LUISS

Department of Political Science
Master's Degree in International Relations

Course of The New Geopolitics of Cyberspace, Intelligence, Surveillance and New Technologies

The European Space Sector as a Pillar of Strategic Autonomy: The Case of Hybrid Threats

Prof. Alfonso Giordano
SUPERVISOR

Prof. Andrea Capati
CO-SUPERVISOR

Alexandre Touati (655822)
CANDIDATE

Academic Year 2024/2025

Table of Contents

List of Abbreviations

4S – 4S

AGS – Ground Surveillance System

AI – Artificial Intelligence

AIS – Automatic Identification System

APSS – Allied Persistent Surveillance from Space

ASAT – Anti-Satellite

ASI – Agenzia Spaziale Italiana

AWACs – Airborne Warning and Control Systems

BRO – Breizh Reconnaissance Orbiter

C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CBSS – Coperncus Border Surveillance Service

CCMs – Copernicus Contributing Missions

CFSP – Common Foreign and Security Policy

CMSS – Copernicus Maritime Surveillance Service

CNES – Centre National d'Études Spatiales

CoHGI – Common Hub for Governmental Imagery

CSDP – Common Security and Defence Policy

CSpOC – U.S. Strategic Command Combined Space Operations Centre

DEWs – Direct Energy Weapons

DG DEFIS – Directorate-General for Defence Industry and Space

DIANA – Defence Innovation Accelerator for the North Atlantic

DLR – Deutsches Zentrum für Luft- und Raumfahrt

ECMWF – European Centre for Medium-Range Weather Forecasts

ECR – European Conservatives and Reformists

EDF – European Defence Fund

EEAS – European External Action Service

EFA – European Free Alliance

EFTA – European Free Trade Association

EIBM – European Integrated Border Management

ELINT – Electronic Intelligence

EMSA – European Maritime Safety Agency

EMPs – Electromagnetic Pulses

EO – Earth Observation

EOGS – Earth Observation Governmental Service

EPP – European People's Party

ESA – European Space Agency

ESPI – European Space Policy Institute

EU – European Union
EUMETSAT – European Organisation for the Exploitation of Meteorological Satellites
EUSPA – European Union Agency for the Space Programme
EUSSSD – European Union Strategy for Space and Defence
FOPEN – Foliage-Penetration
FSB – Federal Security Service
GEO – Geostationary Earth Orbit
GEOINT – Geospatial Intelligence
GMES – Global Monitoring for Environment and Security
GNSS – Global Navigation Satellite System
GPS – Global Positioning System
GRU – Main Intelligence Directorate
GSA – European GNSS Agency
HAPS – High Altitude Platform Systems
HEO – Highly Elliptical Orbits
HR/VP – High Representative / Vice-President
Hybrid CoE – European Centre of Excellence for Countering Hybrid Threats
IAMD – Integrated Air and Missile Defence
IHL – International Humanitarian Law
IMINT – Imagery Intelligence
InSAR – Interferometric Synthetic Aperture Radar
IR – Infrared
IRS – Indian Remote Sensing
ISRO – Indian Space Research Organisation
ISR – Intelligence, Surveillance, and Reconnaissance
JRC – Joint Research Centre
KE-ASATs – Kinetic Energy Anti-Satellite Weapons
LEO – Low Earth Orbit
LIDAR – Light Detection and Ranging
LSA – Luxembourg Space Agency
MDA – Maritime Domain Awareness
MEO – Medium Earth Orbits
MFF – Multiannual Financial Framework
MUSIS – Multinational Space-based Imaging System
NATO – North Atlantic Treaty Organization
NOAA – National Oceanic and Atmospheric Administration
OECD – Organisation for Economic Co-operation and Development
PESCO – Permanent Structured Cooperation
PNT – Positioning, Navigation, and Timing
PO – Polar Orbits

PPP – Public-Private Partnership
PRS – Public Regulated Service
R&D – Research and Development
RF – Radio Frequency
S&D – Progressive Alliance of Socialists and Democrats
SAR – Synthetic Aperture Radar
SAT-AIS – Satellite Automatic Identification System
SatCen – European Union Satellite Centre
SATCOM – Satellite Communications
SESA – Space for Europe's Security and Defence Action
SIGINT – Signals Intelligence
SOCINT – Social Media Intelligence
SSA – Space Situational Awareness
SSO – Sun-Synchronous Orbits
SST – Space Surveillance and Tracking
SVR – Foreign Intelligence Service
UHR – Ultra-High Resolution
UNIDIR – United Nations Institute for Disarmament Research
VHR – Very High Resolution
VLEO – Very Low Earth Orbit

1. Introduction

The return of the Trump presidency and the subsequent realization that Europe must assume primary responsibility for its own defence, have fundamentally challenged the transatlantic link. This shift, completed by the inherent unpredictability of contemporary geopolitics (Golovtchenko, 2026), has forced European policymakers to prioritize a vision of autonomous capabilities designed to reduce reliance on external providers for critical technologies. Originally championed by French strategic thought, the concept of strategic autonomy has be slowly adopted by the European Union and its various institutions (Cellerino, 2023; Libek, 2019; Varma, 2024). Space policy serves as a primary vehicle for this transition, the development of Galileo established a precedent for sovereign assets for Global Navigation Satellite System (GNSS) technologies (Giegerich, 2007; Lewis, 2004; Lindström & Gasparini, 2003), accelerated by current initiatives encouraging the development of the New Space providers to build localized infrastructure for European clients. With the publication of the *EU Space Strategy for Security and Defence*, the continent has signalled a definitive pivot security applications in space. This move represents a departure from a purely environmental focus toward the integration of cutting-edge technologies specifically tailored for security applications under the umbrella of dual use.

Regarding the evolving threat landscape, the proliferation of hybrid warfare since the concept was popularized by Hoffman (2007), has challenged European resilience against both kinetic and non-kinetic means. Recent vulnerabilities in critical infrastructure highlighted a strong dependence on non-European actors for energy and industrial inputs (Gross & Stelzenmüller, 2024), often leaving vital sectors of the economy vulnerable, against hybrid threats and Gray-zone aggression. Consequently, European security providers are increasingly forced to develop their capacity to respond to these threats. While these countermeasures involve traditional forces and tools, there is a distinct trend toward developing sophisticated Intelligence, Surveillance, and Reconnaissance (ISR) into existing methodologies: as a matter of fact, such capabilities are deemed essential to detect, attribute, and deter hybrid threats (Crosetto, 2025; Gannon et al., 2022; Gartzke & Lindsay, 2024; Pischedda et al., 2024; Van, 2017). In the field of ISR, Space plays a significant role, and the development of space-based ISR serves to project European

power, demonstrating a renewed capacity to defend territories and citizens against the strategic competition posed by Gray-zone aggressors such as Russia and China.

While a significant body of literature has explored European strategic autonomy in the space domain (Cellerino, 2023; Fiott, 2018, 2020, 2021a, 2021b; Franzoso, 2024; Patarin-Jossec, 2020; Reillon, 2017; Van Camp & Peeters, 2022) as well as the mechanisms of resilience against hybrid threats (Capaul, 2024; Giannopoulos et al., 2021; Hartmann, 2017; Jungwirth et al., 2023; Linkov et al., 2019; Olech, 2025; Pillai, 2023; Schroefl, 2022; Treverton et al., 2018), this research addresses a distinct, two sided gap in literature. Although several scholars have examined the how space is subject to threats from hybrid warfare (Fiott, 2021a; Reis, 2025), there remains a notable absence of research detailing the concrete deployment of space assets to build resilience against hybrid threats on earth. Existing studies do not present a rigorous, quantitative diagnostic of European capabilities in space, in particular in the field of Earth Observation; while such data exists within fragmented public repositories, it lacks the necessary analysis to correlate technological specifications with specific security applications. Therefore, this study will fill the gap between Earth Observation technical capacities and their practical utility against the contemporary hybrid threats.

The current research seeks to clarify how European space-based systems facilitate the detection, attribution, and mitigation of a broad spectrum of hybrid threats to Europe, extending the analysis beyond threats isolated to the space domain itself. By prioritizing the integration of Earth Observation and geospatial intelligence into broader European defence architectures, the study evaluates the degree to which these European assets diminish dependence on external security providers. The central research question asks: **To what extent does European strategic autonomy in space contribute to strengthening resilience against hybrid threats?** In addressing this, the thesis shifts away from the main topic of research analysing the vulnerability of space assets and how they require protection, but as proactive tool for persistent surveillance that is essential for securing the European continent against unconventional threats.

To address this research question, the study adopts a mixed-methods approach that integrates quantitative analysis with qualitative case studies. The first level identifies

political will and market dynamics to gauge the current level of European strategic autonomy in space, while the subsequent level utilizes empirical data (Lin et al., 2024; Union of Concerned Scientists, 2023) to determine the specific capacities in Earth observation available to European security providers. Understanding how space-based assets affect resilience against hybrid threats forms the central part of the second phase, which evaluates three specific cases of hybrid threats that Europe faced over the last decade. These data streams are further enriched by two semi-structured interviews with experts from the European Space Agency and the World Economic Forum, providing a nuanced perspective on the public-private partnerships defining the sector and the newest development in space.

The structure of this research is as follows, the first part develops a rigorous literature review concerning strategic autonomy, hybrid threats, and the use of space for security application, tracing their evolution over the past years. This theoretical grounding is organized into three distinct sections. First, the analysis focuses on the role of space within the broader framework of European strategic autonomy, examining the potential for emancipation through the lens of dual-use technologies. The second section establishes the theoretical foundations of the dependent variable by reviewing the literature on hybrid threats and defining what resilience against hybrid threats means. This includes a conceptual debate on detection, attribution, and deterrence. Finally, the third section examines what remote sensing from space is and how space technologies for earth observation can be used against hybrid threats.

The second section provides a detailed overview of the adopted research methodology, the overarching research design, and the theoretical framework of strategic autonomy in space. This framework developed by Fiott (2020) is segmented into three distinct branches that structure the subsequent analysis. It is the followed by an introduction to the case studies and the description of the analytical process through a case study matrix, concluding with an evaluation of the research limitations. In the third section, strategic autonomy in space is assessed through its three levels. First, it examines official strategies and publications to understand Europe's political will to achieve strategic autonomy in space, while the second branch analyses the European space market, with a specialized focus on Earth Observation technologies, to determine its current health and future evolutions. The third branch builds a capacity assessment by

comparing European Earth Observation capabilities against those of primary foreign competitors. The final part presents three case studies via the conceptual model of Giannopoulos et al. (2021) illustrating diverse applications of Earth Observation in mitigating hybrid threats. These include the sabotage of the Nord Stream pipelines as a kinetic action, the weaponization of migration at the European eastern border as a disruptive threat mechanism, and the jamming and spoofing of GNSS as a non-kinetic destabilisation operation.

2. Strategic Autonomy and Hybrid Threats

To lay the foundations for the assessment of how Europe's strategic autonomy in space contributes to strengthening resilience against hybrid threats, it is necessary to define the central independent variable used in this research. To this end, this chapter will present the academic debate surrounding strategic autonomy and will then move to the role of strategic autonomy in the space domain. To subsequently assess its impact, the second part of the chapter will define hybrid threats and examine their impact on Europe to date, while highlighting the importance of resilience against these threats. Finally, this chapter will provide context on the European space sector by identifying its actors, dependencies, and fragmentation in both the public and private sectors.

2.1. Strategic Autonomy in Space

2.1.1. Strategic Autonomy as a Concept

At the centre of this research lies the concept of strategic autonomy. This concept, being Europe-centred, is often built in opposition to the United States' security guarantees. Europe, as a Union and as a community of states, has since the first half of the 20th century been highly dependent on the transatlantic bond for its security. Large underinvestment in defence following the end of the Cold War and the consolidation of the NATO Alliance have weakened Europe's native defence capacity. New drivers for a more autonomous approach to strategic issues have emerged and been accelerated by the COVID-19 crisis, the February 2022 events in Ukraine, and protectionist U.S. presidencies, relaunching the debate around this bond and restoring the importance of the concept of strategic autonomy.

Traced back to the Franco–British St. Malo Declaration (4 December 1998) and earlier, strategic autonomy first identified the need for autonomous action that could be used

“in order to respond to international crises”. (Krebs, n.d.) Later, in the 2016 EU Global Strategy, the concept was further developed to consider defence both inside and outside EU borders, while also emphasizing the need for defence capabilities that are complementary to NATO. The Strategy identifies hybrid threats, critical infrastructure, and external border management as key dimensions for CSDP missions and operations, as well as for European Border and Coast Guard cooperation (EEAS, 2016).The importance of technological and industrial autonomy is also highlighted, encouraging collaboration among Member States to jointly develop defence capabilities. This reframing of European strategic autonomy envisions an appropriate level of autonomy in defence matters for EU Member States, once again challenging the transatlantic bond. This new vision also sparked early debates, particularly among Eastern European states, revealing a division between those that viewed NATO as the sole defence and security provider against the Russian threat and those, mainly in Western Europe, that favoured a more autonomous European defence (Varma, 2024). Strategic autonomy therefore does not imply isolationism, but rather the ability to choose to act independently or in collaboration with partners.

To further precise the concept, a new interpretation emerged in 2020 that explicitly defined it as such. With the first uses of the notion by The High Representative of the Union for Foreign Affairs and Security Policy (HR/VP), Josep Borrell, and later by other commissioners, the scope of strategic autonomy broadened (Borrell, 2020). Subsequently, a Foresight Report published in 2021 further expanded the areas in which the EU could strengthen its strategic autonomy to ten domains, moving beyond a sole focus on security and defence to also include trade, finance, investment, and technology (European Commission, 2021a). A single of these domains concerned defence and autonomous access to space, indicating an evolution from the initial perception of the concept. This new interpretation of strategic autonomy, developed in the aftermath of the COVID-19 crisis, is referred to as “Open Strategic Autonomy” (Helwig & Sinkkonen, 2022), and thus frames it as a multifaceted concept that has evolved over time in both its definition and scope.

Strategic autonomy has also recently been recognised under various names such as “European sovereignty”, “freedom of action”, and “strategic sovereignty”, the latter having appeared more recently with the broadening of the concept. These names

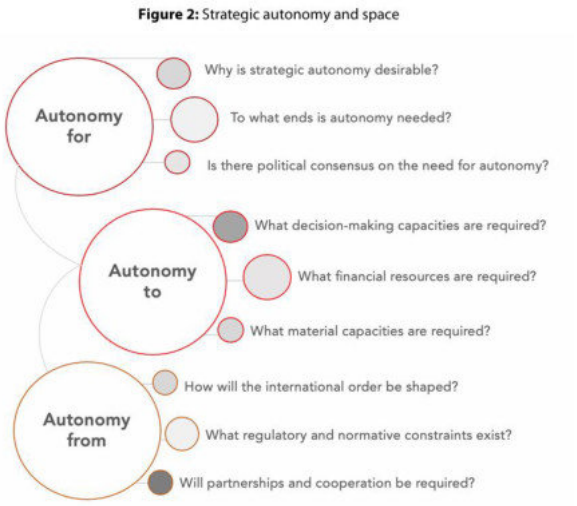
complemented the original understanding of strategic autonomy, which focused more on security and defence (Fiott, 2021b). For the purpose of this research, European strategic autonomy will be defined through three dimensions: political, industrial and in term of capacities as identified by researchers (Libek, 2019). The term itself is composed of two elements that have their own dimensions. The adjective strategic refers to matters linked to the core interests of the community (Cellerino, 2023) while the term autonomy will be defined through two dimensions: political autonomy, referring to the ability to take decisions independently, and operational autonomy, referring to the means and capabilities required to implement those decisions (Anghel et al., 2020).

Building on these variations and the evolution of the concept, the common definition used in this research will be the one laid out by the European Parliamentary Research Service: “EU 'strategic autonomy' [is] the ability to act autonomously as well as to choose when, in which area, and if, to act with like-minded partners. The capacity to act autonomously implies both the ability to decide and to implement decisions in an autonomous manner.” (Retter et al., 2021). This definition encourages viewing strategic autonomy as a spectrum with competing visions among EU Member States, ranging from inclusivity to exclusivity with regard to involving external partners. On the one hand, countries such as France search exclusivity, worrying that external contacts might interfere with the objective of decreasing strategic dependencies towards stronger partners such as the United States through NATO. On the other hand, countries such as the Netherlands and the Nordic states consider the involvement of external partners as a way to maximise comparative advantage (Libek, 2019). This divide in opinion is mainly evident in Permanent Structured Cooperation (PESCO) projects, as well as in a significant portion of European projects more broadly.

2.1.2. The Space Domain in Strategic Autonomy

Strategic autonomy in the context of the space domain is presented by Cellerino (2023) as the capacity of the continent to act autonomously, with a focus on its ability to possess secure and sovereign access to orbital assets and to protect the critical infrastructure upon which European society, the economy, and defence systems depend (Cellerino, 2023). Due to a lack of purely academic sources on this central concept, this section is structured around Fiott's (2020) concept of "autonomy for, to, and from" in order to define the spectrum of strategic autonomy in space. First, *autonomy for* encompasses the desirability of autonomy, given Europe's high dependence on space for financial, technical, and economic purposes and how it is presented by European authorities. Second, *autonomy to* considers Europe's ability to act as a space actor by possessing the industrial base and capabilities required to access space and operate within it. Lastly, *autonomy from* highlights Europe's capabilities and dependencies in its space activities the current possibilities and the areas where it is still left behind.

Fig 1. Strategic Autonomy in Space



Source: (Fiott, 2020)

To allow modern European society to function, European strategic autonomy in space is fundamental for economic and political stability. The dependency of the economy on space is enormous, with satellite navigation services providing vital Position,

Navigation, and Timing (PNT) services to businesses and individuals. Position and navigation services provide users with precise location data, enabling coordination, collision avoidance, and the reduction of traffic congestion. Timing services are equally crucial for financial transactions, banking, and stock market operations, as synchronized timestamps provided by satellites allow for global coordination(OECD, 2021). Earth observation (EO) services have a wide range of applications, producing geospatial data to perform surveillance of environmental changes, critical zone , and policy implementation. Weather forecasting, maritime traffic management, and other emergency services heavily rely on EO technologies, such as for wildfire monitoring(Van Camp & Peeters, 2022). In food supply management, EO satellites are also essential, supporting crop monitoring, equipment guidance, and freshwater resource management. Satellite communications (SATCOM) enable secure communications for governmental and private actors, facilitating crisis management, and coordination of transport and cloud-based services for businesses. SATCOM is also central to terrestrial telecommunications, supporting digital radio, television, and telephone networks, and being a foundation for the modern lifestyle (Van Camp & Peeters, 2022).

For the purpose of allowing Europe to have autonomous access to space and the ability to be active in it, the development of space technologies, as well as other frontier technologies such as quantum computing and AI, is fundamental. The importance of the private sector in this domain is crucial. Europe's pursuit of autonomous access to space follows decades of dependency on Russia and the US for launchers, which led to the development of capabilities such as the current Ariane 6 and Vega C launchers, and the European Spaceport in French Guiana. Dependency on other spacefaring nations is seen as a sign of significant deficits in national leadership and, therefore, sovereignty, has for many years been a source of tension among leaders of the European space sector (Patarin-Jossec, 2020). Similarly, the need for sovereign industries in the manufacturing segment of the space industry has followed a comparable path, resulting today in competition among three leading companies supplying systems and equipment to the European Space Agency (ESA): Airbus in France, OHB in Germany, and Thales Alenia Space in Italy (Eurospace, 2024). These companies share the largest production contracts for space systems. However, this industrial base is subject to the same divisions that affect EU governance at large, with these companies

regarded as national champions and sometimes used as instruments for national influence. These dynamics are further reinforced by ESA's Geographical Return Principle, which aims to distribute contracts based on the financial contributions of Member States, creating competition influenced by national interests that often go beyond logical considerations in contract allocation (Franzoso, 2024). The recent rise of private actors such as SpaceX, which challenge the traditional public-agency model of the space industry, represents a significant challenge to the already established European companies (Reillon, 2017). In addition to mastering technology domains, reliance on supply chains for critical components makes the European space industry vulnerable to disruption and geopolitical uncertainties (Fiott, 2020).

