satellite's critical functions. In this context, a Security Operations Center, operating on an 24/07/365 basis should be established with competent personnel monitoring the alerts created from the SIEM solution and the other utilized capabilities. Thus, comprehensive security monitoring is essential for early detection and response to potential cybersecurity events and/or incidents, ensuring the satellite's continuous and secure operation in the hostile environment of space.

To enable proper response to cybersecurity incidents, a well-defined incident response plan should be in place to enable operators to quickly address and mitigate the impact of each incident. The plan should include processes for isolating affected systems, assessing the extent of the incident, and enabling the return to normal operations. Recovery plans should detail the steps to return the satellite to a secure state, which may involve reconfiguring systems, applying patches, or, in extreme cases, sending commands to reset the satellite to its factory settings.

Additionally, regular updates to the satellite's software and firmware should be performed to patch known vulnerabilities and improve security measures. For example, updating cryptographic algorithms to keep pace with advancements in computing power helps maintain the resilience of encryption methods. Also, all communication links to and from the satellite should employ strong encryption to prevent eavesdropping and interception [103].

Summarizing, to ensure robust in-orbit security monitoring and threat detection for satellites, a comprehensive suite of cybersecurity controls must be implemented. These controls should be designed to protect the satellite's systems from potential cybersecurity attacks and enable the early detection of any malicious activities.

6.4 Ensuring the Security of Satellite-to-Earth Communication

Activities conducted in space heavily rely on the performance of information systems and wireless communication networks that link them via the electromagnetic spectrum. These are the main components that form the cyberspace infrastructure both on Earth and in space. Considering that cybersecurity emerges in every aspect of space operations, including satellite launches, telemetry, tracking, and command, as well as communications, from space to space, from earth to space, and from space to earth, the respective threats, risks, and vulnerabilities should both be identified and mitigated implementing the appropriate cybersecurity related controls [Image 16] [104].

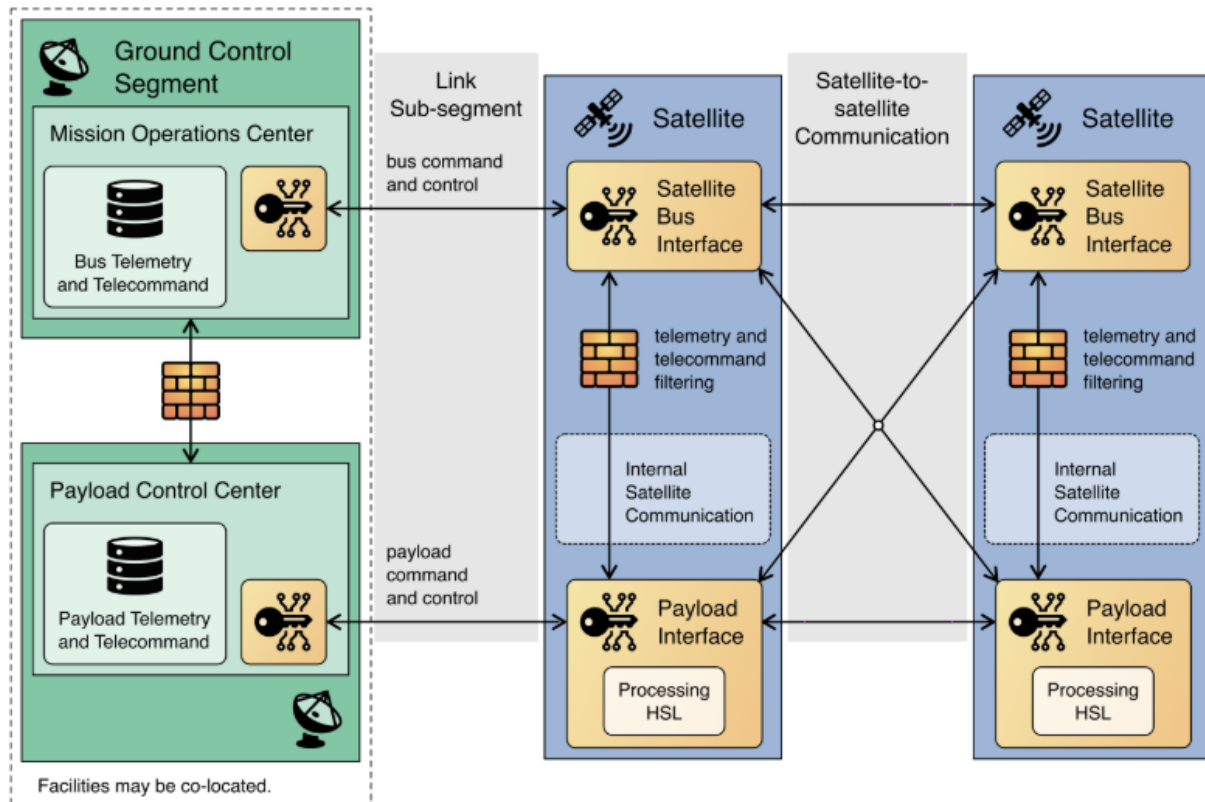


Image 16: Major communication links used in space systems [101]

The primary security risk of communication channels (both uplink and downlink) is jamming, which indicatively can affect the GPS systems. More specifically, jammers for GPS operate by emitting signals on the same frequency used by GPS devices, with the intent to interfere with or distort the signals from GPS satellites. These jammers are easily obtainable and inexpensive, making them accessible to less advanced state entities and private malicious actors. Additionally, GPS spoofing, which involves altering the GPS signal, poses a greater threat than jamming because it can mislead users into believing their GPS functions correctly. Creating a system capable of a software-defined spoofing attack is relatively straightforward and cost-effective, with which an attacker can modify or completely replace authentic signals. In case the downlink to a satellite is compromised, false information will be transmitted into a user's communication system, leading the receiver to determine inaccurate information. Overall, an attacker only needs to create a cost-effective spoofer to take over the uplink signal directed at a satellite. This practice is sometimes known as satellite hijacking, which involves repurposing a satellite for a different use. Another form of communication hijacking is broadcast signal intrusion, where a satellite's broadcast signals are hijacked either by overpowering the original signal at the same frequency or by penetrating the transmitter to replace the signal.

Deliberate tampering of data communicated to a spacecraft can lead to disastrous events, and specifically whether it results in inaction (for instance, if the command is ignored) or in an incorrect response by the spacecraft's onboard systems [105].

Frequently, the communication channel between satellites and terrestrial infrastructure involves the use of radio frequency signals transmitted through the atmosphere, which are vulnerable to interception. In this context, if the signals are unencrypted, they could be subject to interception and surveillance by an adversary. In the foreseeable future, such attacks are expected to persist, originating not just from nation state actors, but also from well-resourced non-state actors (such as criminal organizations aiming for monetary profit), especially as space becomes increasingly utilized for communication technologies. Therefore, the encryption in satellite-to-earth communication serves as a critical control against unauthorized access and interception of transmitted information. Encryption ensures that even if the signals are intercepted, they remain inaccessible to anyone without the proper decryption key, while maintaining the confidentiality and integrity of the transmitted data, protecting against espionage, and preventing malicious actors from gaining insights into operational patterns or commandeering control of satellite functions. Furthermore, encryption enhances the reliability of communications, fostering trust in the systems that support a wide array of services from GPS to international broadcasting and strategic military communications. Overall, the benefits of encryption extend beyond safeguarding information, playing a pivotal role in ensuring the continuous and secure operation of critical infrastructure that relies on satellite systems, thereby supporting economic stability, national security, and the safety of space-based assets.

More specifically, the implementation of robust end-to-end encryption involves encrypting data at the originating point, either a satellite or a ground station, and maintaining that encryption throughout the transmission until it reaches the intended recipient, who then decrypts the data with a secure key. Additionally, the use of advanced cryptographic algorithms and regular update of encryption keys are essential to defend against evolving cybersecurity threats. To complement encryption, a comprehensive security strategy should also include measures, such as anti-jamming technology, secure authentication mechanisms to verify the identity of communicating parties, and intrusion detection systems to monitor for suspicious activities. Together, these controls form a multi-layered defense that significantly enhances the security posture of satellite-to-earth communications, ensuring that critical information remains protected from interception, manipulation, and other cybersecurity threats.

Anti-jamming technology plays a pivotal role in safeguarding satellite communications by thwarting attempts to disrupt signal transmission through jamming. It employs techniques such as spread spectrum, which disperses the signal across a broad frequency range, making it more challenging for jammers to pinpoint and interfere with the communication channel. Frequency hopping is another effective method, where the signal rapidly shifts among different frequencies, eluding jammers that cannot adapt quickly enough to the changing transmission pattern. Additionally, beamforming technology utilizes phased array antennas to focus communication beams precisely, minimizing the signal's exposure to potential interference. These anti-jamming strategies are essential for maintaining the integrity and reliability of satellite-to-earth communications, ensuring that critical data can be transmitted without interruption, even in the presence of deliberate jamming attempts [106].

Furthermore, anti-spoofing technology is essential for defending satellite communication systems against spoofing attacks, where an adversary attempts to deceive the system by mimicking or altering the signal from a legitimate source. This technology is particularly

important for systems like GPS, where ensuring the authenticity of the signal is crucial for accurate positioning and timing. Anti-spoofing methods include cryptographic authentication, which allows a receiver to verify that the incoming signal is from a trusted source by checking for a digital signature or encrypted code that can only be provided by an authentic satellite. Additionally, integrity checks can be employed, where the receiver cross-verifies the incoming signal with other available data sources or sensors to detect anomalies. Advanced signal processing techniques can also be used to distinguish between legitimate signals and those that have been manipulated. By implementing these anti-spoofing measures, satellite communication systems can resist attempts to mislead or corrupt their data, ensuring the security and reliability of their transmissions [107].

Finally, a vital cybersecurity control for enhancing the protection of satellite-to-earth communication is the implementation of strict access control measures. These measures ensure that only authorized personnel and systems can interact with satellite communication networks and control systems. Utilizing a combination of physical and logical access control measures, such as biometric authentication, smart cards, and multi-factor authentication, can significantly reduce the risk of unauthorized access. Access control lists and role-based access control enablement to information systems grant users and entities the least privilege necessary to perform their activities. Additionally, regular reviews of access rights will help to detect any unauthorized permissions.

Summarizing, encryption, anti-jamming, and anti-spoofing mechanisms, as well as strict access control measures are some of the essential cybersecurity controls to ensure the security of satellite-to-earth communication.