Finally, regarding European autonomy from the outside, the fragmentation of the European space sector is notable, primarily due to a complex governance structure shared among the EU, ESA, Member States, and other thematically focused organizations such as NATO. This multiplication of actors generates inefficiencies, with overlapping frameworks and Member State involvement. Operational inefficiency also arises from the separation of competences: the EU focuses on downstream applications and the use of space capacities, while ESA is responsible for the upstream sector, including research, development, and launches. The rise of the New Space economy and interdependencies with non-EU Member States presents significant challenges for European autonomy in space (Reillon, 2017).

From another viewpoint European space assets are also subject to more perverse threats that can be divided into three categories: ground-based threats, space-based threats, and Anti-Satellite (ASAT) threats. Ground-based threats range from cyber-attacks and electronic warfare, such as jamming and spoofing signals to disrupt ground stations receiving satellite data, to the rapid development of new capacities by competitors, which can quickly render technologies obsolete. Space-based risks are more natural in character, encompassing space debris and meteorites, which increasingly congest Low-Earth Orbit (LEO) (Reis, 2025). Regarding ASAT threats, great power competition plays a crucial role. Kinetic Energy ASATs (KE-ASATs), including direct-ascent and co-orbital weapons, have already been tested by China (2007) and Russia (2021), generating thousands of debris fragments (Weeden & Samson, 2023). Non-kinetic attacks use non-physical means to achieve reversible or irreversible effects,

such as Directed Energy Weapons (DEWs). Examples include high-powered lasers used to blind Earth observation satellites, high-powered microwaves, and electromagnetic pulses (EMPs) (Defence Intelligence Agency, 2022).

This overview of the application of strategic autonomy in the space domain has already highlighted the fragmentations, challenges, and difficulties of the European space sector. These serve as a preliminary assessment of the evolution of European strategic autonomy in space and have already touched upon three categories of threats in the space domain. As this research focuses on how these space capacities strengthen resilience against hybrid threats, a more precise overview will be provided in the second section of the literature review.

2.1.3. The History of European Strategic Autonomy in Space

The history of strategic autonomy in space for Europe can be traced along the same timeline as the broader concept of strategic autonomy discussed earlier. Space is a sector that has experienced significant developments alongside conflicts and other defence-related initiatives. Over four phases, the evolution of Europe's space activities demonstrates a multi-decade transition from a focus on science and space exploration to a posture driven primarily by commercial and defence interests in this rapidly evolving industry.

The foundation of Europe's pursuit of strategic autonomy in space can be traced back to the sense of dependence felt by European nations during the conflicts of the 1990s. The Gulf War and the subsequent crises in the Balkans (Bosnia and Kosovo) highlighted Europe's asymmetric reliance on United States military infrastructure (Cross, 2022). During these operations, European forces were dependent on US satellite assets through the NATO and Coalition of the Willing frameworks, essentially for PNT and EO-enabled intelligence. This dependence went beyond technical aspects, including operational and strategic decision-making discordance: the U.S. showed reluctance to be involved in crisis management on the European continent and had diverging priorities during operations concerning the sharing of sensitive data. Crucially, the American-owned Global Positioning System (GPS) was the only GNSS service available to European forces at the time, meaning that European security was

effectively tied to the US Armed Forces, with no guarantee of service should transatlantic priorities shift (Giegerich, 2007).

The drive for autonomy is most visibly represented by the Galileo satellite system, which was developed as an independent alternative to the American GPS monopoly during this period. The European Union and the European Space Agency (ESA) began exploring an alternative to this dependency through an independent Global Navigation Satellite System (GNSS) called Galileo. This caused a period, spanning from 1998 to 2004, representing an important phase of rising tensions in transatlantic relations. The project was initially opposed by the U.S. government, most notably during the 2001 intervention of Deputy Secretary of Defence Paul Wolfowitz, who searched to involve European military leaders within NATO in a project to ensure that the U.S. military could potentially jam Galileo during operations if deemed necessary. Another dilemma arose as Galileo was planned to transmit on ten different signals, divided between civilian use and governmental use through the Public Regulated Service (PRS). One of the latter signals was planned to operate on the same frequency as a future GPS M-code signal (Lindström & Gasparini, 2003). Ultimately, this dispute was resolved not through high-level diplomacy alone, but via a unique form of technological adaptation that served as a bargaining tool. European engineers achieved breakthroughs in signal spectrum overlays that allowed Galileo and GPS to coexist without interference, effectively bringing the U.S. to the negotiating table as an equal (Giegerich, 2007). The resulting 2004 agreement was a revolutionary moment: it transitioned the EU from a subordinate client of American technology to a partner in global infrastructure, establishing that “Galileo, […] would be […] interoperable with civil GPS service” (DoS, 2004, p.4), consolidating the principle of interoperability that allows the U.S. and the EU to work complementarily and more efficiently rather than in competition (Lewis, 2004). This principle still animates most defence and space technology discussions today.

During the early 2010s, the EU space domain was primarily framed as a civilian field driven by market and policy considerations, with security dimensions considered secondary (De Man & Wouters, 2025). The Galileo programme and the Global Monitoring for Environment and Security (GMES) programme renamed, Copernicus in 2012, focused most of their capacities on civilian and environmental monitoring rather than on security-related operations (Golovtchenko, 2026). In 2016, with the publication of the

Space Strategy for Europe (European Commission, 2016), the EU articulated its ambition in space, explicitly considering it a strategic priority. A specific emphasis was placed on achieving autonomy in accessing space in a safe and secure environment, including independent access to space and the resilience of European space infrastructures (Reillon, 2017). This era saw the securitization of European space policy, exemplified by the 2019 creation of the Directorate-General for Defence Industry and Space (DG DEFIS). Through a dedicated Space Regulation in 2021, the EU Space Programme was established to include, beyond Galileo and Copernicus, Space Situational Awareness (SSA) and secure communications through the GOVSATCOM programme, later known as IRIS^2. At the same time, the EU Space Programme Agency (EUSPA) was established to replace the European GNSS Agency (GSA) in managing satellite navigation programmes (European Parliament, 2021). These institutional shifts amplified the Union's ability to manage its orbital assets through a security lens. This trajectory culminated in the 2022 Strategic Compass, a landmark policy document that formally designated space as an increasingly contested domain (A Strategic Compass for Security and Defence, 2022) requiring protection. The discourse shifted from mere cooperation to technological non-dependence, emphasizing that sovereignty in the 21st century is inseparable from a secure and autonomous supply chain, reducing reliance on Chinese components for the construction of space assets (Reis, 2025).

The transition was dramatically accelerated, similarly to the perception of the concept of strategic autonomy in the current geopolitical climate, characterized by the return of high-intensity conflict with Russia's invasion of Ukraine and the rise of hybrid threats, where European space assets were reframed from public goods into strategic infrastructure for security and defence, requiring a coherent strategy (Bartóki-Gönczy & Malinowska, 2025). The 2023 EU Space Strategy for Security and Defence (EUSSSD) reflects this maturity, focusing on the protection of infrastructure against cyberattacks, jamming, and adversarial manoeuvres, with a strong emphasis on the "Defence of Space" (ESPI, 2020). This shift is physically manifested in the development of IRIS², a multi-orbital satellite constellation designed to provide secure, sovereign communications shielded from external disruption. Furthermore, the EU's investment in Space Situational Awareness (SSA) and the Space Surveillance and Tracking (SST) component highlights a shift toward active defence, recognizing that the space domain is highly contested.

2.1.4. The European Space Sector

The European space sector is currently characterized by a complex institutional architecture and a shifting governance paradigm that reflects broader trends in European studies, specifically the tension between supranational integration and intergovernmental cooperation in European policymaking (Fabbrini, 2017). The European space sector is also subject to these dynamics, with a fragmented landscape dominated by three European organisations, which are divided into various agencies and centres, and complemented by the national space agencies of European states. This complex landscape will be outlined in this section to map the variety of actors present in the field and their respective roles.

The division of tasks in the space sector, with a particular focus on security, is shared between the European Commission through the EUSPA, the European Space Agency, and NATO (Muti & Nones, 2024). The European Commission, through the Directorate-General for Defence Industry and Space (DG DEFIS), manages the EU Space Programme, being responsible for both its administration and implementation. In this dual role, it has positioned itself as the primary policy shaper, seeking to synchronize European and national space activities by establishing requirements and guiding future developments (Bartóki-Gönczy & Malinowska, 2025). The EU's use of space is supported at the operational level by various intelligence agencies and centres, including the EU Satellite Centre (SatCen) for geospatial intelligence (GEOINT), the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), and the European Centre for Medium-Range Weather Forecasts (ECMWF), which both focus on meteorological capabilities (Muti & Nones, 2024). In contrast, the European Space Agency (ESA) is an intergovernmental organization that functions as the technological provider for the European space sector. While it exists outside of the EU structures and is constituted by member states differently from the EU, ESA manages the research, development, and construction of flagship programs such as Galileo and Copernicus in collaboration with private actors (Lieberman & Hoerber, 2024). This dual-governance model is further complemented by the EU Agency for the Space Programme (EUSPA), which focuses on the exploitation, security accreditation, and market development of these assets (Poirier et al., 2023). With an exclusive focus on collective security and crisis management, NATO plays an important role in this institutional mosaic. According to NATO's Overarching Space Policy (2019), the Alliance aims to integrate space-related

considerations into its core tasks, particularly collective defence, while serving as a forum for political-military consultation. In the absence of its own satellites, NATO relies on individual states to provide these capabilities, either through national assets or commercial vendors. Beyond the institutional actors, European national agencies also play a significant role in the sector, such as France's CNES, Italy's ASI, or Germany's DLR. These entities maintain independent strategies and budgets, frequently leading to competing positions in international forums (Bartóki-Gönczy & Malinowska, 2025).

In the 21st-century worldwide space sector, a fundamental shift in the core logics of the industry has occurred, transitioning from Legacy Space, led by the public sector and well established companies, to New Space, which integrates private companies often innovators building disruptive technologies. This evolution is marked by a move away from traditional contracts, where governments handled all the risks and owned all space-based assets, toward a service-dominant logic (Zancan et al., 2024). Public space agencies are increasingly adopting a model that relies on service providers, acting as customers for services provided by private companies rather than as developers and owners. This is exemplified by the procurement of the ClearSpace-1 debris removal mission from a Swiss company and by the strategic reliance of Europe and Ukraine on Starlink during the conflict in Ukraine (OECD, 2021). Consequently, Public-Private Partnerships (PPPs) have become the established norm for delivering space capabilities, facilitating efficiency, risk-sharing, and private co-funding (Golovtchenko, 2026). To bolster this transition and, in the same effort, narrow the competitive gap with the United States and China, the EU has introduced initiatives to foster innovation in the space sector, such as CASSINI and the Flight Ticket Initiative, specifically designed to integrate start-ups and SMEs into the space industrial base (Evroux, 2024). NATO has also operated the NATO Defence Innovation Accelerator for the North Atlantic (DIANA), which is designed to bring together universities, industry, and governments to work with start-ups to develop deep-tech dual-use technologies that address critical defence and security challenges, focusing on emerging and disruptive technologies such as those in the space domain (NATO, n.d.-b).

With the multiplication of actors in the space sector, the European governance model creates significant structural barriers that negatively impact the competitiveness of the European space sector. These barriers stem from the friction between supranational

mandates and intergovernmental structures, which blur the distribution of competences between institutions and member states. The divide among member states between the EU and ESA often results in duplicated project teams and inefficient funding streams, despite attempts to integrate ESA with the EU, ultimately making the European space institutional landscape more fragmented (Lieberman & Hoerber, 2024). At the member state level, governance is also often fragmented, with various ministries handling specific portions of the space portfolio and maintaining different contacts with the same institutions (Sagath et al., 2018). One of the principal contentious issues is ESA's Geographical Return Principle, which mandates that contracts be distributed proportionally to national financial contributions. While this principle supports strategic autonomy, the Draghi Report (2024) identifies it as a source of economic inefficiency, fragmenting supply chains and preventing the consolidation of European industrial champions. Furthermore, legal fragmentation exists as well, with non-interoperable national laws creating uncertainty for sector actors and slowing the development of cross-border activities. In response, the European Commission has proposed an EU Space Law (EU Space Act) aimed at reducing barriers for the space economy by enforcing regulatory harmonization and establishing unified rules for orbital traffic management, resilience, and cybersecurity (Evroux, 2025).

The European space sector is also defined by a contemporary strategic turn due to the 2022 Russian invasion of Ukraine, which has accelerated Europe's focus on security and defence. This shift has extended international security concerns into the space domain, encouraging the securitization of European space assets (Bartóki-Gönczy & Malinowska, 2025). The 2023 EU Space Strategy for Security and Defence (EUSSSD) signal a move toward using space for security and defence purposes, enabling further development of space capabilities. Following this shift, ESA is leveraging its institutional expertise in R&D and risk management, increasingly positioning itself as a central security actor by developing resilient, interoperable space systems and fostering strategic collaborations to address evolving threats in the domain (ESA & ESPI, 2023). NATO echoes this urgency, characterizing the space environment as increasingly diverse, disruptive, disordered, and dangerous. The Alliance has responded by designating space as a fifth operational domain, one capable of triggering Article 5 collective defence mechanisms (Hainaut, 2024). This strategic shift highlights the dual-use nature of assets like Galileo and Copernicus, which are now

framed as critical infrastructure (Lieberman & Hoerber, 2024). It also demonstrates the growing importance of strategic autonomy in space in both regulations and institutional strategies, as well as the emergence of a private sector increasingly focusing on security and defence.

2.1.5. Conceptual Shift: the 2023 EU Space Strategy for Security and Defence (EUSSSD)

Due to the enablers mentioned in the previous sections, the EU introduced on March 10, 2023, the EU Space Strategy for Security and Defence (EUSSSD) (European Commission, 2023). This strategy represents a shift in the European policy approach to space, explicitly integrating security and defence aspects to Space policy following the shift towards strategic autonomy integrating Hard power perspective in the debate (González Muñoz & Portela, 2023). The EUSSSD establishes a roadmap intended to improve the EU's strategic position in space, by developing a common understanding of the use of Space in the new strategic reality that Europe faces (European Union Space Strategy for Security and Defence, 2023). This framework is organized around five primary pillars that address all the facets of space security. The first two pillars focus on internal cohesion and resilience of space systems against external threats. EU Collaboration aims to bring closer military space actors that have a long experience of operating in space and emerging space users, in particular from the New Space to encourage collaboration internally and integration trough common programmes. The Threat Response Mechanisms prioritize a unified understanding of space threats. By establishing processes for the detection, attribution, and reaction to such incidents, the EU seeks to create a more resilient operational environment for its space assets (ESPI, 2023).

The remaining pillars of the strategy address the technical, financial, and normative requirements of a secure space domain. Pillar 3 emphasizes the acceleration of dual-use capabilities, specifically in the realms of Earth Observation, Positioning, Navigation, and Timing (PNT), and the IRIS² secure connectivity constellation. This pillar is central as it will allow the EU to leverage its autonomy of action and its *autonomy to* and *autonomy for*, ensuring that the domestic space industry can remain competitive for the security and defence needs that are leveraged by the space domain (ESPI, 2023). To support these developments, the fourth pillar of the strategy calls for increased scale

and flexibility in funding via the European Defence Fund (EDF) and Horizon Europe. Finally, the EUSSSD seeks to project European influence globally by deepening partnerships with the United States and NATO, while developing their partnership with non-EU European states and ESA and the United Nations for responsible behaviour in outer space (European Commission, 2023). These five pillars are found again in the recent proposal for an EU Space Act providing a common legal framework for security and safety across the Union with a focus on the second pillar ensuring that critical space systems are sustainable and resilient against cyber and physical threats (European Commission, 2025).

Among other technologies, Earth Observation (EO) plays an important role in the European approach for security and defence in space, the strategy categorizes it as a "key enabler for security and defence," (European Commission, 2023, p. 11) offering the factual assessments necessary for autonomous European decision-making (EARSC, 2023). Its role is vital in countering a vast range of threats from conventional to hybrid. By providing enhanced situational awareness for maritime and border surveillance, EO facilitates the detection of irregular activities, such as weaponised migration or maritime traffic on the sea and undersea. It helps identifying factors that are responsible for economic disruption, and enables Intelligence, Surveillance, and Reconnaissance (ISR) to monitor offensive actions from adversaries (Czulda, 2024) . It also supports the European External Action Service (EEAS) in its missions and operations abroad providing vital imagery intelligence (IMINT) to its forces in the land and maritime domain. To further develop EO in the EU Space Programme, the strategy presents further developments to Copernicus. Addressing the limitations of the current program, which lacks the high spatial resolution and revisit times required for defence, the strategy proposes a new Earth Observation Governmental Service (EOGS) (González Muñoz & Portela, 2023).

2.1.6. The Conceptual Debate of Dual Use

To clarify the concept of space security, it is necessary to address the ambiguity of the term dual use. While often treated as a general term for technologies serving both civilian and military purposes, its interpretation varies significantly across different legal and regulatory regimes. In the context of export controls, dual use is applied broadly

to any technology with potential military applications. Conversely, International Humanitarian Law (IHL) adopts a much narrower, functionalist approach, minimizing dual use as a formal category and focusing instead on whether an object constitutes a military objective based on its current use or purpose for targeting considerations (Ortega, 2023). In space defence, when a civilian satellite provides critical data to a military chain of command, it complicates the principle of distinction. The dynamics towards generalisation of dual use technologies in EO (Golovtchenko, 2026) potentially rendering civilian infrastructure a legitimate target.

To navigate this ambiguity, Ortega (2023) has proposed a distinction between dual-use and dual-purpose systems. Dual-use systems are defined by their simultaneous integration of functions, such as GNSS constellations that serve both civilian and military applications, supporting areas such as road travel and missile guidance. In contrast, dual-purpose systems refer to technologies initially designed for civilian ends, such as active debris removal or on-orbit servicing, which possess features like robotic arms that could be repurposed for hostile manoeuvres (UNIDIR, 2025). This distinction shifts the focus from the technology itself to the problem of intention behind the use. For the European Union, this conceptual shift is central, by exploiting the dual-nature character of assets like Copernicus and Galileo, the EU is transitioning from a purely civilian space actor to one with both civilian and military applications, enhancing its total defence capabilities but also its risk of being targeted. (González Muñoz & Portela, 2023).

2.2. Defence Against Hybrid Threats

2.2.1. Hybrid Threats

Hybrid threats, as a concept, play a central role in this research, serving as the main dependent variable. This section will outline the concept of hybrid threats, a term that has gained prominence in contemporary security studies, particularly due to advances in new technologies. By tracing the emergence of this concept and examining current debates around its definition and evolution, this section will present a conceptual model for categorizing and assessing hybrid threats.

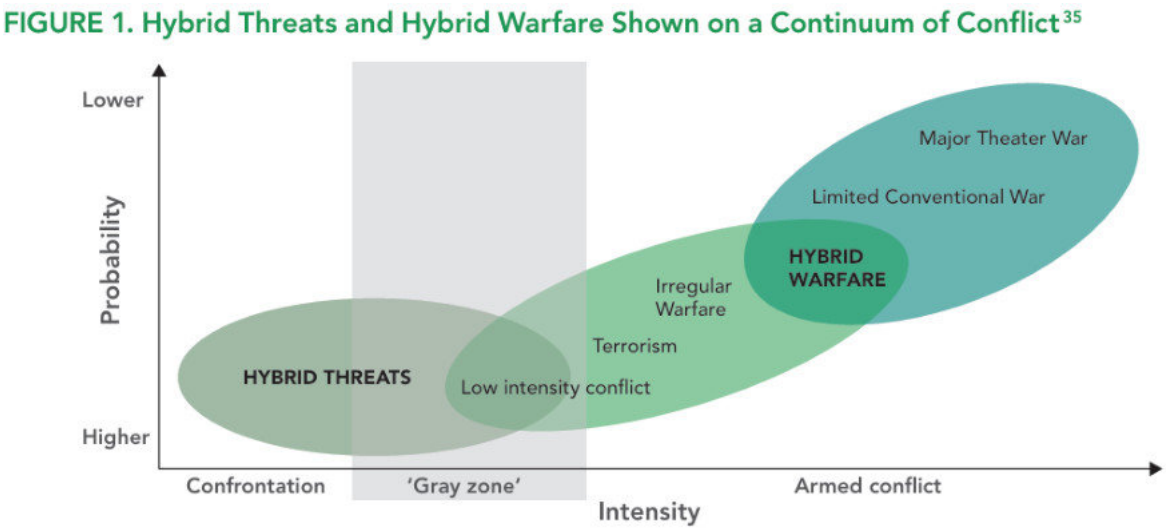
The first popularization of the concept was done by the U.S. Marine Corps through an initial definition that Frank Hoffman (2007) outlines. This definition includes the different modes of warfare, identifying a mix of “conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder” (Hoffman, 2007, p. 14) within a singular, complex battlespace. This original definition was primarily tactical, focusing on how non-state actors, most notably Hezbollah during the 2006 Lebanon War, successfully integrated conventional military capabilities with irregular tactics, considering the effects of these tactics from physical to psychological. However, the literature identifies a significant shift in the perception of the term following the Russian annexation of Crimea by unidentified Russian forces, labelled the “little green men” by media outlets (Shevchenko, 2014). At this point, the concept became more associated with state-driven actions and entered securitization discussions, as NATO and the EU adopted the term to categorize disinformation, economic coercion, and cyber-attacks (Libiseller, 2023; Reichborn-Kjennerud & Cullen, 2016). With the events of 2014, the term migrated from a military description of the battlefield to a broader framework for understanding warfare conducted below the threshold that would require the defender to use conventional armed forces. When these hybrid threats involve kinetic action, they are referred to as Gray zone tactics (Capaul, 2024).

A significant portion of the contemporary literature is dedicated to clarifying the concept of hybrid threats. Scholars such as Sean Monaghan (2019) argue for a necessary analytical distinction between hybrid warfare, the mixing of conventional tactics and hybrid modes in an active armed conflict, a definition closer to the pre-2014 understanding previously presented, and hybrid threats, which refer to strategies targeting a society’s internal vulnerabilities with the aim of provoking a response that can become kinetic. Although different, both challenges are caused by adversaries seeking to neutralize conventional state power (Monaghan, 2019). This overlaps with Mark Galeotti’s (2016) distinction between two senses of hybrid war, separating Political War, which designates a phase of destabilization aimed at dividing, demoralizing, and distracting, from hybrid war in its political-military sense (Galeotti, 2016). As Jan Almäng (2019) suggests, hybrid threats operate by exploiting two types of vagueness: an ontological one, in which the line between peace and war is unclear and arbitrary, and an epistemological one, in which the aggressor deliberately masks their identity and intentions to paralyze the defender’s decision-making process and prevent a clear and

unified response (Almäng, 2019). This latter form of vagueness is categorized under the concept of ambiguity (Reichborn-Kjennerud & Cullen, 2016), which includes the challenges of attributing hybrid actions to the aggressor, ultimately undermining the defender's ability to respond (Mumford & McDonald, 2014).

Despite its common use in policy circles, the term faces academic critique due to its widespread use in the media and public discourse. Critics such as Colin S. Gray (2012) present a general categorization of traditional and irregular warfare, with a third category of hybrid warfare. He, however, criticizes the lack of clarity of the term irregular warfare and traditional warfare, which complicates the understanding of simple changes in tactics, even if the strategic objectives remain the same (Gray, 2012). The core of this objection lies in historical continuity, with the argument that the mixing of traditional and irregular methods is a timeless feature of conflict, practiced since the era of Sun Tzu and utilized extensively during the Cold War under the Soviet label of active measures (Capaul, 2024). From this perspective, the hybrid label serves a political rather than analytical purpose, acting as a rhetorical justification for the EU and NATO to increase defence budgets and modernize capabilities for a multi-domain environment (Caliskan & Liégeois, 2021). This categorization has further negative impacts because it compartmentalizes various threats, even though the strategic objectives of aggressors remain similar, as noted previously (Gray, 2012). While keeping these critiques in mind, this research will combine Hoffmann's (2007) definition with the broadened categorization that followed the 2014 Russian annexation of Crimea.

Fig 2. Hybrid Threats and Hybrid Warfare Shown on a Continuum of Conflict



Source: (Monaghan, 2019)

Hybrid threats have evolved since the early 21st century, and the use of this concept has accelerated. The cause of this surge is the spread of digital technologies, such as social media, widespread access to the internet, and, more recently, artificial intelligence. These developments have lowered the barriers for both non-state and state actors to engage in subversive actions. This acceleration has facilitated common disinformation campaigns and cyberattacks, amplifying the impact of hybrid threats while also increasing their complexity and speed (Capaul, 2024; Treverton et al., 2018).

To empirically analyse and classify hybrid threats beyond academic discussions, a model developed by the Joint Research Centre (JRC) of the EU and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) attempts to structure the concept through a systematic analytical framework (Giannopoulos et al., 2021). This model deconstructs hybrid threats into four essential pillars: Actors, Domains, Tools, and Phases. It recognizes that state actors, as aggressors, utilize a wide array of tools, ranging from physical operations and infrastructure or airspace violations to military exercises, across thirteen domains of interest, including the domain of Space, which is particularly relevant for this research. The model then categorizes activities into three distinct phases: Priming (interference and influence), Destabilization (active operations), and Coercion (war or warfare). It also defines the target of all hybrid threats as the undermining of decision-making capabilities (Giannopoulos et al., 2021). This

framework will be used in this research to guide the quantitative analysis and frame the objects of study, thereby clarifying the dependent variable of resilience against hybrid threats.

2.2.2. Resilience Against Hybrid Threats

Following the exposition of the research question in this paper, the concept of resilience against hybrid threats will be outlined in this section. As resilience is a generic term, focusing on hybrid threats is important for its precise definition. Same as for the concept of hybrid threats, resilience has evolved from a narrow technical definition into a systemic requirement for modern societies. It is defined by David Omand (2005) as the systemic capacity of a society to absorb shocks, recover rapidly, and proactively adapt its essential functions and values to a shifting landscape of disruptions (Omand, 2005).

The literature distinguishes between two mutually reinforcing types of resilience: technical (Hard) and organizational (Soft) (Kahan et al., 2009). Technical resilience focuses on the physical and technological protection of critical assets, emphasizing robustness, the ability to withstand stress, recoverability, and the speed of repair following a kinetic or non-kinetic attack (Divišová et al., 2021). In contrast, organizational resilience addresses the human and institutional dimensions, such as risk management protocols, innovation cycles, and the psychological capacity of a community to endure sustained institutional stress. Operationally, these are attained through a three-stage spectrum: resistance (minimizing the initial threat potential), absorption (mitigating consequences while maintaining core services), and restoration (reconstituting the system to its pre-event state or better) (Kahan et al., 2009). This dual-layered approach is important for understanding the broad significance of resilience in the field. However, space-based assets primarily contribute to technical resilience, as their implications are more physical than psychological, unlike organizational resilience. A complementary model developed by Divišová et al. (2021) identifies a four-dimensional framework of resilience: psychological (cognitive resistance to ideas), social (cohesion and identity), institutional (effectiveness of organizations), and national (the ability of a society to withstand crises while implementing changes). The identification of these four dimensions shows that successful policy should address all four areas to be effectively implemented and ensure long-term strategic resilience (Divišová et al., 2021).

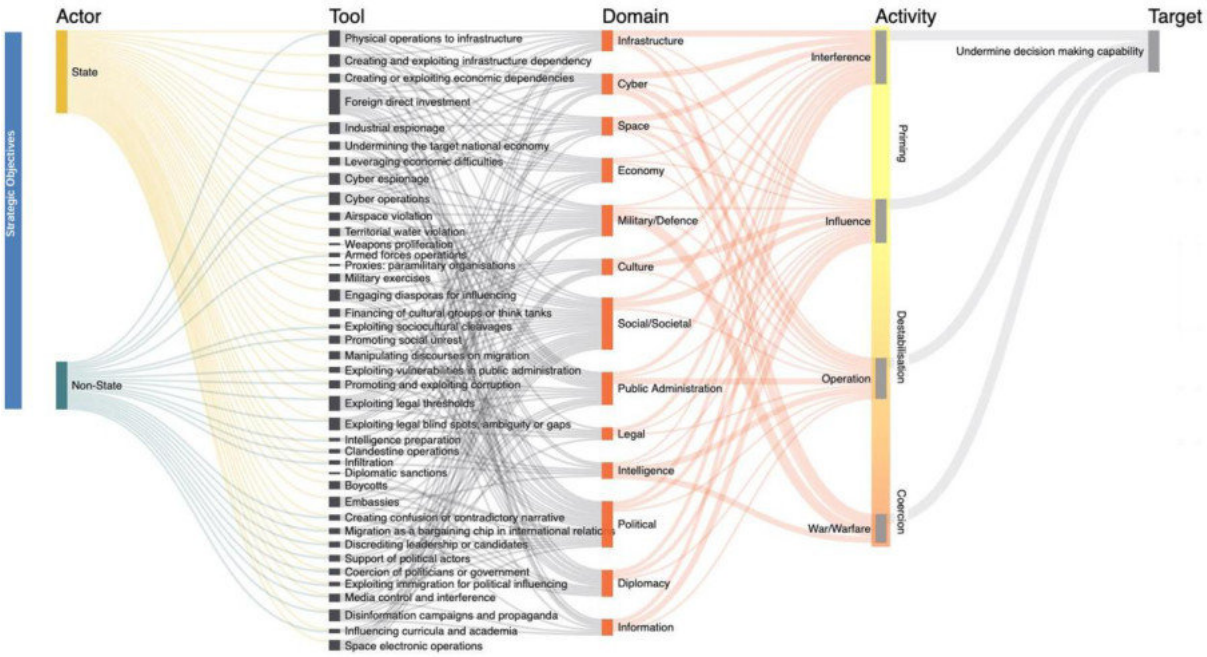
Resilience differs depending on the operational or tactical domain. In the economic and industrial domain, this manifests as technological non-dependence, where states diversify supply chains and stockpile critical materials to prevent adversaries from weaponizing economic interdependencies as a tool of coercion (Murphy et al., 2016). Similarly, modern infrastructure resilience has moved beyond simple protection toward built-in resilience such as trough redundancies. The objective is to ensure that the failure of a single node, whether a power station or a satellite uplink, does not lead to a cascading, catastrophic collapse of the entire network (Linkov et al., 2019). This logic is particularly acute in the cyber, space and maritime domains, where situational awareness plays a central role in enhancing resilience. Given that almost all physical infrastructure is now network-dependent, cyber resilience is framed as a socio-technical problem requiring the integration of human procedures and rapid-response technology to survive sudden cyber events (Jungwirth et al., 2023). In the space domain, resilience is increasingly tied to space situational awareness (SSA) to monitor hostile manoeuvres and to the development of efficient defence systems for orbital assets (Reis, 2025). Meanwhile, in the maritime domain, particularly in regions like the Baltic Sea, resilience focuses on maritime domain awareness (MDA) and the protection of undersea communication cables, which carry 95% of intercontinental data traffic or undersea pipeline that remain highly vulnerable to unattributable sabotage (Murphy et al., 2016).

The most significant trend in recent literature is the shift toward a whole-of-society approach. This shift recognizes that, since hybrid threats target vulnerabilities across society, the military alone cannot provide security. Instead, this approach requires civil-military cooperation to build resilience by merging the resources of the military, civil government, and the private sector (Zekulić et al., 2017). This approach is also evident in the development of the space sector, where actors from all three levels work closely, bringing the concept of dual use back to the table. Closely linked to this, the concept of protean power complements this approach, particularly for Europe in the face of hybrid threats from Russia. It encompasses the capacity to improvise and innovate in response to unpredictable threats that do not follow traditional warfare rules (Baumann & Pynnöniemi, 2025). These two concepts highlight the strategic culture of a state, which encompasses all potential future risks and ensures that it can operate under conditions of ambiguity (Hartmann, 2017). Identifying public trust as the foundational asset of any

resilient system is central to understanding the target of hybrid threats, as aggressors specifically aim to undermine social cohesion and turn internal interdependencies into vulnerabilities. Therefore, maintaining trust between citizens and the state is seen as the ultimate defence (Jungwirth et al., 2023). Finally, the pursuit of technological sovereignty, a concept linked to strategic autonomy in space and exemplified by EU initiatives like the IRIS² satellite constellation, also addresses questions of resilience. It ensures that, in times of crisis or hybrid threats, actions below threshold levels do not disrupt the basic defence mechanisms of society (Jungwirth et al., 2023).

As mentioned in the last part, this research operationalizes resilience against hybrid threats through the JRC/Hybrid CoE Conceptual Model Giannopoulos et al. (2021), a framework that facilitates a transition from event-based observations to a systemic classification across four interacting pillars: Actors, Tools, Domains, and Phases. By identifying 13 distinct domains from legal, cultural, cyber, and space sectors, the model illustrates how aggressors deploy specific instruments from a hybrid toolbox to exploit systemic vulnerabilities inherent to European democracies. These tactics frequently manifest as sabotage, signal jamming, sudden stress on borders or coordinated disinformation campaigns. By mapping the temporal progression from Priming through Destabilization to Coercion, the framework allows for an assessment of a defender's resilience, specifically regarding early warning detection, attribution accuracy, and the establishment of response to deter these actions in the future. The present study focuses primarily on the "Tools" pillar, evaluating how Earth observation satellites might mitigate these interventions to reinforce European resilience against them.

Fig 3. Model Visualisation: Landscape of Hybrid Threats



Source: (Giannopoulos et al., 2021)

2.2.3. Hybrid Threats in Europe

Since the February 2022 invasion of Ukraine, European states have increasingly faced attacks operating bellow the threshold of military conflict orchestrated by the Russian Federation and its proxies. This campaign intensified significantly between 2023 and 2024, with reported incidents nearly tripling as Moscow attempted to erode Western political cohesion (S. G. Jones, 2025). Following the widespread expulsion of Russian diplomatic and intelligence personnel during this interval, the GRU, SVR, and FSB appear to have reorganised their operational methods, pivoting toward a "gig economy" model of sabotage (Edwards & Seidenstein, 2025). This decentralized approach leverages social media platforms, Telegram in particular, to recruit temporary and disposable assets, ranging from local criminals to vulnerable populations and third-country nationals. By incentivizing these actors through liquid financial rewards, Russia facilitates large-scale hybrid warfare while complicating the attribution process and securing a degree of plausible deniability (Edwards & Seidenstein, 2025).

Russian hybrid operations against European manifest through a spectrum of kinetic and non-kinetic actions, differentiated primarily by their impact in the physical world and in the cyber or cognitive environments. As S. G. Jones (2025) observes, kinetic

manoeuvres, those implying direct physical consequences primarily compromise four strategic sectors: transportation networks, government and military installations, critical infrastructure, and the European defence-industrial complex. Sabotage efforts frequently target undersea fibre-optic cables and gas pipelines, while a notable part of these operations targets' logistics and military hubs. Specifically, nearly one-third of recorded incidents focus on sites such as U.S. bases in Germany or manufacturers critical to the European support to Ukraine, such as Rheinmetall, BAE Systems, and Diehl Group (S. G. Jones, 2025). The tactics employed are increasingly sophisticated; for instance, Russia employs a shadow fleet of tankers and commercial vessels with unclear ownership to conduct hybrid operation, such as degrading undersea infrastructure or to bypass Western sanctions on Russian oil & gas (Devlin et al., 2025). Beyond industrial sabotage, the Kremlin exploits human vulnerability through weaponized migration. This strategy involves the orchestrated surge of migrants toward a European border, such as Finnish and Polish borders, often under life-threatening conditions, to put national and European border-management systems under intense stress (Peerboom, 2022). Additionally, the use of incendiary devices, explosives, and unmanned aerial vehicles such as drones has also become usual, exemplified by attacks on civilian warehouses and a sophisticated plot to infiltrate DHL cargo planes with incendiary materials (S. G. Jones, 2025).

Geographically, these threats appear concentrated on the European Eastern flank and towards major Ukraine support states, such as Germany and the United Kingdom. Interestingly, states maintaining more favourable diplomatic postures toward Russia, such as Hungary and Serbia, remain comparatively less impacted by such aggression (S. G. Jones, 2025). Complementing these physical disruptions, Russia integrates non-kinetic instruments, including cyber warfare, electronic GPS jamming, and strategic disinformation, to test European institutional and structural resilience and put the continent's cohesion under stress.

Fig 4. Russian hybrid-threats across Europe, January 2018–June 2025

Source: (Edwards & Seidenstein, 2025)

2.2.4. Deterrence and the Challenge of Attribution and Deniability

Linked to the discussion on resilience against hybrid threats, the conceptual debate regarding deterrence oscillates between viewing hybrid threats, particularly in Gray zone conflicts, as either a functional failure or a strategic success of traditional deterrence (Gannon et al., 2022). Traditional perspectives often characterize hybrid or

Gray zone conflicts as a deterrence failure, arguing that defenders are frequently badly equipped to respond to new tactics, such as cyber operations or the deployment of "little green men" in Crimea, which disrupt the normal functioning of the state without crossing the threshold required to trigger a conventional military response (Van, 2017). In opposition, an alternative school of thought suggests that aggression below the threshold of conventional conflict is actually evidence of deterrence's success. From this viewpoint, aggressors engage in Gray zone operations by intentionally limiting their actions to avoid a decisive, large-scale war with a superior power (Gannon et al., 2022). Focusing specifically on hybrid threats, adversaries adapt their strategies to operate within the shadow of traditional deterrent threats by designing actions around existing frameworks. This involves identifying low-intensity aggression options that provide certain strategic gains while minimizing the risk of provoking a conventional military response from the defender. An aggressor's behaviour is therefore shaped by an internal calculation of operational efficiency, including costs, and external deterrent constraints, namely the fear of escalation into conventional warfare (Gannon et al., 2022).