6.5 Safeguarding the Security of Ground-Based Infrastructure

Attacking space systems is often easier by targeting the infrastructure of ground stations, as these stations house the necessary software and hardware to manage and monitor space objects through established networks and systems on Earth. Additionally, the user segment of space infrastructure should be considered, as it acts as a continuation of the ground segment for consumers of space-related services. This user segment can be a distributed infrastructure that offers connections to a range of applications and services capable of engaging with satellite communications directly or through interaction with additional ground segment systems. Therefore, it is of paramount importance to implement the appropriate security measures to safeguard the ground-based infrastructure.

As attacks in information technology (IT) infrastructures, the methods of compromising space systems include tactics like exploiting system misconfigurations and software flaws, obtaining unauthorized access to critical services, introducing malicious software, and using phishing techniques to acquire sensitive credentials. For example, attackers might take advantage of web security weaknesses or deceive ground station staff into installing harmful software, like Trojans, on their devices, which could then be used to hijack satellites and disrupt their operations. Additionally, altering data can lead to the issuance of incorrect commands to space assets, potentially causing inappropriate or no operation, which can lead to hazardous situations. In addition, physical security attacks, such as gaining unauthorized access to ground stations and other physical assets, can result in the disabling of the ground station, directly endangering the space mission's efficient operation, and taking control over the space assets and their services without technically attacking the systems.

In practical scenarios, vulnerabilities in ground systems or satellite data receivers can serve as pathway for attackers to infiltrate the ground network and remain undetected. A common threat is the intrusion of malware into the satellite's hardware and software,

potentially during the supply chain process, which may subsequently jeopardize the ground systems. An example of such a threat is the Turla attack, where perpetrators exploited a satellite Internet provider to steal IP addresses. This incident was challenging to be detected as it was dependent on whether the IP address was being used by both the attacker and the legitimate user at the same time. It gave the attacker the capability to inject false information to user systems linked to that IP address, leading to catastrophic outcomes like the crash of an autonomous drone. Consequently, such attacks can remain stealthy and unlikely to be detected by standard intrusion detection systems. Additionally, in June 2018, Symantec Corporation disclosed that a complex cybersecurity attack, originating from computers in China, compromised systems in satellite operators, defense contractors, and telecom firms in the United States and Southeast Asia. The incident's report disclosed that the attackers infected the computers responsible for satellite control, potentially granting them the power to alter the satellite's trajectories and disrupt data traffic [108].

Summarizing, the most common ground segment cybersecurity threats, and vulnerabilities encompass a range of malicious activities targeting the vital infrastructures and systems that underpin space operations, as well as the end-users' applications and interactions. These threats include the exploitation of misconfigurations and software vulnerabilities, which attackers leverage to gain unauthorized access to critical systems and networks. Another threat is malware injection into systems that control space operations, as well as into satellite data receivers and transmitters, compromising their integrity. Phishing attacks are frequently employed to deceive individuals into disclosing sensitive credentials, further endangering systems' security is another type of threat. Additionally, the supply chain can serve as a threat for introducing malware into components of ground station systems. Finally, beyond cyber tactics, physical attacks on ground station infrastructures pose a significant risk, potentially disrupting the operations and services of space missions.

To mitigate the threat of exploitation of misconfigurations and software vulnerabilities, indicatively vulnerabilities assessments and penetration tests should be performed on a regular and consistent basis, to identify possible existing vulnerabilities, hardened configuration standards should be formally defined and implemented based on industry standards and common best practices, as well as a structured secure software development lifecycle should be enforced and implemented to ensure that the developed software does not include any exploitable vulnerabilities. Additionally, to avoid malware injection or to timely identify any injection, continuous monitoring of space systems' logs through a Security Incident and Event Management (SIEM) solution should take place, anti-malware and anti-virus solutions should be installed to all space systems, as well as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) should be deployed to timely identify and prevent intrusions.

To eliminate the effective phishing attacks, as human is the weakest link of cybersecurity chain, appropriate training and awareness should be provided to personnel to be able to identify and not become victim of such attacks, along with email filtering solutions that could scan the emails to identify if there is malicious content. Moreover, regarding supply chain threat, a formal and structured third party risk management framework should be established and followed, including the execution of due diligence assessments to third parties to identify if a possible collaboration possesses any security related risks, along with the continuous monitoring of the provided services, the execution of audits and risk assessments to the third parties, as well as to the inclusion of cybersecurity clauses to the signed contractual arrangements. Finally, to protect the ground-based infrastructure, such as the GovSatCom Hubs, from physical security attacks appropriate physical and environmental security controls should be implemented, such as installation of cameras

and alarms to premises, installation of access control system (e.g., through access cards) and provision of access only to authorized parties, monitoring of cameras' recording on a continuous basis, deployment of fire detection and suppression systems, air conditioning, heat controllers, humidity detectors, as well as anti-flood measures.

Additionally, the growing dependence of contemporary space systems on cost-effective Commercial Off-the-Shelf (COTS) components and standardized hardware and software makes it easier for potential attackers to acquire these items and search for weaknesses. As a result, if a flaw is discovered in a single COTS component, all satellites utilizing that component become susceptible to attack. Generally, the commonly used COTS are modems, General Purpose Processors (GPPs), Operating Systems (OS), and wireless communication links. Modems utilized in SatCom systems are susceptible to denial-of-service attacks, unauthorized access, and data interception. For example, attackers could exploit vulnerabilities in the modem's firmware to gain unauthorized entry to the network or launch a Distributed Denial of Service (DDoS) attack by overwhelming the modem with an excessive amount of traffic. General Purpose Processors (GPPs), essential for signal processing and data encryption in satellite payloads and ground stations, are not custom-designed for satellite applications and could be vulnerable to side-channel attacks. Widely used operating systems, like Windows and Linux, are chosen for their accessibility and adaptability in SatCom systems, yet they lack satellite-specific security features and may contain exploitable weaknesses. Additionally, the wireless communication links that form the backbone of connectivity between satellites, ground stations, and user terminals in SatCom systems are at risk of being intercepted or disrupted by malicious attackers [94].

Consequently, it is crucial to implement robust security controls to mitigate the existing cybersecurity threats inherent in the use of COTS components. These measures should encompass appropriate management of supply chain and third-party service providers, execution of thorough security assessments / evaluations to third parties, continuous monitoring, and collection of threat intelligence to be informed about emerging threats. Both government and industry stakeholders should prioritize the incorporation of components that have been subjected to rigorous security testing and certification processes. Additionally, encryption should be a standard practice for most of the satellite communication systems, including terminals, modems, and ground stations. More specifically, regarding encryption standards, the National Institute of Standards and Technology (NIST) has issued the guidelines SP 800-131A rev2 [109] and SP 800-56A rev3 [110], which provide recommendations for cryptographic algorithms and key length selections. Administrative services need to use up-to-date protocols and should have proper security settings activated. For remote access, the preferred protocol is Secure Shell (SSH) version 2. Moreover, servers utilizing the HTTPS protocol should be configured to only allow connections using Transport Layer Security (TLS) version 1.2 or higher to guarantee secure encryption.

In summary, the security of telecommunications networks is crucial to our society and economy, as they underpin the safe functioning of vital infrastructure, government services, and transportation. Given that these networks can represent a systemic point of failure with significant safety and security risks, particularly during interruptions from natural or man-made disasters or cyber-attacks, it is imperative to put in place suitable security measures. Special attention should be given to ground-based space infrastructure, as it is a common target of threat actors, and its compromise could negatively impact the effective execution of the whole space mission.

7. ASSESSING AND SECURING THE GROUND INFRASTRUCTURE: A FRAMEWORK

7.1 Current Threat Landscape

This section presents the results of an in-depth investigation and analysis of the emerging cybersecurity threats. The threat landscape is rapidly evolving, as the attack vectors, including advanced persistent threats, nation-state actors [Figure 12], and intricate cybercriminal organisations continuously evolve [Table 3], [Image 17]. Furthermore, there is a noticeable increase in challenges driven by technological advancements, as the deployment of cutting-edge technologies introduces both opportunities and potential security weaknesses. More specifically, the key new technologies that are significant factors that shape the cybersecurity threat landscape are the quantum computing and artificial intelligence. Therefore, there is a pressing need for proactive implementation of cybersecurity measures to preemptively address these emerging threats.

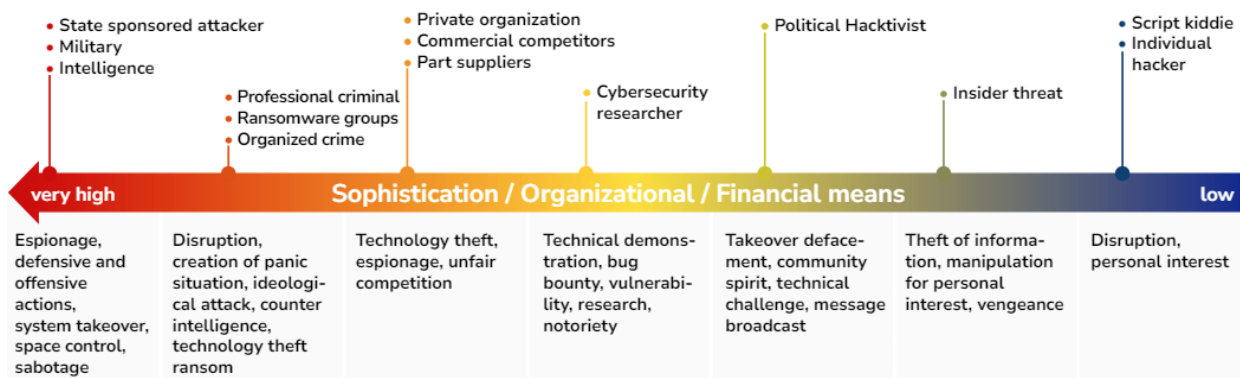


Figure 12: Overview of threat actors and their motivations [61]

Vulnerability/Attack	Common mitigations/recommendations
Lack of Encryption	• Use network encryption solutions, such as IPsec or TLS VPNs, to encrypt network communications over SAT links. • Apply mutually authenticated, encrypted TRANSEC down to the outermost vendor-proprietary transmission protocol. • Apply encryption down to and including the outermost vendor-proprietary transmission protocol. • Use point-to-point communications over IKE/IPsec-encrypted VPNs with strong authentication and key exchange methods.