For deterrence, the space domain plays a pivotal role in shaping the internal calculations of an aggressor, as reconnaissance satellites address major sources of uncertainty by revealing the actions of potential adversaries, thereby denying them the advantage of strategic surprise. By enhancing monitoring capabilities, space-based assets expose covert operations and Gray zone military tactics, resolving the attribution problem that allows aggressors to conceal their actions (Gartzke & Lindsay, 2024). For instance, the 2014 use of "little green men" in Crimea is often analysed as an ambiguous workaround to reconnaissance-supported deterrence, with Russia choosing this Gray zone tactic precisely because Western conventional deterrence had successfully made a large-scale open invasion too strategically risky at that time (Gartzke & Lindsay, 2024). This was later illustrated by the release of confidential geospatial data by President Biden during Russian military preparations leading up to the war in Ukraine (Bo Lillis et al., 2022). However, this enhanced deterrence introduces a critical escalation paradox: if a defender becomes too effective at countering Gray zone tactics, they may inadvertently provoke the aggressor to escalate to conventional war. In such a scenario, the aggressor may conclude that a full-scale conflict is more advantageous than continuing to pursue increasingly ineffective and costly hybrid strategies (Gannon et al., 2022).

The strategic efficacy of hybrid threats relies heavily on their ability to operate in a grey area, make the identification of the perpetrator of these attacks difficult. By utilizing a sophisticated architecture of proxies, ranging from state-controlled operatives to unclearly affiliated non-state actors, the aggressor commands and controls hostile activities while maintaining sufficient distance to ensure plausible deniability. Central to this dynamic is the challenge of attribution. As Pischedda et al. (2024) describe through the Attribution Puzzle, a phenomenon where there is a fundamental disconnect emerging between the defender (victim of the attack) and the international community (observing the attack) regarding its origin. On the one hand, the victimized state, influenced by the direct impact of the aggression, typically identifies the perpetrator with high internal confidence and on the other hand third-party observers, less affected by the attack, often remain sceptic about the rapid attributions. This discrepancy is partially psychological, as the defender's cognitive response to an unattributed attack often triggers a rush toward blame that goes faster than the process for empirical proof. In contrast, unaffected third parties look for a threshold of evidence that is frequently unattainable in the opaque environment of hybrid warfare. This attribution gap creates a diplomatic vacuum that hostile actors deliberately weaponize to evade accountability (Crosetto, 2025). Aggressors also use plausible deniability by taking advantage of the hybrid nature of these operations, effectively protecting themselves from formal retaliatory measures by the defender states (Crosetto, 2025). Enhancing resilience against such activities, therefore, necessitates a robust capacity for timely and accurate attribution, a technical and political task that space-based capabilities are uniquely positioned to facilitate in particular for Earth Observation technologies.

2.3. Space Based Capabilities and Hybrid Threats

Remote sensing from space, specifically Earth Observation (EO), facilitates the monitoring the European continent, avoiding the requirements for physical proximity or a local presence on the ground. These satellite constellations utilize diverse orbital altitudes and specialized sensors to capture data across the electromagnetic spectrum, allowing for permanent situational awareness. As hybrid threats integrate greater complexity in the disciplines of intelligence, the fusion of satellite imagery with multi-source intelligence fusion appears essential for a proactive defence posture and the

fortification of European resilience. Consequently, the following section examines how Earth Observation technologies potentially supports European security frameworks and the broader pursuit of strategic autonomy.

2.3.1. Remote Sensing from Space

Remote sensing, specifically Earth Observation (EO) within the context of this research, is defined by NOAA (2024) as the foundational mechanism for gathering data regarding terrestrial objects or phenomena without necessitating physical proximity or contact. This technological framework relies fundamentally on measuring electromagnetic energy that the Earth's surface either reflects or naturally emits (USGS, 2025). By capturing data across diverse segments of the electromagnetic spectrum, spanning from visible light to non-visible wavelengths, space-based EO assets facilitate a comprehensive global monitoring capability. Bataille (2026) summarize it by the ability of a sensor to pinpoint something on a map. These satellite constellations offer a unique point of view, effectively bypassing the operational vulnerabilities and physical risks inherent to aerial sensors, such as drones and piloted aircraft, or those deployed in the land and maritime domains.

To understand EO satellites, defining their orbit is fundamental as the operational utility of a satellite is fundamentally dictated by its orbital characteristics as a platform's applications is largely dependent of its altitude, swath width, and revisit times over the same area on Earth. Low Earth Orbits (LEO), typically spanning 200 to 2,000 km, remain the primary choice for high-resolution imaging and tactical reconnaissance, this preference stems from both physical proximity to the Earth's surface and the relative accessibility to be launched for various state and commercial providers. Unlike geostationary systems, LEO platforms are not restricted to equatorial planes and can effectively transit polar regions (ESA, 2020b). However, because these satellites move at high velocities relative to the ground, achieving persistent surveillance over the same point necessitates the deployment of vast constellations to mitigate coverage gaps. Medium Earth Orbits (MEO), located near 20,000 km from the earth's surface, function as the critical domain for global navigation satellite systems (GNSS) such as Galileo or GPS. Given that MEO provides an optimal environment for the detection and monitoring of radio frequencies, this altitude has historically hosted specialized remote

sensing assets tasked with the interception of telecommunications, a pillar of signals intelligence (SIGINT) (Remuss, 2009).

At an altitude of approximately 36,000 km, Geostationary Orbits (GEO) enable satellites to remain fixed to a specific area along the equator. This hovering capability makes GEO assets indispensable for continuous regional observation (Onoda & Young, 2017). Such positioning is vital for meteorological monitoring and Space-Based Early Warning systems, which focus on instantly detecting the infrared signatures of ballistic missile ignitions to calculate trajectories and projected impact points. To complement these orbits, Highly Elliptical Orbits (HEO), Sun-Synchronous Orbits (SSO), and Polar Orbits (PO) address the inherent coverage gaps found in LEO, MEO and GEO, particularly at high latitudes and over the poles (ESA, 2020b). By facilitating extended dwell times over the polar regions or specific hemispheres, PO and HEO constellations ensure comprehensive global monitoring. This orbital diversity ensures that strategic movements in sensitive zones like the Arctic remain under persistent observation. Recent geopolitical discourse surrounding the Arctic underscores the region's strategic volatility as its geographical isolation often presents an opportunity for adversaries to exploit the relative scarcity of traditional terrestrial sensors (Lynch, 2025).

Beyond orbital parameters, remote sensing is further categorised by the energy detection methodologies, specifically the critical distinction between passive and active sensors. Passive sensors depend on external energy sources, typically recording solar radiation reflected by the Earth's surface across visible and near-infrared frequencies or detecting thermal heat signatures emitted by terrestrial objects and ballistic projectiles. This captured radiation spectrum facilitates the analysis of colour shifts, humidity levels, and thermal fluctuations (Hennig, 2013). Despite their utility in mapping and environmental monitoring, these sensors remain constrained by exogenous factors like lighting and atmospheric interference; notably, approximately 35% of the Earth’s surface is obscured by cloud cover at any given time (Wang et al., 2023). Active sensors, such as Synthetic Aperture Radar (SAR), bypass these limitations by emitting independent energy pulses and measuring the subsequent backscatter. SAR occupies a vital role in security frameworks because its microwave-based technology penetrates thick cloud cover and smoke, providing a consistent 24-hour, all-weather surveillance capability (Onoda & Young, 2017). Light Detection and Ranging (LIDAR) represents

another significant active modality. By directing constant laser pulses toward the surface, LIDAR calculates the precise distance between the sensor and terrestrial targets, an application that enables the high-resolution modelling of elevation or the assessment of atmospheric particle density, depending on the specific laser frequency deployed (Onoda & Young, 2017).

Assessing the data quality produced by remote sensing satellites requires an examination of three primary resolution parameters: spatial, spectral, and temporal. These dimensions are fundamentally interdependent. Spatial resolution dictates the level of discernible ground detail, where contemporary High Resolution (VHR) systems can capture objects smaller than 30cm. In this context, a single pixel represents a 30cm ground area, facilitating the identification of individual persons and the precise categorization of objects (Wang et al., 2023). Beyond pixel size, spatial resolution is influenced by the swath width of the image, which is determined by the satellite's specific orbital altitude. Recent advancements in Earth observation sensor technology suggest that civilian-owned satellites may soon achieve Ultra High Resolution (UHR) benchmarks of 10cm, providing a level of forensic detail suitable for investigations in environments where aerial or drone surveillance is unfeasible (Palmer, 2025). Spectral resolution involves the sensor's capacity to record energy across discrete frequency bands, with hyperspectral sensors utilizing hundreds of channels to distinguish specific material compositions based on the size and quantity of wavelengths captured (Veraverbeke et al., 2011). Complementing these is temporal resolution, which defines the revisit frequency over a designated geographic coordinate. This rate is a function of orbital mechanics and the density of the satellite constellation. A critical sub-dimension of temporal resolution is data latency, the interval between image acquisition and ground-station transmission. Because Low Earth Orbit (LEO) satellites must maintain a direct line of sight with specific receiving stations to upload data, this communication window can introduce significant operational delays (Frontex, 2025). Optimizing any single resolution parameter typically necessitates a trade-off among the remaining two, often compelling analysts to employ data fusion techniques from multiple sensors to synthesize a more comprehensive intelligence picture (Wang et al., 2023). Furthermore, enhancing these resolutions incurs substantial capital costs, as improvements generally require a proliferation of both satellites and specialized sensors. Operational priorities dictate these choices; security applications typically prioritize high temporal

and spatial resolution for real-time tracking, whereas environmental monitoring may find high spectral resolution more central to its objectives (GMES Working Group on Security, 2003).

Within the operational and security domain, remote sensing data is integrated into the broader discipline of Intelligence, Surveillance, and Reconnaissance (ISR). Although these terms are frequently grouped, they represent distinct functional activities characterized by varying methodologies and strategic objectives. Reconnaissance typically involves targeted, non-permanent operations designed to produce high-resolution snapshots across the electromagnetic spectrum of specific strategic sites to identify developments or answer localized tactical questions (UK Ministry of Defence, 2023). Surveillance, conversely, entails the quasi-permanent monitoring of expansive geographical areas to detect anomalies, such as heat signatures or irregular maritime traffic, over vast regions or particular points of interest (UK Ministry of Defence, 2023). This systemic observation culminates in the generation of Intelligence, which is categorized according to its specific data source. Imagery Intelligence (IMINT) leverages high-resolution visual and radar sensors, following the technical division between active and passive sensors, to provide rigorous mapping and ground activity analysis. Signals Intelligence (SIGINT) complements these visual data sets by capturing and evaluating electromagnetic emissions. This sub-discipline is further refined into Communications Intelligence (COMINT), which centres on the interception of messages, and Electronic Intelligence (ELINT), which analyses non-communication signals like radar signatures to map an actor's potential courses of action. Intelligence, in its final form, represents the synthesized output of this information, providing the analytical basis for an authority to anticipate or attribute attacks within the context of hybrid threats.

2.3.2. Earth Observation Technologies and their Role Against Hybrid Threats

In the contemporary security landscape, Earth Observation (EO) technologies have fundamentally solidified their dual-use character, transitioning from purely scientific instruments to indispensable strategic assets for identifying and mitigating hybrid threats. By providing a comprehensive and persistent surveillance layer, space-based assets empower European and national authorities to detect and attribute covert

actions, including infrastructure sabotage, weaponized migration, and illicit maritime operations, that might otherwise remain obscured (Frontex, 2025; Olech, 2025). This intensified reliance on orbital capabilities among European security providers stems from the increased efficiency found in converging various remote sensing satellite constellations. Such integration facilitates a more robust posture against hybrid interference both within European territory and across its immediate borders.

Earth Observation (EO) satellites function as a technical cornerstone for the European Integrated Border Management (EIBM) framework, providing critical operational support to agencies such as Frontex and the European Maritime Safety Agency (EMSA). One vital application is the surveillance of expansive maritime corridors to detect "ghost boats", vessels that deliberately disable their transponders to mask illicit activities, including sabotage and smuggling (Kotaridis & Benekos, 2023). To mitigate these hybrid threats ranging from undersea cable sabotage to illegal fishing, Synthetic Aperture Radar (SAR) remains indispensable, largely because its microwave sensors penetrate cloud cover and operate independently of solar illumination. When SAR imagery is fused with the Automatic Identification System (AIS), security providers can isolate discrepancies between a vessel's declared position and its actual physical presence. This data synthesis effectively strips away the anonymity of non-cooperative actors operating within Europe’s Exclusive Economic Zones (EEZ) (Bişag & Ilinca, 2025). Beyond coastal waters, EO assets facilitate a pre-frontier intelligence capability. By monitoring regions adjacent to the EU’s eastern flank, these systems provide early warnings regarding assembly points or impending convoys, whether they involve weaponized migration or coordinated incursions (Frontex, 2025). The utility of this surveillance is enhanced by Very High Resolution (VHR) sensors. These platforms offer the rapid revisit times necessary to track individual vehicles or small craft, while automated change-detection algorithms enable analysts to identify emerging illegal crossing routes or clandestine infrastructure development (Remuss, 2009).

High spectral resolution significantly enhances intelligence-gathering capabilities beyond the constraints of standard optical imagery. Hyperspectral sensors, which aggregate data across hundreds of discrete spectral bands, facilitate the identification of minute variations in material composition; this enables the detection of camouflaged assets, illicit agricultural activity, or the distinct chemical residues associated with

munitions manufacturing (Frontex, 2025). Passive Radio Frequency (RF) monitoring augments these capabilities by geolocating electromagnetic emissions from navigation and communication arrays. Such technology proves essential for tracking "dark" vessels that have deactivated their transponders or identifying anomalous concentrations of signals along European frontiers. Integration of RF monitoring with Synthetic Aperture Radar (SAR) systems further permits the detection and geographic attribution of electronic jamming operations initiated by external aggressors. These incidents, which increasingly disrupt civilian aviation, exemplify the utility of remote sensing satellites in monitoring the nuances of grey-zone tactics deployed at Europe's periphery (Ballinger, 2022).

The protection of critical infrastructure constitutes a vital application of modern surveillance, given that hybrid actors frequently target energy grids, subsea cables, and transportation networks to precipitate economic instability (Pillai, 2023). Technical methodologies such as Interferometric Synthetic Aperture Radar (InSAR) are now deployed to detect millimetre-scale ground deformations. This capability enables the continuous oversight of strategic assets like pipelines and railways, allowing security actors to identify physical damages or structural fragilities before a catastrophic failure, whether accidental or resulting from a deliberate attack, occurs (ESA, 2013; Macchiarulo et al., 2022). Complementing these radar-based systems, high-resolution optical sensors facilitate the 3D modelling of sensitive facilities, including nuclear plants, dams, and power grids, to map specific physical vulnerabilities (Remuss, 2009). Such monitoring frameworks extend to the maritime domain through initiatives like the EU-funded VIGIMARE project. By synthesizing high-resolution satellite imagery with ship-tracking data, VIGIMARE isolates suspicious behavioural patterns, such as vessels hovering over critical cable routes (Allen, 2025). The system is notably innovative for its repurposing of fibre-optic cables as passive sensors, by measuring minute fluctuations in light transmission to detect vibrations, these cables effectively "hear" passing ships or dragging anchors. Satellites then provide the requisite visual confirmation to identify perpetrators of undersea sabotage (Allen, 2025). On a broader scale, ESA and SatCen are developing a Digital Twin of the Earth, a sophisticated planetary model driven by Earth Observation (EO) data designed to monitor regional security challenges. In the context of hybrid tactics, this model could facilitate the real-time monitoring of resource

extraction, such as water, to identify deliberate efforts to destabilize specific European communities or regions (Albani et al., 2022).

The utility of Earth Observation (EO) imagery extends significantly to the critical challenge of attribution within Gray zone conflicts. In these ambiguous environments, satellite data serves as an essential repository of evidence regarding troop movements and infrastructure degradation, maintaining continuity for European missions even when terrestrial sensors are rendered inoperable (Bişag & Ilinca, 2025; Schroefl, 2022). Such reliance underscores a broader imperative for technological strategic autonomy through localized initiatives like Copernicus. By securing domestic Earth observation data to facilitate geospatial intelligence, the EU ensures its capabilities remain both competitive and reliable, though this simultaneously necessitates a heightened focus on the systemic resilience of space-based assets (Pellegrino & Stang, 2016) Beyond physical monitoring, EO satellites play a decisive role in neutralizing disinformation campaigns. By delivering precise, verifiable "ground truth" through agencies such as SatCen, the Union can effectively dismantle false narratives designed to polarize European societies, thereby mitigating the traditional advantages of attributional deniability (Giannopoulos et al., 2021). This capability fosters a unified situational awareness that prevents an adversary from exploiting cognitive ambiguity or manipulating public opinion, a manoeuvre frequently observed in Russian hybrid posturing against the continent.

The evolution of defensive frameworks against hybrid threats increasingly centres on enhancing resilience through systematic intelligence fusion. Autonomous systems, which remain acutely vulnerable to hybrid interference, have seen the emergence of innovations such as Maxar Technologies' Raptor software. Introduced in March 2025, this platform enables unmanned aerial vehicles (UAVs) to navigate in GPS-denied environments by correlating live onboard camera feeds with an extensive library of 3D satellite earth observation maps (Erwin, 2025). Development of such localized navigation technology is a direct response to Russian hybrid tactics, specifically the persistent spoofing of GPS signals and electronic warfare manoeuvres observed both in the Ukrainian theatre and across Europe’s eastern flank near Kaliningrad. Because the sheer volume of EO imagery data generated by satellite constellations is enormous, a functional synergy between Artificial Intelligence and Open-Source Intelligence

(OSINT) is required to serve as an intelligence multiplier. This integration facilitates persistent, high-resolution surveillance across the European continent. AI models possess the capability to process these datasets and identify anomalous logistical clusters at speeds far exceeding human analytical capacity. To ensure the evidentiary rigor required for formal investigations, analysts compare satellite-derived IMINT with geolocated social media intelligence (SOCINT) and reports from varied ground or airborne sensors. Such a multi-layered approach allows European security providers to verify kinetic or non-kinetic events in real-time while maintaining a more proactive security posture (Kotaridis & Benekos, 2023).

Through the evolution of the Copernicus (formerly GMES) programme, a collaborative Working Group of European and national experts conducted a detailed analysis of technical resolution requirements tailored to specific security applications. This assessment mapped spatial, spectral, and temporal resolution needs, revealing a diverse spectrum of operational utilities dictated by pre-existing capacities and projected future requirements (GMES Working Group on Security, 2003). The data presented in the following table provides a diagnostic framework for this research to evaluate contemporary European space capabilities. By identifying gaps or dependences, it becomes possible to measure the extent of European strategic autonomy in space in comparison to international competitors.