Weak Authentication/Lack of Access Control	• Implement strong passwords and multi-factor authentication. • Employ RBAC and ABAC access controls. • Implement approved firewalls and network segmentation. • Change all default credentials. • Use intrusion detection and prevention systems. • Implement a need-to-know access policy.
Vulnerabilities in Software and Firmware	• Keep all IT equipment updated with the latest security patches. • Acquire updates and upgrades from trusted sources.
Cross-Site Scripting (XSS)	• Use input validation and output encoding to prevent XSS attacks. • Use Content Security Policy (CSP) to whitelist allowed sources of scripts and resources.
Brute-Force Attacks	• Implement rate limiting. • Use strong and unique passwords. • Encourage two-factor authentication. • Use CAPTCHA or similar techniques.
Jamming	• Employ frequency hopping techniques. • Use anti-jam antennas and polarization diversity. • Use commercial anti-jamming solutions.
Denial of Service (DoS)	• Employ intrusion detection and prevention systems. • Utilize commercial DoS protection solutions.
Malware and Virus	• Employ antivirus and antimalware solutions. • Use network segmentation.
Physical Threats	• Ensure physical security of SATCOM equipment and facilities. • Use tamper-evident seals. • Implement security cameras and monitoring tools. • Use hardened and ruggedized equipment. • Use secure, tamper-evident containers for transportation.

Table 3: Main cybersecurity vulnerabilities and the respective recommendations [94]

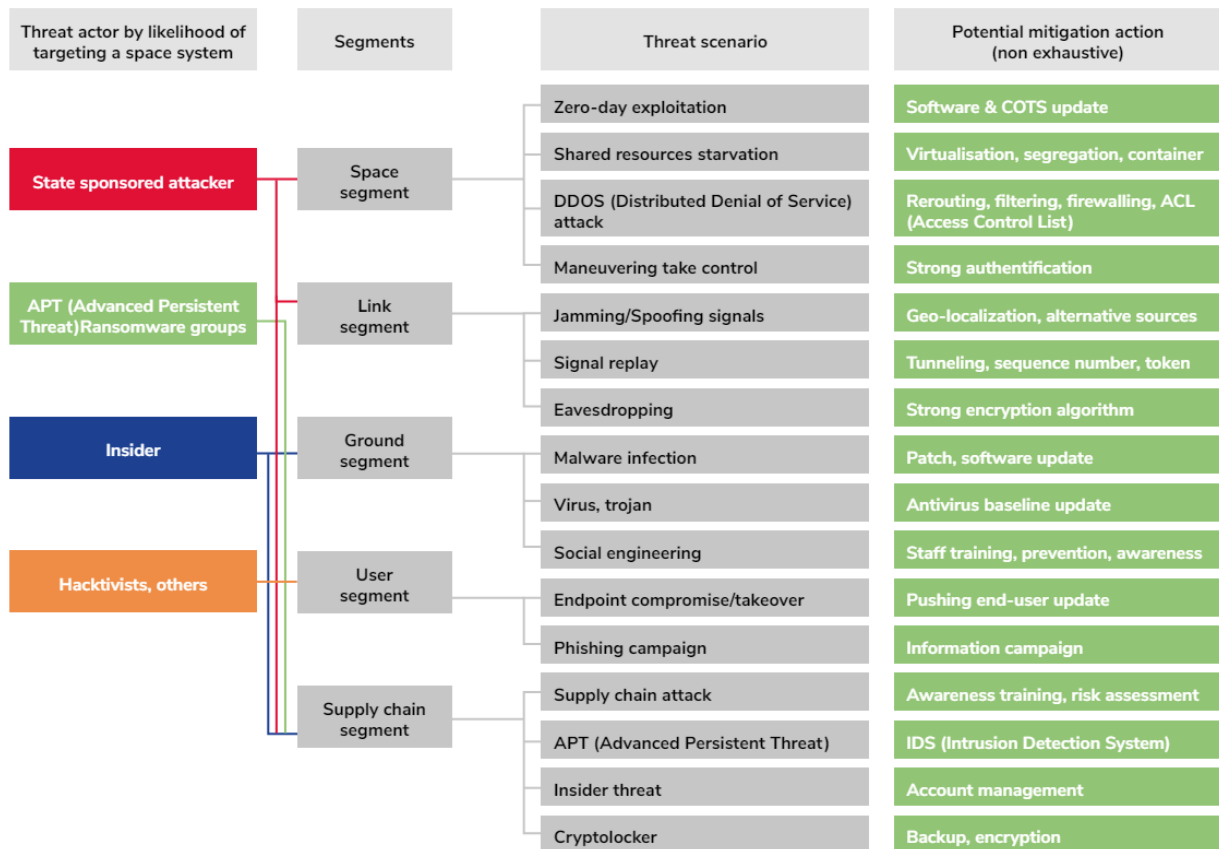


Image 17: Actual cyberattacks and potential mitigation actions examples [61]

While the cybersecurity threat landscape is ever-changing, some threats such as the compromise of supply chain software, have experienced a marginal decrease in their perceived prominence up to the year 2030, yet they continue to represent considerable risks. Furthermore, the issue of increasing digital surveillance and loss of privacy has also seen a slight reduction in both its potential impact and probability. Conversely, other threats such as shortages in cybersecurity skills, and reliance on cross-border ICT service providers as single points of failure has seen an increase in the level of concern among field experts. Finally, the probability of misuse of artificial intelligence (AI), and its role in advancing or disrupting cybersecurity attacks has risen, which aligns with expectations about extensive deployment of AI technologies and concerns about its ethical use [111].

Among the twenty (20) emerging threats until 2030 are the lack of analysis and control of space-based infrastructure and objects, as well as the attacks using quantum computing. State-sponsored attackers infiltrate space-based systems enhancing their technical prowess and establishing their presence to execute cybersecurity attacks. Their objectives include inducing malfunctions within space infrastructure as a means of state-level sabotage or to disrupt the operations and systems of other nations or commercial entities during times of geopolitical tension. Due to the overlap of private and public infrastructure in space, it is essential to scrutinize the security of these emerging infrastructures and technologies. Insufficient knowledge, examination, and management of space-based infrastructure can leave it susceptible to cybersecurity breaches. Regarding the second threat, by the year 2030, it is anticipated that quantum computing capabilities will become more broadly accessible, providing malicious entities with the opportunity to leverage these powerful computational resources to undermine the integrity of prevailing public key encryption systems. Concurrently, there exists a concern that adversaries may presently collect sensitive encrypted data with the intention of decrypt it once quantum computational technology becomes readily available [112].

In this context, some actors, including the United States and several European Union Member States, are proactively addressing these emerging cybersecurity threats by utilizing the means at their disposal. This includes strategizing the shift towards encryption methods that are resilient to quantum computing for the protection of critical data. However, to achieve a cohesive and uniform transition to such post-quantum cryptographic standards, the implementation of a new, coordinated action plan within the EU is imperative. The implementation of EuroQCI initiative will protect Europe's sensitive data and meet the current needs of the European cybersecurity landscape to respond to future quantum attacks on encryption [113].

Entities involved in the space sector are responsible for the development, operation, maintenance, or ownership of space-based systems. These systems present a greater level of complexity in terms of technological development, ownership, and management when compared to Earth-based digital systems. Cybersecurity vulnerabilities present a significant threat not only to the space assets themselves but also to terrestrial critical infrastructures that depend on them. From a technological perspective, a scenario where an adversary aims to disrupt a country's economic activities by targeting cloud services, or financial institutions could be envisaged. Nonetheless, these companies currently allocate substantial resources to cybersecurity, constantly monitoring their systems and networks against malicious activities and vulnerabilities. For a cyber adversary, a more straightforward and potentially more effective strategy might involve attacking the space infrastructures that facilitate connectivity to financial systems and services [Figure 13]. By focusing on the space entities that manage and operate the satellites enabling these services, an attacker could exploit a centralized vulnerability, thus affecting multiple systems simultaneously. This aspect renders space systems particularly appealing targets for cybersecurity attacks [101].

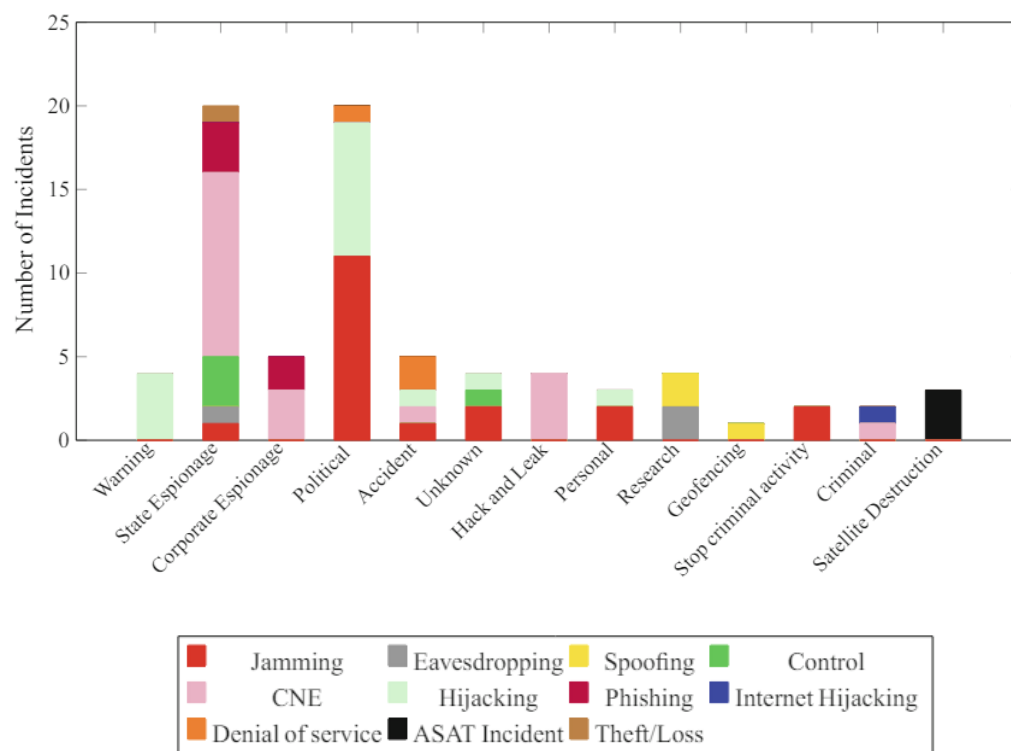


Figure 13: Motivation of satellite incidents and breakdown of used techniques [102]

In this context, space-based services have recently been included in the critical infrastructure taxonomy thanks to the NIS2 Directive. This Directive identifies the space sector as a critical entity, subjecting it to the European Union's stringent cybersecurity

requirements. The space sector will face various consequences under this Directive, as entities will be required to adhere to reporting obligations and disclose any cybersecurity incidents that could affect space infrastructure, such as satellites and ground infrastructure. Consequently, space organizations will encounter challenges in terms of monitoring, identification, and response to potential cybersecurity threats. The Directive also mandates enhanced cooperation and exchange of threat intelligence information between the space industry and regulatory authorities to pinpoint and mitigate potential cybersecurity vulnerabilities, thereby bolstering the sector's cyber defense and resilience. The NIS2 Directive also emphasizes the importance of securing the supply chain within the complex and international context of the space sector. Therefore, space organizations are encouraged to establish comprehensive supply chain risk management framework, which include the supervision of suppliers and external service providers [114].

More specifically, threats to space operations can be categorized into two (2) distinct categories [Image 18].

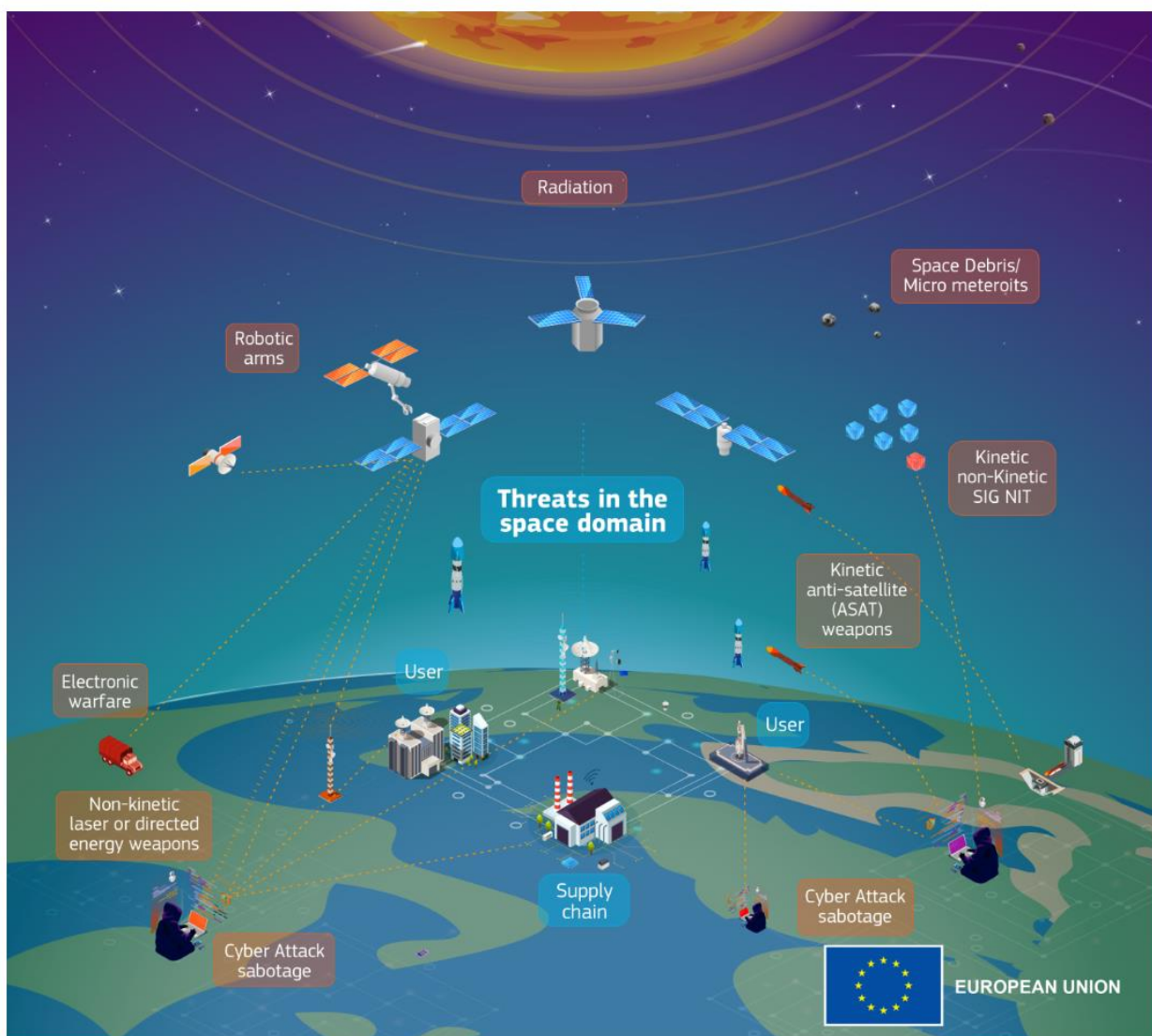


Image 18: Space threats [115]

Unintentional threats like space debris are the first. A notable incident occurred in 2009 when a satellite unintentionally collided with another, resulting in the creation of thousands of debris fragments, which was the first relevant incident in space history. With the increasing number of satellites launches by commercial entities, the issue of space congestion is becoming more pronounced, particularly with the emergence of private

space ventures. Consequently, the probability for satellite collisions and the accumulation of space debris are arising concerns. Effectively addressing these space-related threats necessitates the ability to monitor and comprehend activities within the space environment, as well as the capacity to analyze this information, design appropriate response activities, and implement them. The deliberate implementation of counterspace measures designed to hinder adversaries' space operations represents the other form of space threat. These measures are employed to intimidate adversaries and disrupt their space-based systems. They target satellites in orbit, the terrestrial infrastructure that underpins them, and the communication networks that link them. In recent years, the advancement of offensive and defensive space technologies constitutes a priority for numerous nations [116].

Summarizing, as the cybersecurity threat landscape that affect space systems continuously evolves, the appropriate cybersecurity controls should be implemented and continuously assessed to ensure their effectiveness.

7.2 Assessment Methodology

To tackle the continuously evolving cybersecurity threat landscape, as well as to adequately protect terrestrial infrastructure from cybersecurity attacks, appropriate cybersecurity controls should be implemented, as already mentioned [Figure 14].

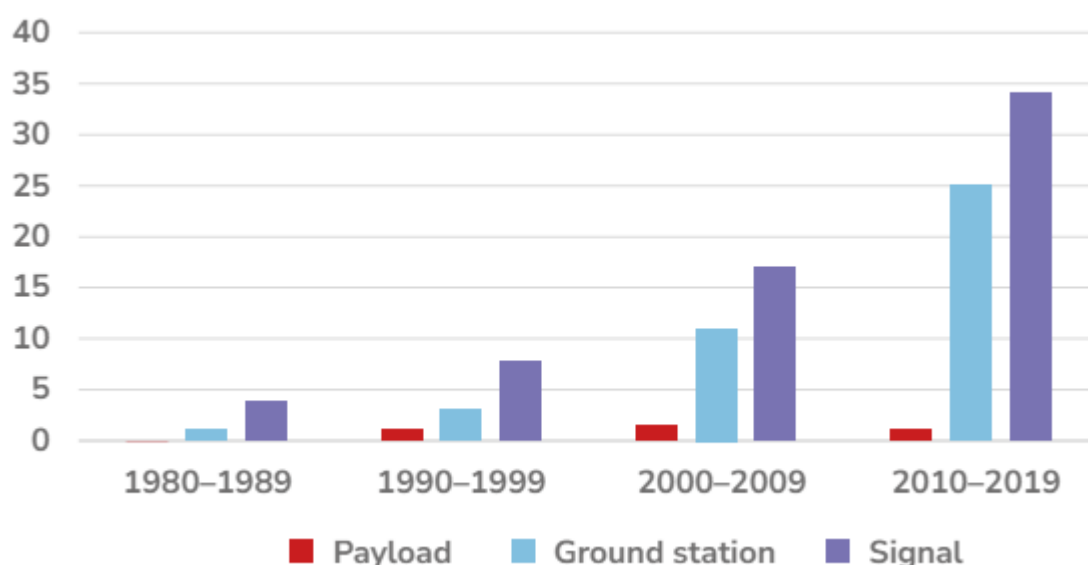


Figure 14: Evolution of cyberattacks on space systems (amount of attacks / year over the last forty years) [61]

However, to identify if adequate cybersecurity measures are in place, a structured and well-defined assessment methodology and assessment framework should be established. This methodology should include several distinct phases, each of them being critical to the overall assessment's effectiveness.

The first phase is the preparation phase, that involves the definition of the assessment's scope, identifying key infrastructure components and/or information systems that will be assessed, as well as establishing the objectives of the assessment. The next phase is the assessment phase, that the current cybersecurity measures are evaluated. This evaluation can be conducted, indicatively or at least, in respect to the assessment framework that is defined to the following section of the current Thesis. This phase aims

to identify any weaknesses or gaps in the infrastructure components and/or information systems cybersecurity defenses. During this phase, the necessary evidence, such relevant documentation, should also be collected and thoroughly reviewed.

It should be mentioned that the robustness of the implemented cybersecurity controls should be commensurate to the risk level of each assessed infrastructure component and/or information system. As satellite communication is an indispensable asset for governmental security actors, they require SatCom with high level of reliability, as well as appropriate level of protection against ill-intentioned acts. In terms of security aspects GovSatCom is positioned between the highly robust and secure MilSatCom and commercially provided ComSatCom [Figure 15] [13].

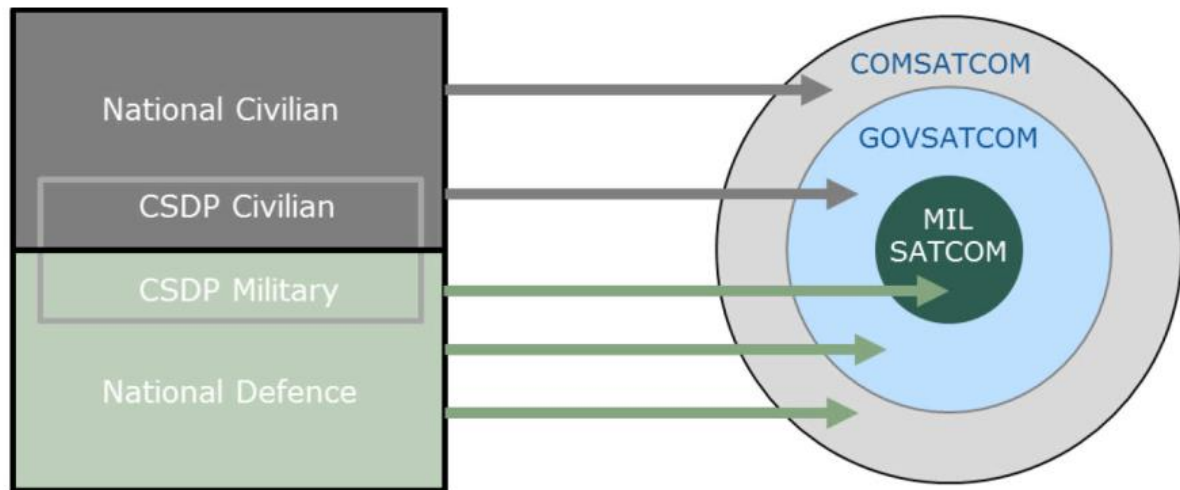


Figure 15: Tiers of satellite communications [13]

Following, the reporting phase is about communicating the findings of the assessment to relevant stakeholders. A comprehensive report should include a detailed description of identified risks and main areas for improvement, as well as strategic recommendations for their remediation. The report should be clear and actionable, enabling decision-makers to understand the risks and take appropriate decisions. Based on the assessment's results, the remediation planning phase involves the development of a plan to address the identified risks. This plan should prioritize actions based on their criticality, allocate resources, and set timelines for their implementation. It should also consider the potential impact on business operations and include contingency plans for any anticipated disruptions.