Table 1. Sample Image Requirement for Earth Observation Satellites

Task	Main Sensor(s)	Resolution (m)	Revisit Time	Delivery Time
Industrial plant analysis	Optical, Thermal Multispectral	0.5 - 2 2 - 10 1 - 4	Mthly, Qtly	Critical
Airfield analysis	Optical	1 - 2	Possibly	Not critical
Barracks analysis	Optical	1	Possibly	Not critical
Port analysis	Optical	1 - 5	Possibly	Not critical
Aircraft identification	Optical	1	Not necessary	Not critical
Missile identification	Optical	0.7	Not necessary	Not critical
Radar identification	Optical	0.4	Not necessary	Not critical
Treaty verification	Optical, Multispectral	0.5 - 2 1 - 4	Possibly	Critical
Crisis management	Optical, Radar	1 - 5 1 - 5	Frequent	Critical
Flood analysis	Radar, Optical	2 - 15 2 - 10	Frequent	Critical
I&W monitoring	Optical, Radar	0.5 - 1 1 - 3	Frequent	Critical
Camouflage detection	Multispectral	1 - 2	Not necessary	Not critical
Terrain analysis	Optical, Multispectral	3 – 10 5 - 15	Not necessary	Not critical
Coastal monitoring	Radar, Optical	2 - 15 2 - 10	Frequent	Critical
Route study	Optical	0.7 - 5	Not necessary	Not critical
Evacuation planning	Optical	0.7 - 5	Not necessary	Not critical
Humanitarian intervention	Optical	1 - 5	Frequent	Critical
Damage assessment	Optical, Multispectral	0.5 - 2 1 - 4	Frequent	Critical
Oill spill monitoring	Radar Optical, Multispectral	2 - 15 2 - 10 2 - 10	Frequent	Critical
Peace keeping	Optical, Radar	0.5 - 2 1 - 8	Frequent	Critical
Peace enforcing	Optical, Radar	0.5 - 1 1 - 8	Very frequent	Critical
Point Location DGI	Optical	0.7 - 1	Not necessary	Not critical
Local DGI	Optical	1 - 2	Not necessary	Not critical
Regional DGI	Optical	5 – 10	Not necessary	Not critical
Wide Area DGI	Optical	10 – 30	Not necessary	Not critical
Technical intelligence	Optical Hyperspectral	0.10 – 0.30 1 - 3	Required	Not critical

Source: (GMES Working Group on Security, 2003)

3. Methods

3.1. Research Design

The second half of this research addresses the core research question: *To what extent does European strategic autonomy in space contribute to strengthening resilience against hybrid threats?*

The methodology of this study adopts a mixed-methods approach to evaluate the current degree of European space autonomy. By quantifying Europe level of autonomy across multiple tiers through a specific assessment of Earth observation (EO) technologies, it becomes possible to compare political ambitions with empirical data regarding sectoral investments and capabilities. To supplement this quantitative baseline, qualitative case studies will bridge the gap between abstract policy and practical application. Specific use cases demonstrating how EO satellite constellations have reinforced European resilience will be analysed to illustrate their utility within the broader security debate.

For the purposes of this study, the term "European" encompasses the continent in its entirety. This definition goes beyond specific institutional frameworks like the European Union or NATO to include significant EFTA nations and independent European organizations that maintain satellite ownership. The research sample comprises 24 nations and 3 organizations identified as space-faring entities. This selection is derived from a catalogue curated by the U.S. Strategic Command Combined Space Operations Center (CSpOC), which integrates 40,000 orbital records synthesized from U.S. Space Command, U.S. Space Force, and proprietary satellite owner datasets (CSpOC, 2026). These records are not only including satellites or active payloads, but it also includes rocket stages and general debris.

Table 2. European Actors in Space

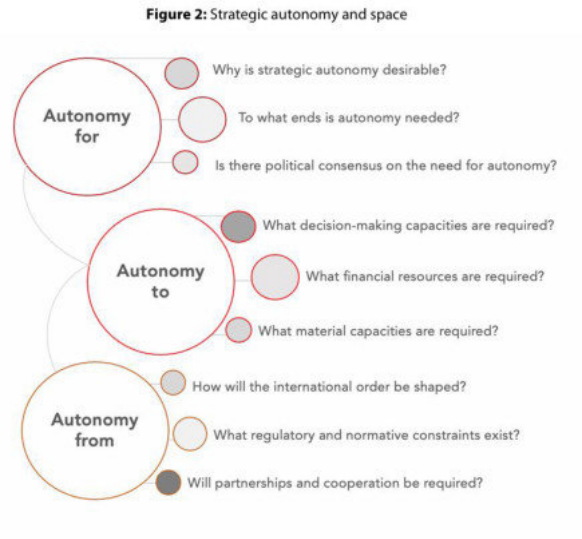
Entity Code	*Objects in Orbit*	*Earliest Launch Date*
***UK** (United Kingdom)*	724	22.11.1969
***FR** (France)*	649	26.11.1965
ESA	129	20.04.1977
***GER** (Germany)*	87	08.11.1969
***IT** (Italy)*	83	25.08.1977
***EUTE** (Eutelsat)*	62	16.06.1983
***SPN** (Spain)*	51	15.11.1974
***FIN** (Finland)*	30	03.12.2018
***NOR** (Norway)*	24	18.08.1990
***EUME** (Eumetsat)*	18	20.11.1993
***SWED** (Sweden)*	13	22.02.1986
***SWTZ** (Switzerland)*	12	23.09.2009
***BEL** (Belgium)*	10	19.06.2014
***POL** (Poland)*	8	21.11.2013
***DEN** (Denmark)*	8	23.02.1999
***LUXE** (Luxembourg)*	7	12.10.2011
***NETH** (Netherlands)*	6	17.05.1988
***GREC** (Greece)*	4	12.10.1992
***BGR** (Bulgaria)*	4	23.06.2017
***CZE** (Czech Republic)*	4	02.08.1995
***HUN** (Hungary)*	4	16.08.2024
***LTU** (Lithuania)*	3	07.11.2020
***POR** (Portugal)*	3	26.09.1993
***SVN** (Slovenia)*	2	03.09.2020
***CZCH** (Czechoslovakia)*	2	28.09.1989
***HRV** (Croatia)*	1	21.12.2024
***EST** (Estonia)*	1	07.05.2013

Source: (CSpOC, 2026)

3.2. The Strategic Autonomy Framework: For, To, and From

In order to operationalize the independent variable, European Strategic Autonomy in Space, this research adopts the three-dimensional framework established by Fiott (2020). This model categorizes strategic autonomy into three distinct pillars: "Autonomy For," "Autonomy To," and "Autonomy From." Utilizing this three levelled structure facilitates an objective assessment of the European space sector’s current maturity, specifically regarding the development and deployment of Earth observation satellites.

(repetition) Fig 1. Strategic Autonomy in Space



Source: (Fiott, 2020)

The first pillar of **Autonomy For** serves to articulate the strategic imperative and desirability of autonomous capacity. This section provides a systematic examination of European trajectories regarding Earth Observation (EO) specifically for security-related mandates. By interrogating official publications, legal frameworks, and doctrinal shifts, the analysis illustrates the strategic vision of institutional stakeholders within the European space ecosystem. Central to this first pillar is the role of EO as a proactive defence mechanism against hybrid threats. The methodology traces the evolution of the European posture toward the securitization of space, while many space-faring nations maintain distinct national and military space strategies. This research prioritizes a selection of documents from the EU, ESA and NATO to capture the multilateral dimension of the domain. Synthesizing these directives provide an understanding of "autonomy for," elucidating why the continent's transition toward becoming a consolidated space power is a geopolitical necessity.

A collection of these publications is drawn from Chapman (2025) and official documentation provided by NATO (2025).

Table 3. Selected European Space Strategies

Organisation/ Country	***Documents***
European Space Agency	2015 ESA Annual Report
	High-Level Advisory Group on Accelerating the Use of Space in Europe (2021)
	2023 ESA Annual Report
	ESA Agenda 2025: Make space for Europe
European Union (EU)	Space Policy (2005)
	Competitiveness Council: Space policy—Preparation of the 3rd Space Council (2005)
	Agenda 2011 (2006)
	Galileo: Overcoming Obstacles—History of EU Global Navigation Satellite Systems (2017)
	EU Space Programme (2021)
	Action Plan on synergies between civil, defence and space industries (2021)
	EU Space Strategy for Security and Defence (2022)
	Toward EU Leadership in the Space Sector through Open Strategic Autonomy Cost of non-Europe (2023)
	Council Conclusions on the EU Space Strategy for Security and Defence (2023)
	The 2023 EU Capability Development Priorities
	European Union Space Strategy for Security and Defence (2024)
	2024 EDA Long-Term Review
	EDF, Indicative multiannual perspective 2024-2027 (2024)
	European Defence Industry Programme (2024)
NATO	Nato Standard AJP-3.3 Allied Joint Doctrine for Air and Space Operation (2016)
	Nato's Overarching Space Policy (2019)
	Nato STO Science & technology trends: 2020-2040
	Nato 2022 Strategic Concept
	Allied Persistent Surveillance from Space (APSS) (2023)

Source: (Chapman, 2025; NATO, 2025)

Building upon this foundation, the second pillar, **Autonomy To**, evaluates the continent's substantive capacity for independent action. This assessment relies on a quantitative examination of investment benchmarks, active satellite populations, and the prevailing technological sophistication of the European industrial base. Strategic autonomy is thus operationalized through operational, industrial, and technical capabilities, while simultaneously considering structural difficulties, such as a fragmentation of actors and the reliance on the public sector, that attenuate European strategic autonomy. To analyse numerically these dimensions, the study integrates primary industry datasets with established economic frameworks, ranging from OECD metrics to Eurospace indices. Specifically, the Eurospace (Eurospace, 2024, 2025) "Facts

& Figures" reports serve as a primary diagnostic for the economic vitality of the space industrial sector. These figures are contextualized against broader global shifts using the OECD (2023) Space Economy in Figures report. To bridge the gap between financial inputs and tangible orbital outcomes, the analysis incorporates data from McDowell (2026) via Jonathan's Space Report, tracking orbital launch attempts and satellite manufacturing statistics as physical proxies for funded commercial and military activity. The resulting quantitative analysis remains largely descriptive, mapping trends within European markets. It should be noted that as market analysis are of high value for the organisations putting them together, that generate an important part of their revenue with it, it was not possible to find a numerical dataset to conduct precise statistical analysis.

The final pillar of this conceptual framework, **Autonomy From**, evaluates European technical capacities through a targeted benchmarking exercise. This analysis correlates European military and dual-use Earth Observation (EO) requirements, specifically the spatial, spectral, and temporal resolution standards identified by the GMES Working Group on Security (2003), against the current functional parameters of European satellite constellations. To facilitate this comparison, the research utilizes a comprehensive technical dataset compiled by Lin et al. (2024) complemented by the data of the Union of Concerned Scientists (2023) which aggregates data on EO missions and their constituent sensors. This merged dataset encompasses 776 missions, of which 409 remain operational and 117 are controlled by European entities. By synthesizing disparate open-source repositories, the Lin et al. (2024) data provides a robust empirical baseline for quantifying European orbital assets. The specific metrics extracted for this research include:

Table 4. Data Designation

Table Column Header	RDF Property (Exact Name)	Key Properties & Examples
Satellite	schema:name	*Name, Alternate Name, COSPAR ID, NORAD ID, Launch Date, and Agency.*
Owner	eo-ont:owner	*National and organizational owners (e.g., NASA, ISRO, China, Arab Satellite Communications Organization).*
Status	eo-ont:operationalStatus	*Categories such as Operational, Non-operational, Decayed, and Spare.*
Orbit	eo-ont:orbitType	*Orbit Type (e.g., LEO, GEO, Sun-Sync), Apogee, Perigee, Inclination, and Period.*
Sensor	schema:name	*Name of the sensor technology*
Spatial Resolution	eo-ont:resolutionBest	*Meters of ground resolved per pixel*
Temporal Resolution	eo-ont:revisitTimeBest	*Duration in days for a satellites to pass over the same exact point*
Spectral Region	eo-ont:wavebandRegion	*Operational bands linked to waveband regions (e.g., "Near infrared", "Green", "Red").*

Source: (Lin et al., 2024)

3.3. Case Study Selection and Operational Analysis

Following a comprehensive assessment of European strategic autonomy in space, the core methodology employs in-depth case studies to analyse how space-based assets are leveraged against hybrid threats, specifically those linked to Russian operations on European territory, excluding Ukraine, since February 2022. These instances demonstrate the operational utility of Earth observation (EO) technologies across the defensive spectrum, from initial detection and active response to the long-term deterrence of hybrid campaigns.

With the aim of evaluating the dependent variable, which is resilience against hybrid threats, this research examines three specific cases where Earth observation provided critical strategic value. These selections reflect diverse manifestations of hybrid warfare as categorized within the Landscape of Hybrid Threats developed by Giannopoulos et al. (2021), encompassing distinct tools that affect varied domains, from the weaponization of migration to the sabotage of subsea infrastructure and electromagnetic interference. Each case study illustrates how remote sensing satellites function as essential enablers of resilience by generating the granular intelligence

necessary for detection and attribution, with a particular emphasis on their role in cross-domain deterrence (Gartzke & Lindsay, 2024).

The first case study investigates the 2022 sabotage of the Nord Stream undersea pipelines in the Baltic Sea. This analysis explores how multi-sensor data integration facilitates multi-level intelligence, utilizing optical imagery from Sentinel 2 and Pléiade Neo, Synthetic Aperture Radar (SAR) from Sentinel-1 and ICEYE and localized methane detection from GHGSat to reconstruct the leak timeline and identify anomalous vessel behaviour. Such autonomous EO capabilities arguably provide the forensic evidence necessary for Europe to attribute attacks on subsea infrastructure allowing additionally to establish a credible deterrent against future interference trough Unseenlabs RF satellite constellation. The second case study examines the 2021–2022 border crisis at the European border, between Poland, the Baltics and Belarus, framed as a campaign of weaponized migration. Methodologically, this section analyses the utility of high-resolution satellite imagery from commercial sources in tracking migrant movements and the strategic positioning of border agents and containment measures. By evaluating how Earth Observation (EO) data furnished the European security providers with situational awareness independent of general public narrative, the analysis demonstrates the strategic value of space assets in mitigating political pressure and addressing the complexities of the Attribution puzzle" conceptualised by Pischedda et al. (2024).

Thirdly, the research analyses electronic interference, specifically Russian spoofing and jamming activities across the Baltic region and the European eastern flank. The methodology focuses on the fusion of remote sensing assets with signals intelligence (SIGINT) to geolocate high-intensity electromagnetic emissions. By correlating signal disruptions with known adversary assets and corroborating these findings with optical imagery, the study assesses whether European space-based capabilities allow for the detection of hybrid threats that elude simple optical identification. These electronic disruptions pose a substantive risk to civilian transportation and compromise the integrity of global navigation systems. Collectively, these case studies evaluate European strengths in countering hybrid manoeuvres, illustrating how EO capacities might ultimately fortify the continent's strategic posture amidst escalating great power competition. Each case highlights the specific utility of diverse technological tiers,

ranging from active and passive sensors to hybrid methodologies combining both categories.

The case analysis will be made through a standardized analytical matrix derived from the conceptual frameworks established in the preceding chapter. Adopting this uniform methodology facilitates a rigorous cross-case comparison and allows for the subsequent correlation of findings with the quantitative dimensions of the research. The resulting matrix, synthesized from the disparate classification models explored earlier (Capaul, 2024; Fiott, 2020; Gartzke & Lindsay, 2024; Giannopoulos et al., 2021; GMES Working Group on Security, 2003; Lin et al., 2024; Reis, 2025), serves as the foundational tool for this investigation:

Table 5. Case Study Matrix

Dimension	***Assessment***
Classification of the hybrid threat (Giannopoulos et al., 2021)	*Tool*
	Domain
	Activity
Detection	*Which EO technologies was used?* *What can European EO capabilities illustrate from this incident?*
Attribution and Response **(Gartzke & Lindsay, 2024)**	*How was the threat attributed to the aggressor?* *How was the threat mitigated and monitored?*
Way forward	*What measures were implemented to avoid these events in the future?* *How EO capabilities are mobilised for surveillance and deterrence?*

3.4. Limitations

Following the articulation of the research design, this section delineates the inherent limitations of the selected sampling criteria. These analytical boundaries primarily involve data classification protocols, the specific prioritization of Earth Observation (EO) capabilities, and the volatile pace of technological evolution within the European and global space sectors.

A significant challenge in quantifying European strategic autonomy persists in the pervasive opacity of sensitive, highly classified satellite data. Although this capacity framework evaluates primarily civilian-operated systems, a substantial portion of

remote sensing infrastructure remains under the ownership of national armed forces. In the realm of Geospatial Intelligence (GEOINT), precise sensor specifications and orbital resolutions are rarely disclosed. It is clear that certain high resolution assets are hidden from public registries to safeguard national security interests. Because the technical details of sovereign military assets, specifically their exact spatial resolutions, temporal revisit frequencies, and encryption architectures, remain classified, this analysis must necessarily rely upon civilian-use capacities or approximation of military capacities. Moreover, the operational application of this data is frequently obscured, as sensitive intelligence exchanges often occur within intergovernmental channels rarely published openly. Nevertheless, the strategic declassification of imagery during pivotal geopolitical events, such as the Russian military buildup on the Ukrainian border in early 2022, offers am empirical window into the actual capabilities of military satellite constellations. Parallel to the barrier of classification is a significant financial hurdle, as access to Very High Resolution (VHR) Earth Observation data from commercial providers typically comes with extensive costs, this constraint is partially mitigated through the utilization of open-source datasets, notably those disseminated via the Copernicus EO Browser.

Assessing European Strategic Autonomy within the space domain necessitates a broader analytical lens than one confined strictly to Earth Observation (EO) technologies. Nevertheless, this study deliberately prioritizes EO assets as the primary mechanism for the detection and attribution of hybrid threats. This research does not evaluate the complete spectrum of space-based assets, purposefully excluding a detailed examination of Positioning, Navigation, and Timing (PNT) signals or Satellite Communications (SATCOM). While focusing the analysis on EO facilitates a detailed investigation into maritime and terrestrial situational awareness, such a narrow scope potentially obscures some strategic issues. For instance, cyber-attacks or signal interceptions directed at SATCOM architectures could effectively decouple EO data from command-and-control centres during high-intensity crises, rendering high-resolution imagery unactionable. The urgency of addressing these vulnerabilities is underscored by a recent, high-profile incident involving the interception of European orbital assets by Russian "inspector" satellites (S. Jones et al., 2026).

A final constraint involves the unprecedented velocity of the contemporary space race, which consistently outpaces both empirical data availability and the formulation of corresponding policy frameworks. Because the data analysed here centres on the 2022 Russian invasion of Ukraine, the scope frequently terminates at the 2023 or 2024 threshold. Consequently, these quantitative assessments function as temporal snapshots, potentially failing to capture the rapid evolutionary shifts occurring in the last years. This volatility is complemented by the emergence of the New Space, where the proliferation of private actors complicates the definition of European as a category. As commercial entities increasingly engage in international ventures and cross-border partnerships a European capacity can switch rapidly form European to transatlantic with a merger. Such shifts inevitably reopen the debate regarding the sovereignty of strategic technologies and the feasibility of maintaining European strategic autonomy in space.

4. Capacity Assessment

4.1. EO for Security in Institutional Strategies

This section systematically examines European institutional perspectives on Earth Observation (EO), particularly concerning security-related mandates derived from official strategies and publications. By evaluating a curated selection of legal frameworks and doctrinal documents, the analysis clarifies the strategic vision held by primary stakeholders within the European space ecosystem. By citing concrete parts of each strategy and document this part allows for an authentic report and understanding of the intentions behind the document and the initiatives that are being implemented. To understand the appetite for Europe in space security in particular on EO technology this part will divide its analysis between the three major security providers and institutional space actors in Europe, the EU, ESA and NATO.

4.1.1. European Space Agency

One of the main pillars of the ESA Agenda 2025 is Space for Safety and Security. This pillar “covers state and collective security, safety and security of people, access to resources, and critical economic activities." (ESA, 2025) Concretely, it allows ESA to

contribute “to national policies and the EU Common Foreign and Security Policy (CFSP)”(ESA, 2025). To achieve the objectives set in this pillar, ESA will apply its “recognised R&D experience, covering the entire spectrum of space activities, to address many of the safety and security challenges faced by its Member States and those of the EU”(European Council, 2016). Therefore, the Agenda 2025 envisions ESA as the "natural technical partner for developing space infrastructure with safety and security purposes at the European level" (ESA, 2025). It will do so by deploying “its R&D support to activities, for example, in maritime safety and security, [as well as] surveillance and reconnaissance”(ESA, 2025).