During the implementation phase, the defined remediation plan should be consistently implemented. This may involve the deployment of new cybersecurity controls, patching of identified vulnerabilities, revision of documented policies and procedures, as well as execution of training and awareness activities. Effective implementation requires coordination across different teams and clear communication channels to ensure that all stakeholders understand their roles and responsibilities. The final phase is the follow-up, which ensures that the remediation activities have been effectively implemented and that the infrastructure components and/or information systems cybersecurity posture has been enhanced. This involves monitoring of the implemented changes, performance of a post-remediation assessment, as well as addressing of any remaining issues. Continuous improvement is a key aspect of this phase, as it allows the adaptation to new threats and maintenance of a robust cybersecurity posture over time.

By following this structured methodology, a systematic cybersecurity assessment can be performed, aiming to improve the cybersecurity posture of terrestrial and/or space-based infrastructure.

7.3 Assessment Framework

This section defines an assessment framework, designed to assess the information security / cybersecurity posture of terrestrial infrastructure, such as of GovSatCom Hubs. This assessment framework is established taking into consideration the industry standards and best practices, as well as the applicable legal and regulatory requirements, such as the NISD2, ISO 27001:2022, ISO 22301:2019, NIST, and GDPR. This assessment framework includes a minimum number of questions regarding the implemented information security / cybersecurity related controls / measures, encapsulating distinct aspects of cybersecurity for assessing the cybersecurity maturity of terrestrial infrastructure. A more granular and detailed set of questions can be defined to assess the cybersecurity maturity of terrestrial infrastructure more holistically; however, this is not included in the scope of this Thesis.

Therefore, the assessment framework includes the following questions:

1. Cybersecurity Risk Management: Have you formally defined, documented, communicated, and enforced a Cybersecurity Risk Management Framework (e.g., Cybersecurity Risk Management Methodology, Cybersecurity Risk Management Procedure, and Cybersecurity Risk Management Tool) to identify potential existing cybersecurity risks to information systems of terrestrial infrastructure?
2. Cybersecurity Governance: Have you formally defined, documented, communicated, and enforced a Cybersecurity Governance Model, with clearly defined cybersecurity roles and responsibilities, reporting lines, etc. to ensure that all involved stakeholders are aware about their cybersecurity related responsibilities and duties to protect the terrestrial infrastructure against cybersecurity attacks?
3. Cybersecurity Policies and Procedures: Have you formally defined, documented, communicated, and enforced Cybersecurity Policies (e.g., Incident Response Policy, Business Continuity Policy, Logical Access Control Policy, Physical Security Policy, etc.), as well as Cybersecurity Procedures (e.g., Incident Response Procedure, User Access Management Procedure, Backup Procedure, etc.) to define the main cybersecurity principles that should be implemented to terrestrial infrastructure's information systems?
4. Cybersecurity Training and Awareness: Do you provide cybersecurity related trainings to terrestrial infrastructure's employees to raise awareness about cybersecurity best practices?
5. Cybersecurity Metrics: Do you capture, measure, and analyze cybersecurity metrics to assess the overall effectiveness of the implemented cybersecurity related controls to the terrestrial infrastructure and identify potential areas of improvement?
6. Third Party and Supply Chain Cybersecurity Risk Management: Have you formally defined, documented, communicated, and enforced a Third Party and Supply Chain Cybersecurity Risk Management Framework (e.g., Methodology, Procedure, and Questionnaire) to identify potential cybersecurity risks that may arise from collaboration of the respective third party that provides services and / or products related the operation of terrestrial infrastructure?

7. Cybersecurity Compliance: Have you identified the applicable legal and regulatory cybersecurity related requirements to ensure that the appropriate measures are taken to comply with them?
8. Data Protection and Privacy: Have you implemented the appropriate organizational [e.g., documentation of a Data Protection and Privacy Framework, execution of Data Protection Impact Assessments (DPIAs), creation of Record of Processing Activities (RoPAs), etc.] and technical (e.g., deployment of a Data Leakage Prevention (DLP) solution, encryption of sensitive data, pseudonymization, de-identification, and/or data masking of personal data, etc.) to ensure that the GDPR requirements are met, as well as that the personal data processed from the terrestrial infrastructure's information systems are properly protected?
9. Identity and Access Management: Do you provide and/or revoke identities (i.e., user accounts and passwords), and logical access rights, based on a need to know and least privileges principles, to terrestrial infrastructure's information systems based on a structured process and only to authorized stakeholders to ensure that the access to information systems are managed in a secure manner?
10. Asset Management: What capabilities / solutions are in place to discover IT assets that are connected on the network? Do you maintain and keep up to date an inventory of both physical and virtual assets that are connected on the network?
11. Physical Security: What physical security controls (including the environmental security controls) have you implemented to the terrestrial infrastructure to ensure that it is protected from physical security hazardous events?
12. Business Continuity and Disaster Recovery: Have you performed a Business Impact Analysis (BIA) exercise to identify the most critical business processes of the terrestrial infrastructure? Have you formally defined the Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and Maximum Tolerable Period of Disruption (MTPD) to identify the time and status of recovering upon a disastrous event? Have you formally defined, documented, communicated, and enforced Business Continuity Plans (BCP), Disaster Recovery Plans (DRP) and/or Crisis Management Plans (CMP) to define the process that should be followed to enable business continuity and effectively recover from a disastrous event?
13. Cloud Security: What cybersecurity measures / controls (e.g., Cloud Risk Assessment Exercise, logging, and monitoring, etc.) have you implemented to secure the cloud environment?
14. Secure Software Development: How is cybersecurity integrated into the Software Development Life Cycle (SDLC) to ensure that the developed software that is used from the terrestrial infrastructure's information systems does not contain security flaws and exploitable vulnerabilities?
15. Cybersecurity Architecture and Engineering: Which security architecture and engineering principles and standards (e.g., security by design) are adopted and implemented to ensure that terrestrial infrastructure's information systems architecture and network design is secure and appropriately protected by cybersecurity attacks?
16. Cybersecurity Infrastructure: What cybersecurity measures / controls [e.g., anti-virus, firewalls, proxies, web application firewalls, routers, network segmentation via Virtual Local Area Network (VLAN) and/or Demilitarized Zone (DMZ), patch management, backup, Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.]

have you implemented to secure the information systems' infrastructure of the terrestrial infrastructure?

17. Cybersecurity Incident Management: Have you formally defined, documented, communicated, and enforced an Incident Response Policy, and Incident Response Plan or Procedure to follow a structured process in case of a cybersecurity incident occurrence to terrestrial infrastructure's information systems to ensure effective response?
18. Cybersecurity Monitoring: Have you implemented a SIEM (Security Information and Event Management) solution, as well as established a Security Operations Center (SOC) team to monitor the alerts from the SIEM solution to timely identify possible cybersecurity incidents to the terrestrial infrastructure's information systems?
19. Vulnerability Management: Do you regularly perform penetration tests and vulnerability assessments to identify possible existing vulnerabilities? Have you formally defined, documented, communicated, and enforced a Vulnerability Management Procedure to define the process that should be followed for the identification, classification, prioritization, handling, and remediation of the identified security vulnerabilities to terrestrial infrastructure's information systems?

Summarizing, this section outlines an assessment framework to evaluate the cybersecurity posture of terrestrial infrastructure, measuring the robustness of cybersecurity protocols, resilience of information systems against cybersecurity threats, as well as the overall effectiveness of measures in place to protect such critical infrastructure from potential cybersecurity attacks.

8. CONCLUSIONS

The advantages gained from space activities have become broadly acknowledged and valued by a wide-ranging audience, resulting in a significant increase in awareness about the space industry in recent times. Space-based resources have become essential, providing global connectivity through high-speed data services, and supporting various functions, including television and news distribution, space exploration, monitoring of Earth, and navigation. Moreover, the advancement of space engineering and technology has paved the way for new prospects. In the war in Ukraine, satellite technology emerged as a pivotal element in crisis management and support of military operations, while the conflict underscored the use of sophisticated technologies and cybersecurity attacks, prompting a reevaluation of defense capabilities and tactics. Therefore, the conflict in Ukraine has underscored the security weaknesses inherent in satellite systems, emphasizing the importance of ensuring reliable access and enhancing security measures to safeguard against interference and breaches.

We are now capable of constructing and deploying a greater number of space assets equipped with sophisticated software and functionalities that enhance the gathering, analysis, and distribution of information. The fusion of space assets, data applications, and artificial intelligence is set to transform various sectors, offering opportunities for improved efficiency and innovative approaches. The seamless integration of ground and space infrastructure promises to open a world of potential and collaborative benefits, reshaping industries and fostering unprecedented innovation.

Focusing on space communications services, three (3) strategic initiatives at European level aim to enhance the operational benefits and cybersecurity posture of provided satellites communications services. More specifically, GovSatCom initiative, being already operational in some countries, aims to enable EU's Member States to share the overcapacities of their government-owned (non-military) communication satellites to provide reliable, resilient, secure, and cost-efficient satellite communication services for EU. On the other hand, the IRIS² initiative aims to provide resilient, secure, uninterrupted, and cost-effective satellite communications services through a multi-orbital satellite constellation, which will incorporate the security-by-design principle reducing the probability of realization of cybersecurity threats and risks. Additionally, IRIS² leveraging the robustness of quantum cryptography via the EuroQCI, aims to deliver unparalleled security to its users. However, in April Commissioner Bretton stated that the programme, which is considered as the EU alternative to Elon Musk's Starlink space-based communications network, faces delays.