Over the years, “ESA has established itself as an actor for the development of space-based solutions addressing security challenges, in a technological way. ESA implements a number of projects related to security; “it builds and deploys systems that […] contribute to the conduct of security missions. For instance, the Earth Explorer satellites allow to forecast emergencies, and the 4S and SAT-AIS initiatives foster the use of telecommunications systems for security purposes.”(ESA & ESPI, 2021). Focusing in particular on the Space Component of Copernicus, Sentinel satellites have become indispensable to use applications linked to the Copernicus Security Services such as the Copernicus Border Surveillance Service (CBSS), Copernicus Maritime Surveillance Service (CMSS), and Service on Support to EU External and Security (SESA). Beyond the Copernicus Space Component (ESA sentinel satellites), Copernicus Contributing Missions (CCM) have also been essential contributions to the Copernicus Security Services, they “have currently been redesigned to take stock of New Space data, and in particular to account for European strategic autonomy and industrial competitiveness” (European Commission, 2023).

In terms of strategies, ESA, through its “strategic foresight capacity, its secure cyber environment, its recognised regulatory framework and its strong risk management culture, the [European Space] Agency was heralded as an appropriate actor to develop and implement strategies and programmes related to “space for security”” (ESA & ESPI, 2023) As highlighted in the ESA Agenda 2025, the EUSSSD, and during the 2nd ESA Security Conference, ESA has been recognised as a credible and leading force in R&D for safety and security. Concretely, it has been mentioned that ESA “will also pursue R&D activities for the development of new systems, which will be interoperable by

design and will put into focus the challenges of end-to-end system security and resilience."(ESA & ESPI, 2023) This important part of ESA's work is also expect to be carried out in collaboration "with other organizations dealing with security issues […] to deliver tangible outcomes".(ESA & ESPI, 2023)

On the business development side, "taking into account the commercial challenges in prospect and the increasingly competitive environment, this security-based approach is a way for Europe to broaden the financial or commercial base of its space activities" (ESA, 2002). By acting as a facilitator, ESA responds to a growing need for EO data assisting Europe's broader goal of achieving strategic autonomy in space, as "Space-based Earth Observation supports autonomous assessment and decision–making. [and as] It is a key enabler for security and defence."(European Union Space Strategy for Security and Defence, 2023).

One of the most concrete security applications of ESA's work, is the Civil Security from Space programme (CSS), that embodies the security evolution of ESA Earth Observation activities from a purely civilian lens to a dual use approach. ESA's "CSS aims to foster the use of space-based solutions, which help save lives and livelihoods and enable civil security players to act swiftly to support humanitarian responses, law enforcement, safety and emergency events."(ESA, 2022a). The CSS functions as a strategic mechanism to consolidate industrial efforts toward addressing civil security and crisis management exigencies, primarily through the integration of disparate terrestrial and space-based sensors for immediate deployment by security practitioners. Such an initiative exemplifies the European Space Agency's burgeoning relevance within the security domain, particularly regarding its capacity for research and development to yield sophisticated technological solutions. This evolution reflects a broader institutional shift wherein the Agency transitions from its traditional mandate as a purely scientific and civilian entity toward a more operational role, developing space assets tailored for European security actors like SatCen and the wider European Union framework.

4.1.2. European Union

Regarding the regulatory landscape, the EU Space Programme Regulation establishes the primary framework for Union-based space initiatives between 2021 and 2027, with Copernicus functioning as a central pillar. This legislative instrument highlights the strategic necessity of space-based assets across both civilian and security dimensions. Within the security apparatus, the Union frames space-derived data as a fundamental requirement for securing operational freedom and strategic autonomy. Consequently, the mandate prioritizes the preservation of an autonomous access to space (European Parliament, 2021) while mandating the protection of orbital infrastructure, reflecting its systemic importance across multiple sectors. By funnelling resources into high-end technological research and incentivizing industrial breakthroughs, the EU intends to ensure the competitiveness of the European space industry in the future (European Parliament, 2021). This is seen as playing "an essential role in preserving many strategic interests [given that] The Union's space industry is already one of the most competitive in the world" (European Parliament, 2021).

Regarding strategic developments, the European Union introduced an Action Plan in February 2021, frequently termed the Three-Point Belt Plan, designed to foster synergies across the civil, defence, and space industries. This framework centres on the multidimensional interactions within an ecosystem comprising aeronautics, space, and defence alongside various civil sectors, such as security. By establishing specific objectives throughout the Union, the plan seeks to bridge disparate EU programs and incentivize targeted funding for research and development within the space and defence domains. Mentioning "Copernicus, which offers environmental and security services that are regularly used by various user communities for civilian and defence purposes, in particular applications such as compliance verification and enforcement with EU law" (European Commission, 2021b). The 2021 Action Plan finds its grounding in the EU MFF 2021-2027 that finances the whole EU space programme.

On February 15th, 2022, before that the Strategic Compass was adopted, the European Commission, released a communication to strengthen the defence dimension of space at an EU level. The Commission contribution to European defence addresses a series of actions and related timeline to be launched in EU's critical areas for defence and security, those include space at a central position. Mentioning for EO

that “The evolution of Copernicus should also take into account defence requirements” (European Commission, 2022) and that “the Commission will promote a ‘dual use by design’ approach for EU space infrastructures, with a view to offering new resilient services that address governmental needs.”(European Commission, 2022). This communication has created the essential building blocks of the future EU Earth Observation governmental service (EOGS) by tasking the commission with assessing “the feasibility to develop and deploy a more resilient and secured Copernicus service for governmental purposes, taking into account defence requirements to the extent possible.”(European Commission, 2022)

The formal adoption of the Strategic Compass in March 2021 marked a pivotal shift in the Union's approach to collective security, specifically outlining mechanisms to bolster relevant EU capabilities. By establishing clear priorities for a comprehensive action plan, the document aims to fortify European security and defence policy through 2030. Crucially, the Strategic Compass identifies the space environment as a congested and contested operational domain, emphasizing that the EU Space Programme remains indispensable for the protection of European interests. Each of the four directives underscores this strategic reality by incorporating explicit references to the space sector. The INVEST directive mentions specifically EO, declaring that the EU “will develop new cutting-edge technology sensors and platforms […] notably the development of Space Based Earth Observation […] which are key to providing independent decision-making. The focus area Defence in Space represents a first step in this direction.”(A Strategic Compass for Security and Defence, 2022)

Finally, in 2023, the EU Space Strategy for Security and Defence address a new space governance system with shared competences between the Commission, EUSPA and other entities. On EO following difficult debated on the possibility to expand the range of services that are currently provide by Copernicus, the EUSSSD states that “Although Copernicus delivers security services, it was not designed to comply specifically with defence requirements”(European Union Space Strategy for Security and Defence, 2023). Therefore, the commission initiated the work on the EOGS “as part of the evolution of Copernicus services”(European Union Space Strategy for Security and Defence, 2023).

The EU has been integrating space services into its defence strategy since the beginning of its space activities. In recent years, there has been a significant increase in defence-related funding, services, and applications. Space as an indispensable tool for defence and security has been encompassed in many of these opportunities. Among the funding opportunities for EO for Security, the European Defence Fund (EDF) plays an important role in supporting disruptive technologies. The EDF became operational in January 2021 with a budget of approximately €7.9 billion for the period 2021-2027. In the last years the EDF investments for space were split into various areas one of them being Earth observation for ISR applications. Regarding EO for ISR applications, the EDF funded the Space-based Persistent ISR for Defence and Europe Reinforcement (SPIDER – 33 months), a feasibility study on the development of "innovative multi-sensor space-based Earth observation capabilities towards persistent and reactive ISR"(European Commission, 2024a). Another funding source serving as opportunity lies in the European Defence Industry Programme (EDIP). A financial programme providing support with €1.5 billion from the EU budget over the period 2025-2027. (European Commission, 2024b) EDIP is already addressing "the early development stage of technologies and products for small optical satellites for maritime surveillance (OPTISSE 2019 – 12 months; NEMOS 2020 – 24 months)"(European Commission, 2024a). Finally, the programme Horizon Europe has financed for €8 million a call for proposal for the development of Copernicus for Security, especially on the particular Copernicus Security Services to provide groundbreaking technological development of the service (European Commission, 2023).

On the Commission side, declarations from public figures as commissioners have shown the trends in the EU approach to space. At the 14th European Space Conference held in Brussels, Thierry Breton, addressed the Union's future targets in the "defence dimension of the EU's space policy". Among them were a) the expansion of the "defence dimension in existing and upcoming EU [space] infrastructures"; b) the development of "new infrastructures as dual use by design, integrating the defence needs from the outset"; and c) the potential future establishment of a European Space Command. On Copernicus in particular, the commissioner mentioned how "it is also facing a growing and very acute competition from private actors".(Breton, 2022) Following the June 2024 elections and the appointment of Kaja Kallas as the next HR/VP, the EU intentions towards Security and Defence is expected to grow towards the goal of

attaining strategic autonomy without showing significant changes for now. In 2025, the Joint Research Centre has also included formally Earth Observation for security in its portfolio, focusing specifically on maritime surveillance, and border surveillance, in an attempt to streamline technological needs and innovations (Joint Research Centre, 2025).

From the perspective of key stakeholders, various EU Member States, specialized agencies, and prominent think tanks have scrutinized the prospective evolution of the Union's Space Programme, with a specific focus on Earth Observation (EO) applications within the security domain. This discourse often centres on the inherent complexities of multi-purpose infrastructure; notably, ESPI emphasized the significance of the dual-use challenge as a primary hurdle for the future of the EU Space Programme (ESPI, 2024a). Showing “The policy and capability gaps in space for security and defence continue to grow in comparison to other space powers”(ESPI, 2024b). Consequently, proposing that the European “space policy needs to support future European dual-use space programmes” (ESPI, 2024b) allowing to converge civilian and military needs, as well as R&D and more efficient financing. Additionally, the European Defence Agency (EDA) through its Defence in Space (DiS) Forum, welcomes the ambition to integrate military and security users’ requirements of relevant new EU space systems (EDA, 2024a) while highlighting “the challenges of appropriately integrating dual use (civil and military) requirements in civil EU space systems”(EDA, 2024a). The Danish Ministry of Higher Education and Science suggests that a significant limitation exists within the current EU space program components, noting their restricted capacity to deliver services tailored to European security and defence requirements. This structural deficiency implies that the existing framework fails to align sufficiently with the strategic necessities of the Union (KEFM & UFM, 2024). While the program serves various civilian functions, its inability to effectively bridge the gap between orbital infrastructure and the evolving defence landscape remains a critical point of concern for national stakeholders.

From a political perspective, the 2024 European Parliament elections signalled a significant shift in the strategic discourse surrounding orbital assets. While the 2019 cycle saw space-based security and defence priorities concentrated largely within the Renew and Green/EFA platforms, the 2024 landscape reveals a broader consensus that spans the political spectrum, with a marked increase in engagement from centre-

right and right-wing factions. This evolving rhetoric frames space as a cornerstone of European strategic autonomy, focusing specifically on the necessity of early detection systems, persistent satellite monitoring, and the security of industrial supply chains. Current policy debates underscore a deepening commitment to intra-European cooperation on security-related space initiatives, ranging from integrated disaster management and border surveillance to the hardening of critical space-based infrastructure against emerging threats. Specifically on Copernicus, during the discussion on the EU Space Programme Regulations, the EPP “stressed the necessity to continue and expand activities with Copernicus” while the S&D, the Greens/EFA and the ECR “stressed the importance of civil security over military matters” and the “importance of the open use of data.(ESPI, 2024c)

Following the proposal made in the EUSSSD "as part of the evolution of Copernicus services, and as already presented to Member States, an EU Earth Observation governmental service would be beneficial to provide a fully reliable, highly resilient, and continuously available situational awareness service"(European Union Space Strategy for Security and Defence, 2023) the EU launched, in 2023, two feasibility studies for an EOGS. The EOGS will be a European space-based ISR constellation able to provide reactivity (e.g. tactical tasking of satellites and delivery of space ISR, if needed via a secure space-based communication infrastructure) and near real time monitoring (e.g. high revisit on areas of interest) while offering diversity of sources (e.g. night vision/infrared, hyperspectral, radar, signals intelligence). Such capability might take the form of a constellation of small satellites and complement existing high-end national/multinational governmental and commercial capabilities. It will also cover ground segment aspects, including, where possible, those promoted within the PESCO framework, including EDF22 SPIDER and the Common Hub for Governmental Imagery (CoHGI). Synergies with the EU Space programme will also be explored (e.g. shared use of the system based on predefined use cases, possible agreed governance and co-financing)(European Commission, 2024a). For the moment a study is undergo led by two consortiums, one led by Telespazio and the other one by OHB. The Commission proposed to help define the appropriate governance through a "pilot" which will be tested by SatCen and EUSPA within Copernicus during the 2021-2027 MFF, without prejudice to any decision on the future MFF. The Council also underlined the need to

respect the civilian nature of Copernicus and to maintain its current data and information policy.(European Union Space Strategy for Security and Defence, 2023)

4.1.3. EU-ESA Cooperation on Space

The legal basis for the ESA/EU cooperation is provided by a Financial Framework Partnership Agreement (FFPA), the most recent of which was officially signed on 22 June 2021. The agreement represents an EU investment of almost €9 billion in the period of 2021 to 2027. This funding adds to ESA's budget and consolidates an ambitious set of mandatory and optional programmes defined by ESA Member States. The FFPA defines the roles and responsibilities of all partners and ensures the level of autonomy of ESA that is needed to efficiently develop and implement the programmes.

In addition to that, In October 2021, ESA and the European Defence Agency (EDA) agreed to further expand their cooperation and it is considered that through "the two partners' deepening cooperation, Europe is better equipped to implement priority objectives across […] maritime security, intelligence, surveillance and reconnaissance, […] and Earth observation."(ESA, 2020a)

The EU-ESA Space Council offers opportunities to jointly discuss the development of a coherent overall European space programme. During the May 2024 Council both organisations recognised "the urgency of enhancing European autonomy as regards security, safety and resilience in and through space"(European Council, 2024). While also highlighting the importance to reinforce "the ESA-EU strategic partnership in its various forms of cooperation in view of fostering a globally competitive European space economy […] for the development of the overall European Space Policy".(European Council, 2024)

4.1.4. NATO

NATO sees the space environment as becoming more Diverse (multitude of actors), Disruptive (cheaper to access), Disordered (lack of updated laws) and Dangerous (greater range of threats). Threats to the space domain are considered in terms of counterspace capabilities (kinetic or not) or in term of congestion on the LEO; these threats are exacerbated by the high dependency of Western nations on space. Therefore, NATO Leaders agreed to further integrate space into the Alliance by

developing a new NATO Overarching Space Policy and by integrating space as a fifth operational domain capable of triggering Art. 5 of the Atlantic Treaty (collective defence). This approach to space is more of a rediscovery, as the Alliance had its own missile warning, SATCOM (satellite communication) and ISR (Geospatial intelligence) satellites from the 1970s until 2010.

According to NATO's overarching Space Policy, NATO's Approach to Space, outlines four key points for NATO. The first is to integrate "space and space-related considerations into the delivery of NATO's core tasks", particularly in collective defence. Second, to ensure "effective provision of space support and effects to the Alliance's operations, missions and other activities". Third, to serve "as a forum for political-military consultations and information sharing on relevant deterrence and defence-related space developments" (NATO, 2019), In the absence of its own satellites, NATO relies on individual states to provide this capacity, through national assets or commercial vendors.

On concrete space applications, NATO has signed for SATCOM a multi-year agreement with several Allies, and for ISR, NATO is developing a multinational Allied Persistent Surveillance from Space (APSS) program, which will consist of a virtual constellation of governmental satellites to provide imagery and support to the intelligence community. Finally, the Alliance will work on the resilience of space-based systems against the counter-space capabilities of its strategic competitors (RUS, CHN, IRN, PRK). NATO sees 6 key functional areas for space to enable all its operations and activities. On EO use for security, NATO considers that "Intelligence, surveillance and reconnaissance require space capabilities for strategic, operational and tactical assessment, situational awareness and to support decision-making and planning". On EO use for environment, NATO also considers that "Space-based monitoring of the atmospheric, oceanic and space environments is important for planning and execution of NATO missions and operations"(NATO, 2019). More generally, the Alliance plans to enhance its space activities and improve its Space Operations Centre. NATO is also poised to further integrate the space domain into its planning, exercises and operations, with a new Centre of Excellence in Toulouse contributing to the development of doctrine and trainings. In all its activities, NATO will also seek partnerships with other nations and international organisations (the UN and the EU) and promote responsible

behaviour in space more broadly. NATO also identifies challenges, namely the shortage of space professionals, the rapid pace of technological development and the unique nature of the military space domain.

Moreover, in a report dating back to March 2020, NATO defined core areas in which the inclusion of the domain of space emerges as a primary security frontier to ensure the Alliance's ability to defend its member States. It includes EO through integrated tactical warning and threat assessment; environmental monitoring; and surveillance and reconnaissance. The report considers that "communications and observation (i.e. C4ISR) have always been important motivators for the use of space." Therefore, NATO ACT has put efforts towards the "development of specialised EO/IR sensors (electro-optic/infrared) notably to support missile defence, SAR (synthetic aperture radar), ELINT (e.g. Automated Identification System (AIS))"(NATO STO, 2020). The investments in R&D are from the NATO Innovation Fund, supporting both emerging start-ups and established venture capital funds. For NATO's ability to conduct operations, EO data collected by satellite constellations are fundamental to provide NATO forces with accurate information on adversary armies' movements. Several NATO's most advanced systems result to be still dependent on space assets. Examples include the Integrated Air and Missile Defence (IAMD) programme, the Ground Surveillance System (AGS) and the Airborne Warning and Control Systems (AWACs).(Chabert, 2023)

In addition, since 2021, NATO has operated NATO Defence Innovation Accelerator for the North Atlantic (DIANA). It is designed to brings together universities, industry and governments to work with start-ups to develop deep-tech dual-use technologies to address critical defence and security challenges. This program focuses on emerging and disruptive technologies and aims to tackle critical issues in fields as diverse as artificial intelligence (AI), autonomous systems, quantum technologies, biotechnologies and space.(NATO, n.d.)