EuroQCI is the third strategic initiative, being an integral part of IRIS² as well as of the European Cybersecurity Strategy which aims to ensure resilience to cybersecurity threats, as well as to ensure that both citizens and businesses benefit from trustworthy digital technologies. Also, the European Cybersecurity Strategy aims to ensure resilience to cybersecurity threats for its (CSDP. EuroQCI aims to protect Europe's critical infrastructure and sensitive data, safeguarding them against cybersecurity threats and ensuring the preservation of information security of vital systems, enabling secure data storage and exchange within various data centers, while ensuring data protection and privacy of governmental processed data. Overall, the vision regarding the EuroQCI infrastructure is to evolve into the backbone of Europe's Quantum Internet. These pivotal initiatives present distinct synergies and differences, such as their operational status, targeted users, geographical coverage, technological resources, and services objectives.

Considering that the threat landscape is rapidly evolving, with the threats of lack of analysis and control of space-based infrastructure and objects, as well as the attacks

using quantum computing are two of the most prevalent threats until 2030, the proactive implementation of cybersecurity measures is required to address the emerging threats. The absence of inherent security features in space systems presents an opportunity for attackers to identify and exploit weaknesses, potentially allowing them to maliciously control remote space objects. To identify if adequate cybersecurity measures are in place, a structured and well-defined assessment methodology and assessment framework should be established and consistently followed, considering the industry standards and best practices, as well as the applicable legal and regulatory requirements, such as indicatively the NISD2, ISO 27001:2022, ISO 22301:2019, NIST, and GDPR. Some of the cybersecurity pillars that should be assessed are the cybersecurity risk management, third party and supply chain cybersecurity risk management, identity and access management, physical security, business continuity and disaster recovery, incident management, security monitoring, as well as vulnerability management.

Generally, research has been conducted on cybersecurity within the satellite communications field, discovering various cybersecurity vulnerabilities. However, the new perspectives introduced by the new space paradigm, with IRIS² being a representative example, have not been thoroughly examined by researchers in terms of cybersecurity. Considering the present condition of space systems, a critical evaluation of cybersecurity enhancements is imperative to ensure the robustness of future satellite constellations. Furthermore, when specifically examining the user segment, existing studies are either not up-to-date or fail to encapsulate a holistic overview of the diverse space products. Furthermore, there has been insufficient exploration into whether the existing standards and legal requirements currently meet the existing space threats. Therefore, there is the need for increased research into the cybersecurity of space infrastructures, especially concerning the user and terrestrial components of SatCom systems. Efforts to reach a global consensus on certain "rules of the game" for space activities could help enhance the existing legal framework.

Finally, another strategic recommendation is the combination of the extensive reach of satellite networks with the agility and precision of Unmanned Aircraft Systems. IRIS² has the potential to greatly improve the efficiency of search and rescue efforts in the event of natural or human-made disasters. Access to prompt and precise information is crucial for life-saving measures post-disaster. Specifically, IRIS² could facilitate the use of coordinated Unmanned Aircraft Systems, managed through satellite communications, allowing them to cover extensive regions quickly and effectively. These Unmanned Aircraft Systems equipped with advanced technology, such as high-resolution cameras, thermal sensors, and additional detection devices, can enable them to reach areas that are otherwise unreachable for human rescue teams due to obstacles like rubble, floodwaters, or ongoing hazards. For instance, following an earthquake, IRIS² could facilitate the deployment of Unmanned Aircraft Systems to evaluate the destruction, identify secure paths for rescue personnel, and locate survivors trapped under debris. Furthermore, IRIS²'s ability to integrate with other systems could aid in utilizing Unmanned Aircraft Systems to transport critical supplies like medications, food, and water to isolated areas cut off from traditional supply lines. The synergy of IRIS² with Unmanned Aircraft Systems innovations showcases the initiative's capacity to transform disaster response tactics, converting satellite communication into an active instrument for improving the promptness, precision, and overall efficacy of emergency responses. This innovative approach not only improves survival rates in the immediate aftermath of a disaster but also supports the broader goals of resilience and recovery in the face of challenging situations.

LIST OF ABBREVIATIONS AND ACRONYMS

3GPP	3 rd Generation Partnership Project
AES	Advanced Encryption Standard
ASI	Italian Space Agency
B2B	Business-to-Business
BCP	Business Continuity Plan
C2	Command and Control
CEF Digital	Connecting Europe Facility
CHPAs	Collecting Heat Pipe Assemblies
CM16	2016 Council Meeting at Ministerial Level
CMP	Crisis Management Plan
ConOps	Concept of Operations
ConOps	Concept of Operations
COTS	Commercial Off-the-Shelf
CSDP	Common Security and Defense Policy
CSF	Cybersecurity Framework
CT	Computerized Tomography
DDoS	Distributed Denial of Service
DLP	Data Leakage Prevention
DMZ	Demilitarized Zone
DoS	Denial of Service
DPIA	Data Protection Impact Assessment
DRA	Direct Radiating Arrays
DRP	Disaster Recovery Plan
DRS	Data Relay Services

DSSPA	Dual Solid State Power Amplifier
EDA	European Defense Agency
EDRS	European Data Relay System
EEAS	European External Action Service
EEAS	European External Action Service
EGNOS	European Geostationary Navigation Overlay Service
ENISA	European Union Agency for Cybersecurity
ENTRUSTED	European Networking for satellite Telecommunication Roadmap for the governmental Users requiring Secure, inTeroperable, innovativE, and standardiseD services
ESA	European Space Agency
ESHS-WG	European Space and Human Security Working Group
ESP	European Space Policy
EU	European Union
EUCI	EU Classified Information
EUGS	Global Strategy for the European Union's Foreign and Security Policy
EuroQCI	European Quantum Communication Infrastructure
EUSPA	European Union Agency for the Space Program
EUSST	European Union Space Surveillance and Tracking
Frontex	European Border and Coast Guard Agency
FSS	Fixed Satellite Services
GaN	Gallium Nitride
GEO	Geostationary Orbit
GMOC	Government Mission Operations Centre
GovSatCom	Governmental Satellite Communications

GPPs	General Purpose Processors
GSA	European GNSS Agency
GVA	Gross Value Added
HR	High Representative
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IPS	Intrusion Prevention Systems
IRIS ²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
IT	Information Technology
KMSs	Key Management Systems
KPIs	Key Performance Indicators
LEO	Low Earth Orbit
LHPs	Loop Heat Pipes
LSA	Luxemburg Space Agency
M2M	Machine-to-Machine
MCC	Mission Control Centre
MCCM	Multichip Control Modules
MEO	Medium Earth Orbit
Meta-MCC	Secure Meta Mission Control Centre
MILSATCOM	Military Satellite Communication
MRI	Magnetic Resonance Imagery
MSS	Mobile Satellite Services
MTPD	Maximum Tolerable Period of Disruption
NATO	North Atlantic Treaty Organization

NatQCI	National Quantum Communication Infrastructure
NCSA	National Cybersecurity Agency
NDICI	Neighborhood Development and International Cooperation Instrument - Global Europe
NGOs	Non-Governmental Organizations
NIST	National Institute of Standards and Technology
NSA	National Security Authority
NTN	Non-Terrestrial Network
OS	Operating Systems
OST	Outer Space Treaty
P2P	Point-to-Point
PKI	Public Key Infrastructure
PPP	Public-Private Partnership
PQC	Post-Quantum Cryptography
PSS	Pooling and sharing
PUFs	Physically Unclonable Functions
QCI	Quantum Communication Infrastructure
QH	Quantum Hub
QKD	Quantum Key Distribution
QSIP	QCI Space Interface Point
QSIPs	Quantum Secure Interconnect Points
QSIPs	Quantum Secure Interconnect Points
RDI	Research, Development, and Innovation
ROI	Return of Investment
RoPA	Record of Processing Activities
RPAS	Remotely Piloted Aircraft Systems

RPO	Recovery Point Objective
RTO	Recovery Time Objective
Sat Cen	European Union Satellite Centre
SATCOM	Satellite Communication
SCC	Satellite Control Centre
SCCA	Secure Connectivity Competent Authority
SCCA	Secure Connectivity Competent Authority
SDLC	Software Development Life Cycle
SECTELSAT	Secure Telecom by Satellite
SIEM	Security Incident and Event Management
SMEs	Small to Medium-sized Enterprises
SNR	Signal-to-Noise Ratio
SOC	Security Operations Centre
SOC	Security Operations Center
SpaceQCI	Space Quantum Communication Infrastructure
SSA	Space Situational Awareness
SSH	Secure Shell
SUE	SpaceQCI User Equipment
TerrQCI	Terrestrial Quantum Communication Infrastructure
TLS	Transport Layer Security
TT&C	Tracking and Command
TT&C	Tracking, Telemetry, and Command
TV	television
UAV	Unmanned Aircraft Vehicle
VLAN	Virtual Local Area Network

BIBLIOGRAPHY

- [1] Euroconsult, "Satellite Connectivity and Video Market - A Euroconsult Report," Euroconsult, 2023.
- [2] P. Mancini and G. Naja-Corbin, "European Space and Human Security Working Group Report," European Space Agency, 2006.
- [3] Council of the European Union, "European Space Policy: "ESDP and Space"," Council of the European Union, Brussels, 2004.
- [4] Council of the European Union, «Outcome of proceedings of the Council (Competitiveness) on 21-22 May 2007 - Resolution on the European Space Policy,» Council of the European Union, Brussels, 2007.
- [5] E. D. General, "Agenda 2011 - A Document by the ESA Director General and the ESA Directors," ESA Communications, Netherlands, 2007.
- [6] A. Kolovos, "Enabling SATCOMs in the EU Space Programme: Setting the CSDP Priorities Straight," *European Space Policy Institute (ESPI)*, pp. 1-9, February 2016.
- [7] European External Action Service (EEAS), "Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy," European External Action Service (EEAS), 2016.
- [8] European Commission, "EU Space Programme," 18 March 2022. [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-programme_en. [Accessed 10 April 2024].
- [9] L. C. B. Sorrells, "WHITE PAPER ON SPACE BASED VULNERABILITIES OF THE EUROPEAN UNION," AWC RSS, Deterrence, 2024.