Many NATO allies possess their own EO capacities for ISR and NATO trends towards a unification of all these assets through common programs, while still not acquiring its own means. The unification will be done with the NATO's Allied Persistent Surveillance from Space (APSS) that is set to allow the Alliance's to monitor activities on the ground and at sea in an accurate and timely manner. With the signing of the Memorandum of

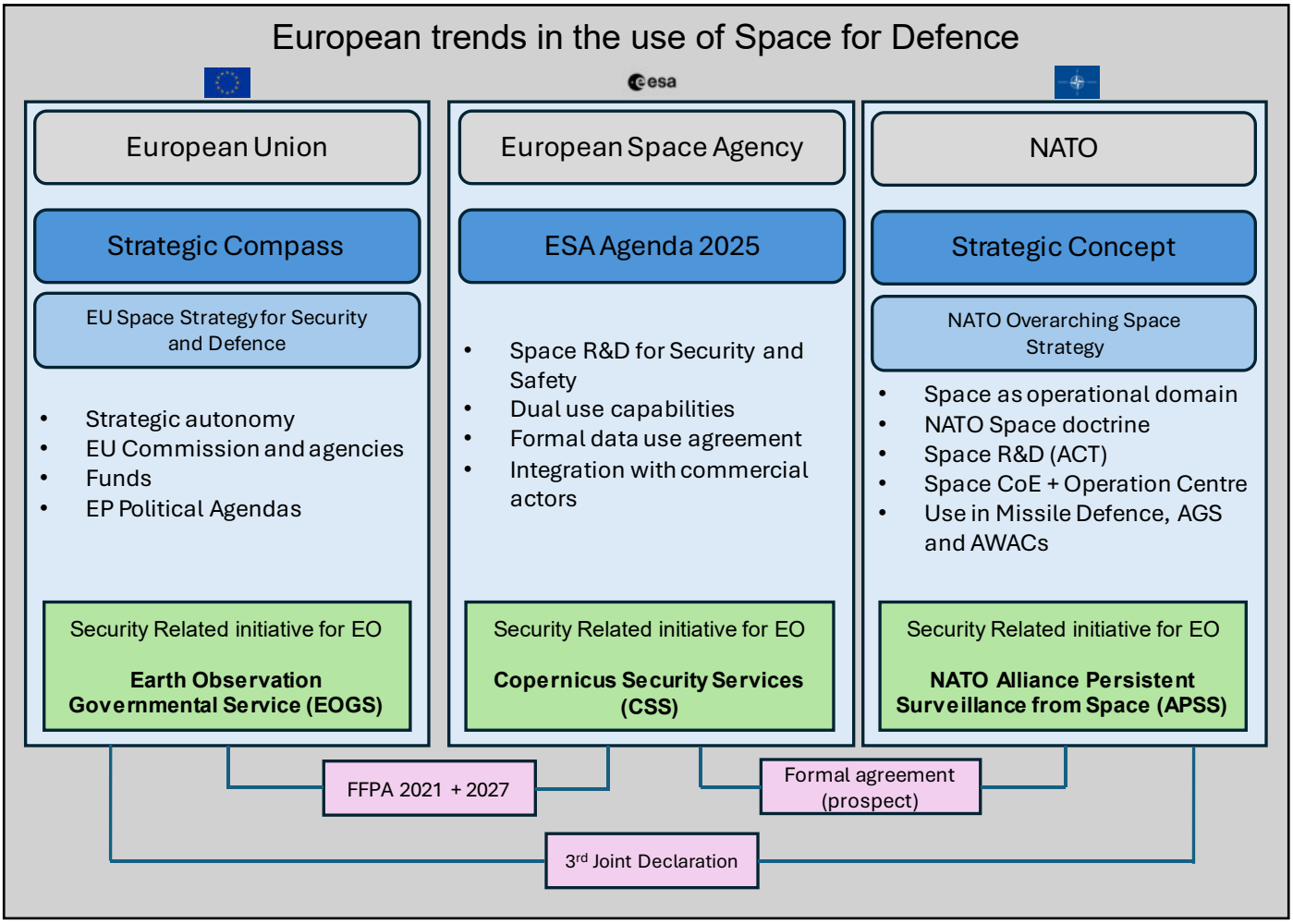
Understanding, APSS is now into the implementation phase in which over the next five years, 17 Allies are contributing the equivalent of more than $1billion to leverage commercial and national space assets, and to expand advanced exploitation capacities.(NATO, 2023) The APSS, will contribute to the development of assets in the field of Earth observation with a view to obtain a clear illustration of eventual military displacements on the ground. More precisely, the mechanism will establish a constellation of pre-existing government and commercial surveillance satellites known as Aquila, which will provide real-time information on enemy forces movements, state of terrains and weather conditions. In August 2024, Planet announced the signature of a contract to set the alliance with high-resolution data from Planet's SkySat fleet (Erwin, 2024). NATO's reliance on both governmental and commercial satellites means that it will undertake to make extensive use of the proliferation of LEO satellites. In wartime, it aims to increase the resilience of the NATO space enterprise. However, a key issue for wartime will be to ensure that the commercial capabilities being relied upon are in fact available for use as required.(Kramer et al., 2024)

4.1.5. EU – NATO Cooperation on Space

The EU and NATO want to further strengthen, deepen and expand their strategic partnership, political dialogue and cooperation regarding outer space. This goal has been presented in the third 'Joint Declaration on EU/NATO Cooperation', signed on 10 January 2023. The two organisations, want to address "the growing geostrategic competition, resilience issues, protection of critical infrastructures, emerging and disruptive technologies, [and] space".(NATO & EU, 2023) According to the publicly funded European think thank *Friends of Europe* "The two organisations look at space with very different eyes. NATO's approach is operational, whereas the EU's primary focus is promoting economic growth, scientific achievement and security, notably at its borders. […] there is a natural complementarity between NATO's analytical emphasis on space-based intelligence on regions outside Europe, and the EU's focus on Europe and its immediate neighbourhood. Space is one of the rare security areas in the relationship where the EU would not be a junior partner. With large existing dual-use capabilities, […] including Copernicus earth observation system, […] the EU has key assets of its own that are of interest to NATO." (Taylor, 2022)

4.1.6. Trends

Fig 5. Graphical Summary of the Relevant European Regulatory and Strategic Frameworks



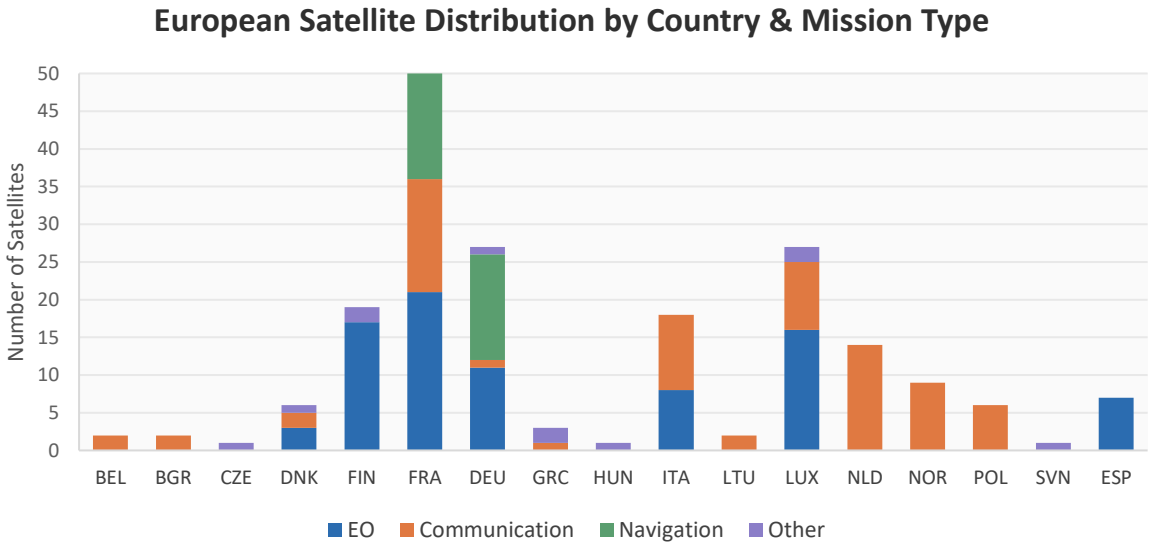
4.2. Health of the European Space Industry (to)

4.2.1. European Space Market

Defence-related space activities in Europe are predominantly driven by a core group of states possessing sophisticated industrial bases, specifically France, Germany, Italy, Spain, and the UK. These actors pursue developmental objectives through a mixture of unilateral investment and multilateral cooperation frameworks, often leveraging international organizations detailed previously. A prominent example is the EU space program within the 2021-2027 Multiannual Financial Framework, which allocated €14.88 billion for the designated period (European Commission, 2021c). Similarly, the European Space Agency utilizes a multinational budgetary structure to execute its

various mandates. Beyond these centralized efforts, less nationalized architectures exist, such as the Multinational Space-based Imaging System or MUSIS, which facilitates critical interoperability between national ground segments. While European orbital presence, defined here by functional satellites rather than scientific missions or the International Space Station, remains significant, it is largely fragmented among the individual nations of this study. To evaluate the second pillar of the Fiott (2020) framework regarding European strategic autonomy, this section examines the continent's capacity for independent space operations and the overarching vitality of the European space sector.

Establishing the necessary context for this analysis requires an initial survey of the specific orbital assets maintained by individual European nations. Earth observation and general remote sensing capabilities remain concentrated among a limited number of member states, whereas more recent entrants into the space sector tend to prioritize satellite communications (SATCOM) within their national agendas. Similarly, Positioning, Navigation, and Timing (PNT) infrastructures appear largely restricted to established space powers like France and Germany, given the significant industrial and financial demands of maintaining effective constellations; consequently, many other states remain dependent on the broader European Galileo framework. While the possession of sophisticated earth observation tools represents a critical step toward national sovereignty, such systems often encounter operational constraints regarding satellite revisit frequencies, responsiveness, and spectral diversity.



Data: (Lin et al., 2024; Union of Concerned Scientists, 2023)

As France, Germany, and Spain remain important space faring nations in Europe with a relationship to their size, a country stands out for the maturity of it space programme, it is Luxembourg. The success of Luxembourg's space presence can be explained by its regulatory frameworks and pro-business rules that facilitate it the implement action of new companies active in the field. The government established the Luxembourg Space Agency (LSA) in 2018 with a mandate focused on business development rather than leading mission execution by itself, it is also governed as a company headed by a CEO and not like a traditional governmental agency. The milestones that made Luxembourg so attractive, that it now hosts around 60 space companies that generate almost 2% of the country's GDP, is when it positioned itself in 2017 as the first European nation to adopt an open legal regime securing private property rights for materials and resources harvested in space. This opened the gateway to the targeting of the high-growth potential market of outer space mining, from asteroids to the moon. This strategy investing on space start-ups despite the inherent risks shows the engagement of Luxembourg to utilize strategic fiscal policies and research funding to align its space sector with long-term economic prosperity and European market leadership. Another possible incentive, especially in the field of earth observation, is the NATO GDP threshold for investment in defence, that is difficulty attainable for Luxembourg and its small armed forces in comparison to GDP, that positioned the country as an important investor into the Allian multinational space projects.

While major European powers such as France, Germany, and Spain maintain space-faring capabilities proportionate to their geopolitical scale, Luxembourg represents an anomaly due to the precocious maturity of its national space program. This institutional success stems largely from the implementation of agile regulatory frameworks and a commercialized governance model designed to lower entry barriers for emerging enterprises. By establishing the Luxembourg Space Agency (LSA) in 2018, the state departed from the traditional mission-led agency archetype, instead forming a business-oriented entity headed by a CEO. A pivotal moment for this ecosystem occurred in 2017 when Luxembourg became the first European state to codify a legal regime securing private property rights for resources extracted in situ. This legislative move effectively signalled the country's intent to dominate high-growth niches like extraterrestrial mining, attracting approximately 60 firms that now account for nearly 2%

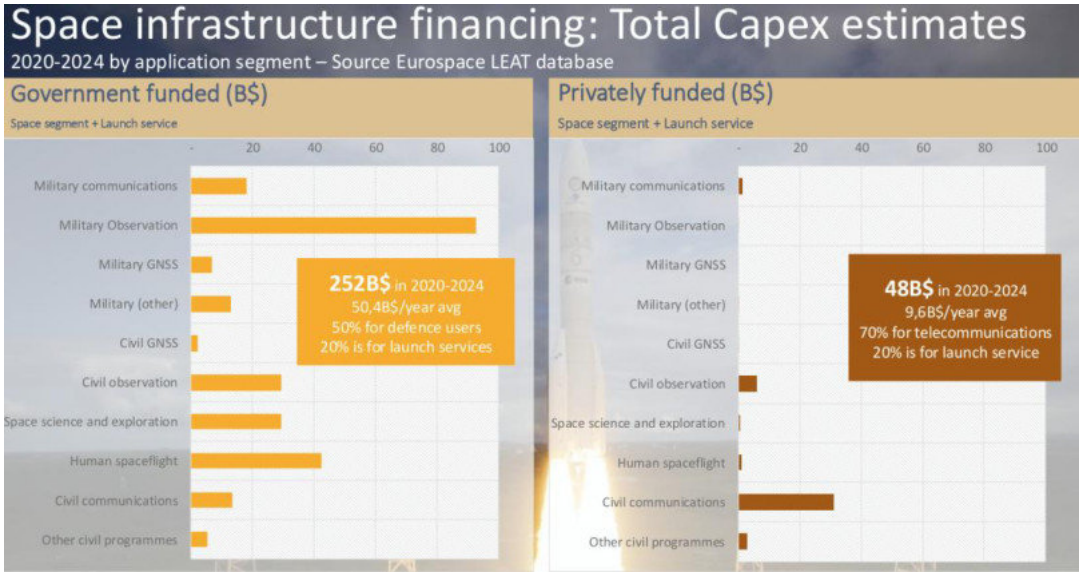
of the national GDP (Brennan, 2019). Such a trajectory indicates a calculated willingness to utilize strategic fiscal policy and targeted research funding to secure long-term economic resilience and continental leadership (Brennan, 2019). Additionally, the difficulty of meeting the NATO defence spending threshold through conventional military means has likely incentivized the Sultanate to pivot toward multinational alliance projects, particularly in earth observation, thereby fulfilling its security obligations through high-tech aerospace contributions (Hainaut, 2024).

Parallel to governmental developments, the European private sector continues to diversify its capabilities, deploying assets ranging from high-resolution satellites with rapid revisit rates to dense constellations of medium-resolution small satellites. These services, exemplified by Finnish SAR specialist ICEYE, cater to an expanding demographic of state and corporate clients. Although these commercial platforms are not exclusively engineered for defence requirements and possess inherent technical constraints, the inherent efficiency of the European New Space model facilitates the production of massive datasets at competitive price points. This cost-effectiveness serves as a primary driver for sustained investment and technological evolution within the sector.

A comprehensive analysis of the European space market requires an examination of its dual funding architecture, split between private venture capital and public sector allocations. Regarding the latter, primary financial support originates from national defence and space ministries, alongside institutional bodies like BPI France, Italy's CDP, and the European Investment Bank. Additional capital is channelled through the EU Space Programme and ESA via its established georeturn mechanism. Currently, defence users account for approximately 50% of space infrastructure investment (Eurospace, 2025), with a distinct emphasis on military-grade remote sensing. This market dominance is largely dictated by the exorbitant R&D and fabrication costs associated with next-generation sensors, particularly those designed to enhance spatial and spectral resolution or expand constellation capacity. Examples of this trend include the recent development of advanced RF remote sensing and hyperspectral sensors (Bataille, 2026). Furthermore, the human spaceflight segment has garnered renewed attention; the European launcher crisis, exacerbated by the geopolitical shifts following the Russian invasion of Ukraine, exposed significant vulnerabilities in the

region's reliance on Arianne and AVIO. Conversely, private investment remains comparatively modest, a reflection of the relative immaturity of the European New Space ecosystem. Private actors tend to prioritize downstream applications over resource-heavy hardware, focusing on data transformation and the Space as a Service model (Space Industry Database, n.d.). This shift toward service-oriented architectures may prove pivotal in attracting external capital by demonstrating tangible use cases, such as integrating Earth observation data into existing surveillance tools for monitoring supply chains and critical infrastructure.

Fig 6. Space Infrastructure Financing



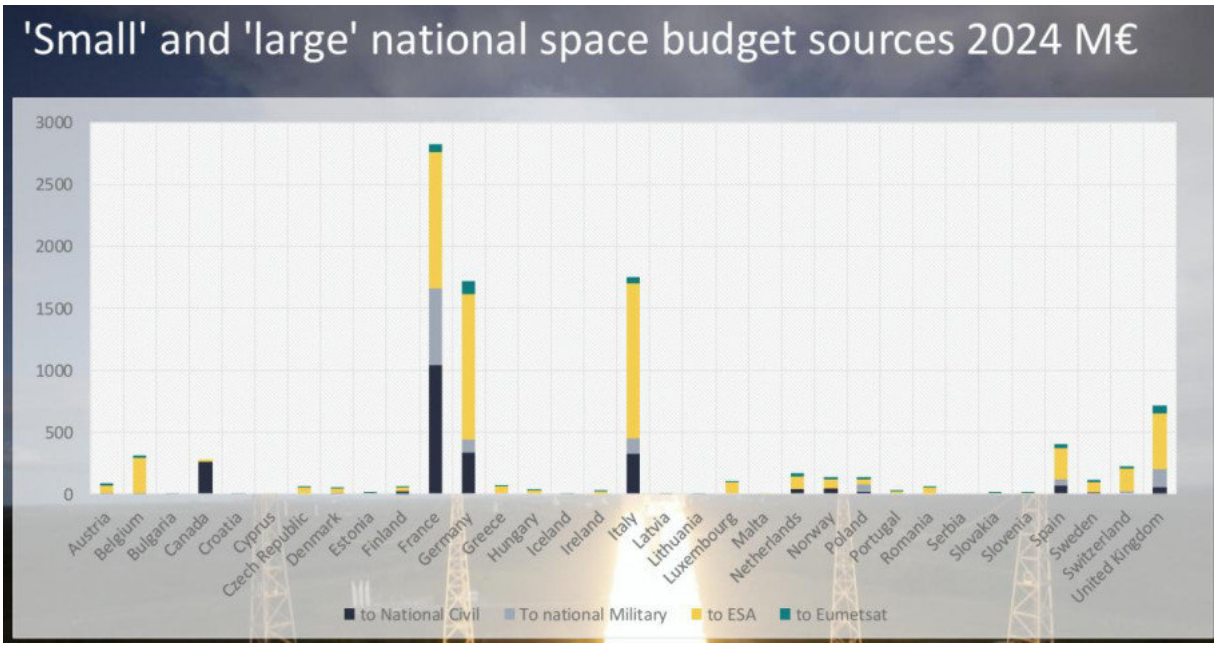
Source: (Eurospace, 2025)

4.2.2. Investments in Earth Observation

By 2025, the structural divergence between traditional and "new space" models remains pronounced; the preponderance of capital still originates from state actors who rely upon established aerospace conglomerates across the continent. These investments from European national governments typically flow through dedicated space budgets managed by national agencies or, in the case of emerging space nations, smaller ministerial departments. Disparities in funding levels among European states do not necessarily correlate with their total orbital assets but rather reflect their broader geopolitical influence within the region. Leading actors, notably France, Germany, and Italy, drive this sector by channelling significant resources into the European Space Agency to facilitate the pooling of technological expertise and

financial risk. Nevertheless, domestic investment continues to be a vital instrument of statecraft, particularly for France, which remains a primary architect of the drive toward European strategic autonomy discussed earlier in this study. Although the subsequent data illustrates the broader distribution of national space budgets, the persistent commitment to funding the European Space Agency underscores a dominant trend in regional space policy.