- [10] European Court of Aditors, "EU space programmes Galileo and Copernicus: services launched, but the uptake needs a further boost," Publications Office of the European Union, Luxembourg, 2021.
- [11] European Union Agency for the Space Programme (EUSPA), "GOVSATCOM," 29 April 2024. [Online]. Available: <https://www.euspa.europa.eu/eu-space-programme/secure-satcom/govsatcom>. [Accessed 30 April 2024].
- [12] European Defense Cooperation, "GOVERNMENTAL SATELLITE COMMUNICATIONS (GOVSATCOM)," [Online]. Available: [https://eda.europa.eu/what-we-do/all-activities/activities-search/governmental-satellite-communications-\(govsatcom\)](https://eda.europa.eu/what-we-do/all-activities/activities-search/governmental-satellite-communications-(govsatcom)). [Accessed 15 April 2024].
- [13] European Commission, "COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT GOVSATCOM," European Commission, Brussels, 2018.
- [14] The European Parliament, and the Council of the European Union, "REGULATION (EU) 2021/696 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations and Decision," *Official Journal of the European Union*, vol. I, no. 170/69 , pp. 1, 9, 17, 18, 19, 23, 24, 25, 27, 57, 58, 59, 60, 12 May 2021.
- [15] European Commission, "COMMISSION STAFF WORKING DOCUMENT - EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT - GOVSATCOM," European Commission, Brussels, 2018.
- [16] M. Bataille and V. Messina, "Europe, Space and Defence - From "Space for Defence" to "Defence of Space"," European Space Policy Institute (ESPI) , Vienna, 2020.
- [17] ENTRUSTED, "GOVSATCOM in action - successful demonstrations," [Online]. Available: <https://entrusted.eu/resources/demonstration/>. [Accessed 21 April 2024].

- [18] European Commission, "GOVSATCOM in a Nutshell," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom-nutshell_en. [Accessed 16 April 2024].
- [19] European Commission, "GOVSATCOM," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom_en. [Accessed 16 April 2024].
- [20] European Commission, "Background Information," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/background-information_en. [Accessed 16 April 2024].
- [21] Horizon Europe, "GOVSATCOM Service developments and demonstrations," 03 November 2022. [Online]. Available: <https://www.horizon-europe.gouv.fr/govsatcom-service-developments-and-demonstrations-31477>. [Accessed 21 April 2024].
- [22] European Commission, "Objectives & Benefits," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/objectives-benefits_en. [Accessed 16 April 2024].
- [23] European Commission, "Potential Users," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/potential-users_en. [Accessed 21 April 2024].
- [24] European Commission, "Applications & Services," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/applications-services_en. [Accessed 21 April 2024].
- [25] European Commission, "Support to key infrastructure management and diplomatic communication networks," 27 April 2021. [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/support-key-infrastructure-management-and-diplomatic-communication-networks_en. [Accessed 21 April 2024].
- [26] European Commission, "Support to Border Surveillance and Maritime Surveillance Operations," 27 April 2021. [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/support-border-surveillance-and-maritime-surveillance-operations_en. [Accessed 21 April 2024].

- industry-space.ec.europa.eu/document/download/3fd7ed11-b5e0-4e0a-91ac-cbeedd7f46cd_en?filename=DEFIS_EU_SPACE_GOVSAT%20-%20Border%20Maritime%20Surveillance.pdf. [Accessed 21 April 2024].
- [27] European External Action Service (EEAS), "High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM)," Council of the European Union, Brussels, 2017.
- [28] Directorate-General for Defence Industry and Space, "GOVSATCOM System Overview," 27 April 2021. [Online]. Available: https://defence-industry-space.ec.europa.eu/document/download/cd9a1eb9-3ed6-4473-8b5b-6cefc1028893_en?filename=DEFIS_EU_SPACE_GOVSAT%20-%20Overview.pdf. [Accessed 21 April 2024].
- [29] European Commission, "Support to Crisis Management Operations," [Online]. Available: https://defence-industry-space.ec.europa.eu/govsatcom/support-crisis-management-operations_en. [Accessed 21 April 2024].
- [30] European Union Agency for the Space Programme (EUSPA), "Major consultation underway with prospective GOVSATCOM users," 08 December 2022. [Online]. Available: <https://www.euspa.europa.eu/newsroom-events/news/major-consultation-underway-prospective-govsatcom-users>. [Accessed 21 April 2024].
- [31] European Commission, "How it works," 27 April 2021. [Online]. Available: https://defence-industry-space.ec.europa.eu/document/download/60fa3896-a5da-432c-85ba-eb4cae32a67c_en?filename=DEFIS_EU_SPACE_GOVSAT%20-%20How%20it%20works.pdf. [Accessed 21 April 2024].
- [32] Connectivity & Secure Communications, "Next Generation Secure Satellite Network," 14 June 2024. [Online]. Available: <https://connectivity.esa.int/projects/ngssn>. [Accessed 15 June 2024].
- [33] HELLENIC REPUBLIC MINISTRY OF DIGITAL GOVERNANCE GENERAL SECRETARIAT OF TELECOMMUNICATIONS AND POSTS, "Greek Initiative Announcement of Opportunity under the ESA ARTES Space Systems for Safety

& Security (4S) Strategic Programme Line," HELLENIC REPUBLIC MINISTRY OF DIGITAL GOVERNANCE GENERAL SECRETARIAT OF TELECOMMUNICATIONS AND POSTS, Athens, 2020.

- [34] R. Heron, "GOVSATCOM SERVICES - Bringing to market secure, innovative and guaranteed satellite communications for governments and institutions," SES Networks, 2018.
- [35] B. Rafał, H. Kaja and C. Paweł, "GOVSATCOM makes the EU stronger on security and defence," *Security & Defence*, vol. 28, no. 4.0, pp. 47-48, 16 March 2020.
- [36] HISDESAT SERVICIOS ESTRATÉGICOS, S.A., "PACIS 3," HISDESAT SERVICIOS ESTRATÉGICOS, S.A., Madrid.
- [37] A. Matina, "PACIS 5 - A technology demonstrator for the GOVSATCOM Secure Pooling & Sharing system," Airbus, 2019.
- [38] The European Space Agency, "Govsatcom Precursor 'Pacis-5' project to demonstrate satcom sharing system," 23 January 2020. [Online]. Available: <https://connectivity.esa.int/news/govsatcom-precursor-%E2%80%99pacis5%E2%80%99-project-demonstrate-satcom-sharing-system>. [Accessed 28 April 2024].
- [39] Immarsat, "Govsatcom Precursor Pacis-6 contract signed with Inmarsat," 10 April 2018. [Online]. Available: <https://www.inmarsat.com/en/news/latest-news/government/2018/govsatcom-precursor-pacis-6-contract-signed-with-inmarsat.html>. [Accessed 28 April 2024].
- [40] Immarsat, "PACIS-6 GOVSATCOM Precursor," Immarsat, 2018.
- [41] European Commission, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Union Secure Connectivity Programme for the period 2023-2027," European Commission, Strasbourg, 2022.
- [42] Information Portal for Funding Programmes, "EU GOVSATCOM for a safer and more secure EU," 26 October 2023. [Online]. Available:

<https://www.fundingprogrammesportal.gov.cy/en/call/eu-govsatcom-for-a-safer-and-more-secure-eu/>. [Accessed 06 May 2024].

- [43] C. Evroux, "EU secure connectivity programme 2023-2027 - Building a multi-orbital satellite constellation," European Parliamentary Research Service (EPRS), 2023.
- [44] European Commission, "Space: Commission invites the industry to submit proposals to deploy the new EU secure connectivity satellite constellation, IRIS²," 24 March 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1882. [Accessed 12 June 2024].
- [45] A. K. Kolovos, "Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict," *ResearchGate*, no. 3, pp. 3, 8, 17, 18, 19, 20, 22, 30, 31, February 2023.
- [46] E. C. / C. o. t. E. Union, "A Strategic Compass for a stronger EU security and defence in the next decade," 21 March 2022. [Online]. Available: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>. [Accessed 06 July 2024].
- [47] European Commission, "Welcome IRIS²: Infrastructure for Resilience, Interconnectivity and Security by Satellite," 17 November 2022. [Online]. Available: https://defence-industry-space.ec.europa.eu/welcome-iris2-infrastructure-resilience-interconnectivity-and-security-satellite-2022-11-17_en. [Accessed 2 June 2024].
- [48] European Commission, "IRIS² Industry Information Day," European Commission, Brussels, 2023.
- [49] O. BOMSEL and A. DAGICOUR, "Space Fordism and Europe," *Fondation Robert Schuman - Policy Paper*, vol. N°676, p. 4, 11 July 2023.

- [50] European Commission, "IRIS²: Save the date for an Information day on a call for tender," 23 March 2023. [Online]. Available: https://defence-industry-space.ec.europa.eu/iris2-save-date-information-day-call-tender-2023-03-23_en. [Accessed 02 June 2024].
- [51] European Commission, "IRIS²: the new EU Secure Satellite Constellation," [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en. [Accessed 02 June 2024].
- [52] European Space Policy Institute (ESPI), "IRIS2: The new (material) girl on the block," European Space Policy Institute (ESPI), Vienna, 2022.
- [53] B. Neuro, "EU To Counter Elon Musk's Starlink With A Multi-Billion Euro Satellite System," 26 January 2024. [Online]. Available: <https://www.benzinga.com/news/24/01/36796522/eu-to-counter-elon-musks-starlink-with-a-multi-billion-euro-satellite-system>. [Accessed 06 July 2024].
- [54] P. B. D. Selding, "Iris2 constellation and proposed EU Space Law, already behind schedule, face further delays with EU elections," 10 April 2024. [Online]. Available: <https://www.spaceintelreport.com/iris2-constellation-and-proposed-eu-space-law-already-behind-schedule-face-further-delays-with-eu-elections/>. [Accessed 06 July 2024].
- [55] J. POSANER, "Brussels slams Berlin's 'ill-founded' effort to delay EU satellite project," 01 May 2024. [Online]. Available: <https://www.politico.eu/article/iris-2-eu-satellite-project-germany-delay/>. [Accessed 06 July 2024].
- [56] European Space Policy Institute (ESPI), "Space Spectrum Management: Foundations for an informed policy discussion towards WRC-23 and beyond," European Space Policy Institute (ESPI), Vienna, 2023.
- [57] European Commission, "Commission welcomes political agreement to launch IRIS², the Union's Secure Connectivity Programme," 17 November 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6952. [Accessed 04 June 2024].

- [58] European Commission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative," European Commission, 18 April 2024. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>. [Accessed 08 May 2024].
- [59] R. J. STEINER, "How EuroQCI supports the uptake of QC in the EU/QT communications," European Commission, Munich, 2023.
- [60] J.-B. Laithier, "IRIS2 : A new LEO constellation competitor ?," Euroconsult Group, 2023.
- [61] R. d. Costa, "EUSPA Secure SATCOM - Market and User Technology Report," Publications Office of the European Union, Luxembourg, 2023.
- [62] EU Global Action on Space, "Making the best of satellite connectivity: how IRIS² can bring Europe and Africa closer together," 19 October 2023. [Online]. Available: <https://eu-global-space.eu/news-media/making-best-satellite-connectivity-how-iris2-can-bring-europe-and-africa-closer-together>. [Accessed 08 June 2024].
- [63] Copernicus, "IRIS2 Ambassadors," [Online]. Available: <https://www.copernicus.eu/en/node/48667>. [Accessed 08 June 2024].
- [64] European Space Agency (ESA), "IRIS2 PHASE 1 USER TERMINAL SECURITY TESTBED," 06 November 2023. [Online]. Available: <https://esastar-publication-ext.sso.esa.int/ESATenderActions/details/69723>. [Accessed 09 June 2024].
- [65] J. Williams, "EU launches Nostradamus – prepares Europe for a quantum world," 16 January 2024. [Online]. Available: <https://www.telekom.com/en/media/media-information/archive/eu-launches-nostradamus-prepares-europe-for-a-quantum-world-1056746>. [Accessed 09 June 2024].
- [66] G. Tricco, "The upcoming of Iris2: Bridging the digital divide and strengthening the role of the EU in International Space Law," *Journal of Law, Market & Innovation*, vol. 2, no. 2/2023, pp. 18, 19, 28, 29, 30, 31, 32, 33, 34, 35, 31 July 2023.

- [67] European Union, "COOPERATION AGREEMENT between the European Union and the Agency for Aerial Navigation Safety in Africa and Madagascar (ASECNA) on the development of satellite navigation and the provision of associated services in ASECNA's area of competence," *Official Journal of the European Union*, pp. 4-9, 26 October 2018.
- [68] Copernicus, "OBSERVER: Copernicus gets sibling— IRIS², the new EU Secure Communication Constellation," 16 February 2023. [Online]. Available: <https://www.copernicus.eu/en/news/news/observer-copernicus-gets-sibling-iris2-new-eu-secure-communication-constellation>. [Accessed 09 June 2024].
- [69] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "REGULATION (EU) 2023/588 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027," *Official Journal of the European Union*, vol. L, no. 79/1, pp. 2, 3, 4, 5, 7, 12, 14, 15, 16, 17, 20, 21, 22, 28, 33, 34, 35, 17 March 2023.
- [70] HellasQCI - Quantum Communication Infrastructure for Greece, "Frequently Asked Questions," [Online]. Available: <https://hellasqci.eu/frequently-asked-questions-faq/>. [Accessed 08 May 2024].
- [71] HellasQCI - Quantum Communication Infrastructure for Greece, "A Brief overview of the EuroQCI Thematic Working Group Meeting," [Online]. Available: <https://hellasqci.eu/a-comprehensive-report-on-the-euroqci-thematic-working-group-meeting-etwg-in-brussels/>. [Accessed 08 May 2024].
- [72] Quantum Flagship, "Quantum Communication Infrastructure - Europe's Quantum Communication Infrastructure initiative - EuroQCI," [Online]. Available: <https://qt.eu/ecosystem/quantum-communication-infrastructure>. [Accessed 08 May 2024].
- [73] E. Commission, "The Cybersecurity Strategy," 07 June 2022. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>. [Accessed 06 July 2024].

- [74] European Commission, "EU Cybersecurity plan to protect open internet and online freedom and opportunity," European Commission, Brussels, 2013.
- [75] F. Mogherini and M. Kunasek, "The Common Security and Defence Policy of the European Union," Federal Ministry of Defence of the Republic of Austria, Vienna, 2019.
- [76] European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," European Commission, Brussels, 2017.
- [77] E. COMMISSION, "The EU's Cybersecurity Strategy for the Digital Decade," 16 December 2020. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>. [Accessed 06 July 2024].
- [78] European Commission, "Quantum Technologies Flagship," European Commission, 19 December 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>. [Accessed 08 May 2024].
- [79] OPENQKD, "Truly secure quantum communication is here," [Online]. Available: <https://openqkd.eu/>. [Accessed 08 May 2024].
- [80] Petrus - EuroQCI, "PETRUS Project," [Online]. Available: <https://petrus-euroqci.eu/>. [Accessed 12 May 2024].
- [81] Horizon Europe, a programme of the European Union, "EU-FUNDED SPACE R&I - BE PART OF THE COMPETITIVE EU SPACE INDUSTRY AND DEVELOP CUTTING EDGE SPACE TECHNOLOGY," Horizon Europe, a programme of the European Union, [Online]. Available: https://www.euspaceweek.eu/system/files/2023-10/DEFIS_B2_CommsKit_brochure_v2.pdf . [Accessed 14 June 2024].

- [82] The European Space Agency, "Eagle-1," [Online]. Available: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1. [Accessed 08 May 2024].
- [83] European Commission, "The future is quantum: EU countries plan ultra-secure communication network," European Commission, 31 January 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>. [Accessed 11 May 2024].
- [84] D. I. Papastamatiou, "HellasQCI and EuroQCI, emerging technologies and infrastructures for Quantum Key Distribution (QKD)," GRNET, Athens, 2023.
- [85] European Commission, "Quantum communication infrastructure (EuroQCI)," European Commission, [Online]. Available: https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about/quantum-communication-infrastructure-euroqci_en?prefLang=fr. [Accessed 12 May 2024].
- [86] Quantum Flagship, "Quantum Key Distribution (QKD)," [Online]. Available: <https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd>. [Accessed 12 May 2024].
- [87] M. N. S. R. J. M. M. P. A. A. V. M. S. S. A. P. C. P. a. M. V. M. Mehic, "Quantum Key Distribution: A Networking Perspective," *ACM Computing Surveys*, vol. 53, no. 5, pp. 3, 4, 28 September 2020.
- [88] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, pp. 3-5, 18 January 2022.
- [89] R. J. STEINER, "EuroQCI Concept of Operations (ConOps)," European Commission, Brussels, 2023.
- [90] European Commission, "Testing and Evaluation Infrastructure for European Quantum Communication Infrastructure (EuroQCI)," European Commission, 05 July 2023. [Online]. Available: <https://digital->

strategy.ec.europa.eu/en/funding/testing-and-evaluation-infrastructure-european-quantum-communication-infrastructure-euroqci. [Accessed 13 May 2024].

- [91] National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," National Security Agency, [Online]. Available: <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>. [Accessed 18 May 2024].
- [92] M. A. D. Oliveira, "Quantum cryptography with structured light," University of the Witwatersrand, Johannesburg, 2020.
- [93] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang and Q. Wang, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43-47, 18 August 2017.
- [94] F. Casaril and L. Galletta, "Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2," *ScienceDirect*, vol. 140, no. 103799, pp. 3-10, May 2024.
- [95] Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default," 2023.
- [96] B. Butler, "PROTECTED SATELLITE COMMAND AND CONTROL (C2) WAVEFORMS AND ENHANCED SATELLITE RESILIENCY," 34th Space Symposium, Colorado, United States of America, 2018.
- [97] S. S. Saha, S. Rahman, M. U. Ahmed and S. K. Aditya, "Ensuring Cybersecure Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 8, pp. 34 - 49, 01 August 2019.
- [98] O. W. Hoernig and D. R. Sood, "Command System Protection for Commercial Communication Satellites," *MILCOM 1986 - IEEE Military Communications*

Conference: Communications-Computers: Teamed for the 90's, pp. 1-6, 27 March 2009.

- [99] K. W. Ingols, "Design for security: Guidelines for efficient, secure small satellite computation," *2017 IEEE MTT-S International Microwave Symposium (IMS)*, pp. 3-7, 05 October 2017.
- [100] G. Falco, "When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience," *Aerospace Research Central (ARC)*, pp. 2-10, 02 November 2020.
- [101] M. Scholl and T. Suloway, "Introduction to Cybersecurity for Commercial Satellite Operations," National Institute of Standards and Technology, Gaithersburg, 2023.
- [102] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar and A. Davis, "Cyber security in New Space - Analysis of threats, key enabling technologies and challenges," *International Journal of Information Security*, pp. 1, 2, 6, 7, 8, 10, 12 May 2020.
- [103] S. Salim, N. Moustafa and M. Reisslein, "Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments," *IEEE Communications Surveys*, pp. 1-7, 03 June 2024.
- [104] D. Housen-Couriel, "IAC-21-E-9 (Paper ID: 67116) Information sharing for the mitigation of outer space-related cybersecurity threats," *ScienceDirect*, vol. 203, pp. 546-550, February 2023.
- [105] V. Varadharajan and N. Suri, "Security challenges when space merges with cyberspace," *ScienceDirect*, vol. 67, pp. 1-9, February 2024.
- [106] C. Han, A. Liu, L. Huo, H. Wang and X. Liang, "Anti-Jamming Routing For Internet of Satellites: a Reinforcement Learning Approach," *IEEE Communications Surveys*, pp. 3-7, 09 April 2020.
- [107] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," *IEEE Communications Surveys*, vol. 8, pp. 165444 - 165496, 07 September 2020.

- [108] V. Varadharajan and N. Suri, "Security challenges when space merges with cyberspace," *ScienceDirect*, vol. 67, no. 101600, pp. 2, 3, 4, February 2024.
- [109] E. Barker and A. Roginsky, "NIST SP 800-131A Rev. 2 - Transitioning the Use of Cryptographic Algorithms and Key Lengths," *NIST*, pp. 1-5, March 2019.
- [110] E. Barker, L. Chen, A. Roginsky, A. Vassilev and R. Davis, "NIST SP 800-56A Rev. 3 - Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography," *NIST*, pp. 1-5, April 2018.
- [111] R. Mattioli and A. Malatras, "FORESIGHT CYBERSECURITY THREATS FOR 2030 - UPDATE," EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), 2024.
- [112] J. Lepassaar, "FORESIGHT 2030 THREATS," European Union Agency for Cybersecurity (ENISA), 2024.
- [113] A. G. Rodríguez, "A quantum cybersecurity agenda for Europe - Governing the transition to post-quantum cryptography," European Policy Centre, Brussels, 2023.
- [114] E. Union, Ed. "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," *Official Journal of the European Union*, pp. 9, 14, 39, 67, 27 December 2022.
- [115] European Commission, "EU Space Strategy for Security and Defence for a stronger and more resilient European Union," European Commission, [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en. [Accessed 29 June 2024].
- [116] S. Clapp and C. Evroux, "EU space strategy for security and defence," European Union, 2023.