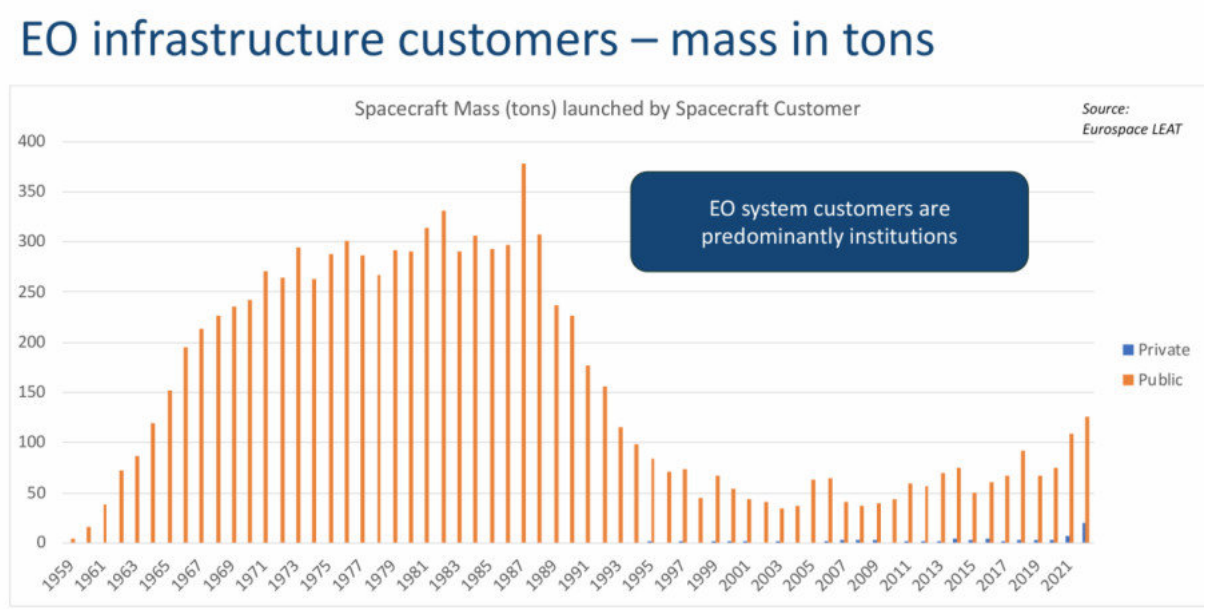
Fig 7. National Space Budgets 2024



Source: (Eurospace, 2025)

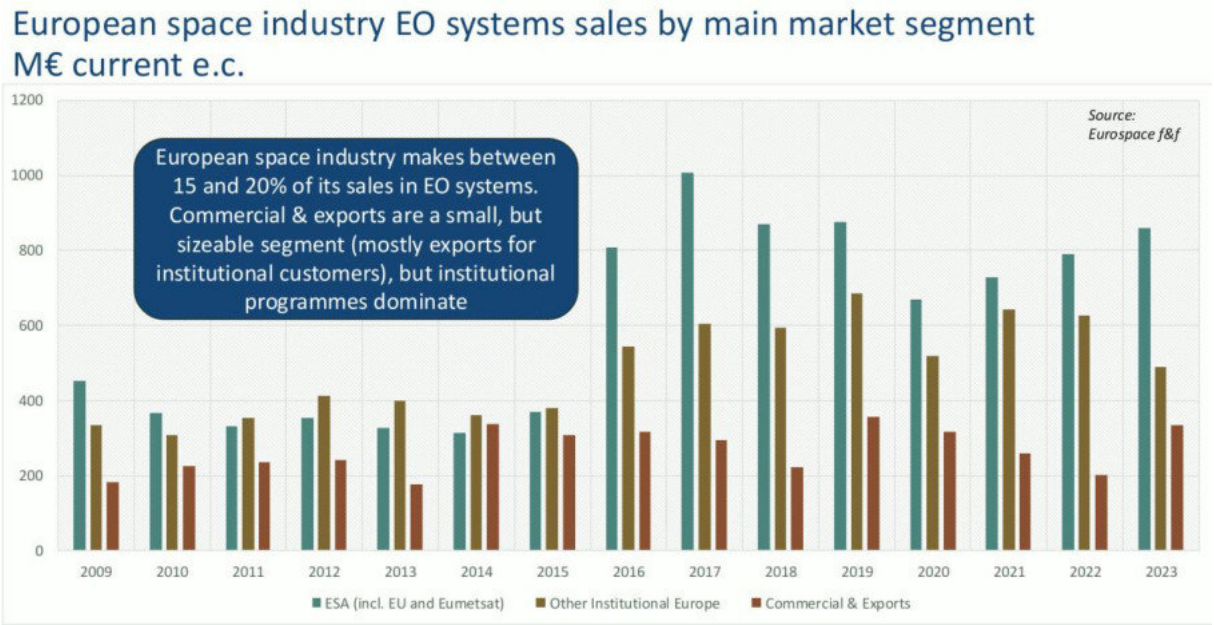
In the specific domain of earth observation, public procurement has historically functioned as the primary catalyst for industrial development since the inception of the Cold War space race. A sustained lack of penetration into the most dynamic international market segments has arguably compelled the European industry to deepen its reliance on institutional contracts, which currently constitute the overwhelming majority of total revenue (Golovtchenko, 2026). When examining the temporal data, a distinct contraction in the mass launched into orbit is evident following the Cold War's conclusion, succeeded by a significant resurgence around 2022 at the onset of the conflict in Ukraine. This pattern implies a robust correlation with defence expenditures, reinforcing the status of space systems as critical dual-use technologies that serve a pivotal function in contemporary warfare.

Fig 8. EO Infrastructure Customers



Source: (Lionnet, 2023)

Fig 9. European EO System Sales



Source: (Lionnet, 2023)

The European Space Agency persists as the Earth Observation (EO) sector's primary anchor customer, bringing approximately €1B in annual revenue into the industry. Given that private investment accounts for a mere 15-20% of total sales, institutional frameworks continue to underpin the broader market structure. This upward trajectory since the COVID-19 pandemic indicates an industry gaining significant momentum, maintaining consistent developmental progress over recent years. Conversely, the persistently low figures for exports and commercial sales underscore a relative immaturity in the sector's international footprint. These dynamic highlights a European space industry that appears constrained when measured against the expansive capabilities of global powers like the United States, China, Russia, and India.

4.2.3. Actors of the Earth Observation Industry

The emergence of the New Space industry signifies a pivotal shift in the space domain, driven by a surge in private investment and the proliferation of digitalized European industrial applications. Within the satellite sector, the downstream segment, often categorized as the insight pillar, comprises firms dedicated to generating value-added solutions from raw orbital data. A particularly salient actor for this investigation is Preligens, recently rebranded as Safran AI, which develops sophisticated software for the automated analysis of satellite imagery. These technological advancements represent a transformative shift with profound dual-use implications. By facilitating the seamless detection, attribution, and subsequent categorization of events (Safran, n.d.), such platforms offer a robust response to the fundamental challenges regarding resilience against hybrid threats identified in this research.

Fig 10. European New Space Ecosystem

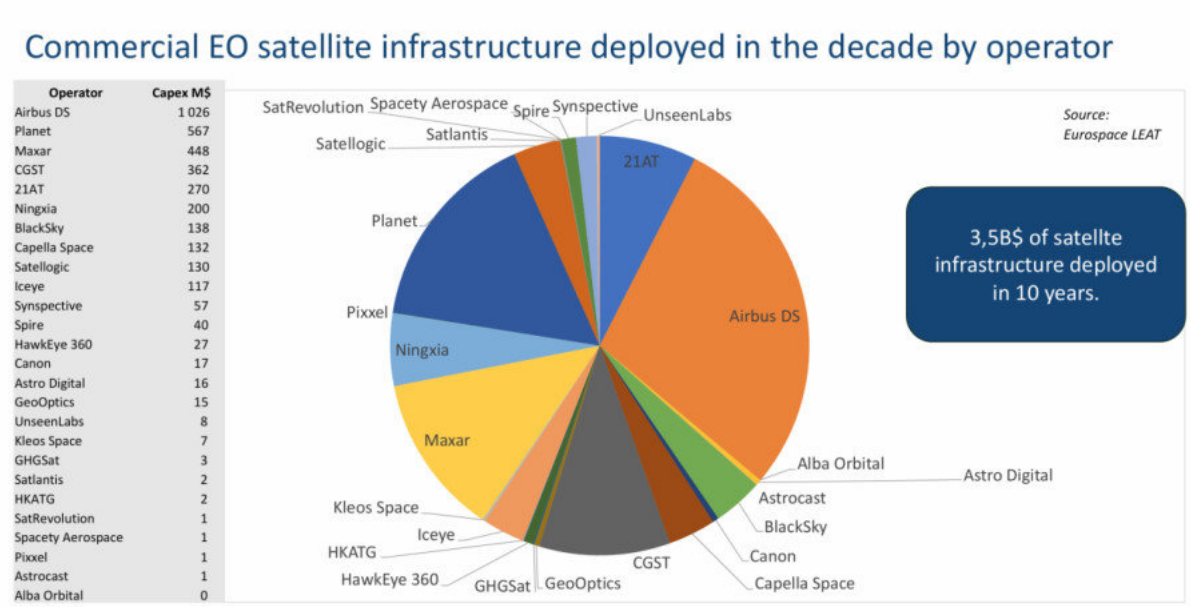
Source: (Ravichandran, 2021)

Regarding upstream capabilities and satellite operators, conceptualized here as Signals, several prominent European firms are beginning to exert a more defined influence within the Earth Observation (EO) market. Although non-European entities continue to dominate the New Space EO sector, as illustrated in the figure below, firms like ICEYE have established themselves as industry benchmarks for Synthetic Aperture Radar (SAR) imagery. This growth is often underpinned by public sector contracts, where security-related motivations remain a primary driver for procurement (Golovtchenko, 2026). In emerging technological niches such as radio frequency (RF) monitoring, the French firm Unseenlabs maintains a notable presence, effectively augmenting American solutions spearheaded by HawkEye 360 (Bataille, 2026). Concurrently, specialists in Very High Resolution (VHR) optical imagery, specifically Planet Labs and Maxar, retain their leadership by supplying critical data to news organizations, government agencies, and academic researchers.

Over the last decade, the development of EO satellite infrastructure has been dominated by Airbus Defence and Space. Representing the traditional aerospace sector, this single entity is responsible for constructing one-third of all EO infrastructure deployed during this period. Such a concentration of production highlights Airbus's

asymmetric influence on the global landscape, particularly through its role as the primary provider for the Copernicus constellation and various international programs. This legacy is further reinforced by the firm's entrenched position within the broader aviation industry. However, the reliance on a single, centralized corporation to this degree potentially introduces significant systemic risks.

Fig 11. Commercial EO Infrastructure per Operator



Operator	Capex M$
Airbus DS	1 026
Planet	567
Maxar	448
CGST	362
21AT	270
Ningxia	200
BlackSky	138
Capella Space	132
Satellogic	130
Iceye	117
Synspective	57
Spire	40
HawkEye 360	27
Canon	17
Astro Digital	16
GeoOptics	15
UnseenLabs	8
Kleos Space	7
GHGSat	3
Satlantis	2
HKATG	2
SatRevolution	1
Spacety Aerospace	1
Pixxel	1
Astrocast	1
Alba Orbital	0

Source: (Lionnet, 2023)

The domain of remote sensing has shifted from an exclusively state-controlled endeavour to a diversified landscape where private entities own approximately 40% of active satellites. Currently, over 60 corporations and 50 sovereign states manage space-based data collection assets, reflecting a significant decentralization of orbital power. Commercial providers increasingly prioritize the deployment of expansive constellations comprising small to mid-size satellites; these systems frequently provide spectral, radiometric, or temporal resolutions that complement or even exceed the capabilities of traditional high-spatial-resolution platforms. Such a structural evolution offers distinct advantages to tactical war fighters who depend upon persistent surveillance and near real-time intelligence. This burgeoning international commercial Earth Observation sector now functions as a highly competitive, integrated segment of the global information value chain, effectively reducing entry costs. Organizations like Planet, maintaining a fleet of roughly 200 satellites to image the Earth's landmass daily,

facilitate critical applications in crisis management and security. This trend toward militarized commercial utility was further underscored in 2022 when SpaceX inaugurated Starshield, a specialized satellite service tailored for government defence requirements. Starshield assets incorporate sophisticated functions including target tracking, optical and radio reconnaissance, and early missile warning (Roulette & Taylor, 2024).

To foster synergy across the spectrum of European Earth Observation initiatives, commercial systems and European Space Agency Member State capacities are integrated through the Copernicus Contributing Missions. This framework encompasses more than 20 distinct satellites designed to fill critical data gaps. The architecture includes Synthetic Aperture Radar platforms such as TerraSAR-X, Kompsat-5, COSMO-SkyMed, RADARSAT-2, and ICEYE, which deliver high-resolution radar imagery regardless of atmospheric conditions. These are supplemented by optical assets like SPOT 6/7, PlanetScope, Vision-1, and PLEIADES, which provide precision imaging within the visible spectrum. The mission portfolio continues to broaden its technical scope by incorporating multi-spectral, thermal infrared, and hyperspectral sensors, alongside atmospheric composition instruments operating across various resolutions.

These missions are “delivering data that complements the output of the Copernicus Sentinel missions”(European Commission, 2023), supporting critical applications in environmental monitoring, disaster management, and security services. The “CCM satellites help cover the needs of Copernicus Service Providers, particularly for very high-resolution data and new space data.”(European Commission, 2023)

Commercial enterprises currently spearhead research and development for emerging space-based Earth Observation (EO) capabilities across the entire sensor technology spectrum. These advancements provide critical utility to security actors, particularly within the context of the Ukrainian conflict and in addressing multifaceted hybrid threats. Regarding optical imagery, the war in Ukraine has highlighted the role of Maxar and other commercial operators like Planet Labs, Pléiades Neo, and BlackSky. These entities deliver high-resolution data capturing Russian logistical convoys, troop concentrations, and airfield operations. Such imagery has been disseminated

extensively through the media (Höyhtyä & Uusipaavalniemi, 2023) and utilized by the Ukrainian Armed Forces to inform tactical planning and shape global perceptions of the hostilities.

In the domain of Synthetic Aperture Radar (SAR), the firm ICEYE enables the Ukrainian military to access radar satellite data at a critical temporal frequency (ICEYE, 2026), alongside specialized video radar functions. A broader ecosystem including Capella, PredaSAR Corp, Umbra Lab, and Synspective, alongside established systems such as TerraSAR-X and Cosmo-SkyMed, continues to expand commercially owned SAR constellations. These assets are significant for their ability to penetrate atmospheric obstructions and maintain persistent surveillance regardless of diurnal cycles.

Developments in infrared and hyperspectral sensing by companies such as HySpecIQ, Teledyne, Constellr and Orbital Sidekick introduce the capacity to identify specific chemical compositions from orbit. While such technology allows agricultural firms to optimize crop distribution, its security application lies in the potential to differentiate between natural foliage and camouflage materials concealing military hardware. Furthermore, in the realm of Radiofrequency and signals intelligence (SIGINT), providers like Unseenlabs, HawkEye360, and Aurora Insight have pioneered satellite-based radio frequency (RF) remote sensing. By geolocating diverse RF emitters, these systems facilitate maritime tracking and search-and-rescue operations. Similarly, developers Spire and Kleos are deploying constellations designed to detect RF signatures, offering specialized capabilities for monitoring global shipping lanes and identifying instances of GNSS interference.

4.2.4. Trends

Institutional investment serves as the primary engine for industrial innovation within a European space sector fundamentally defined by a public-contract-driven model. At the heart of this framework lies the European Space Agency (ESA) and its Geographical Return principle. This mechanism facilitates a balanced distribution of high-tech capabilities among the continent's leading space nations, specifically France, Germany, Italy, the UK, Luxembourg, and Spain, while fostering a reciprocal industrial ecosystem that aligns national economic growth with shared European objectives. As

Europe navigates an increasingly competitive global landscape, particularly in Earth Observation (EO), the region appears to be approaching a state of strategic autonomy. The continent currently possesses sophisticated end-to-end capabilities, ranging from advanced sensor development and data analytics to independent launch systems. This comprehensive infrastructure positions Europe as a sovereign power rather than a mere participant in the global space economy. By securing its own launch capacities and technical infrastructure, the continent remains equipped to monitor its borders and manage environmental data independently of external actors, thereby addressing its security and scientific requirements through domestic technological means. Nevertheless, further advancements are likely required regarding temporal resolution and emerging technologies, including radio frequency sensing, automated data processing, Very Low Earth Orbit operations, and expanded investments in hyperspectral capabilities.

4.3. Assessment of Europe's EO capacity (from)

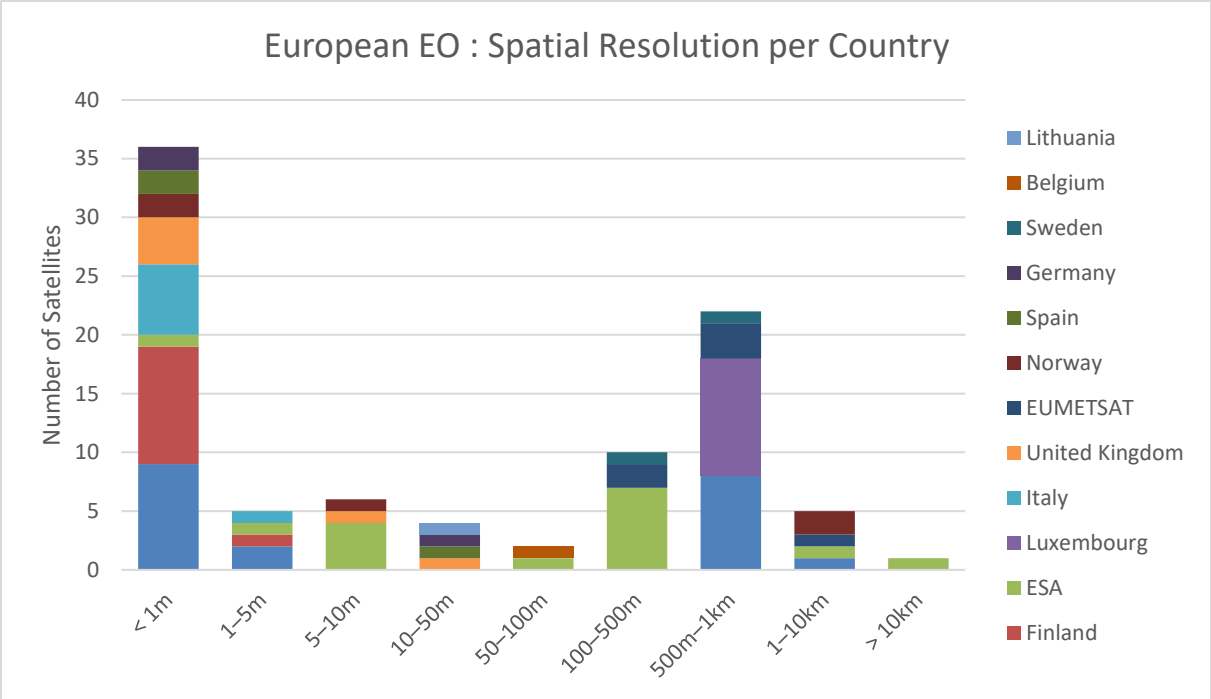
Having evaluated Europe's political commitment to integrating Earth Observation (EO) into its security architecture against hybrid threats facilitated by its three primary space organizations, the analysis shifted toward the industrial landscape. This previous examination detailed the corporate ecosystem and identified critical technologies attracting significant investment. To complete the theoretical framework established by Fiott (2020), the focus now turns to "Autonomy From." This entails assessing Europe's domestic EO capabilities through the technical criteria defined earlier. Utilizing the dataset compiled by (Lin et al., 2024), this section scrutinizes European assets across three dimensions: spatial resolution, which dictates pixel clarity; temporal resolution, concerning the revisit frequency over specific coordinates; and spectral resolution, denoting the range of electromagnetic frequencies captured by various sensors.

Beyond these technical parameters, the discussion extends to practical applications by building upon the GMES Working Group on Security (2003) diagnostic framework. This approach correlates specific spatial, temporal, and spectral requirements with a spectrum of security operations relevant to counter-hybrid warfare, highlighting which states or organizations lead in capability and how their contributions coalesce. To

contextualize these findings, Europe's capacities are weighed against those of major space competitors, specifically China, Russia, and India. Such a comparison serves to isolate existing technological gaps and project the trajectory of European development and its future strategic presence in the space domain.

4.3.1. Spatial Resolution

The spatial resolution of European Earth Observation (EO) satellites remains a critical variable determined largely by orbital altitude; while satellites in Low Earth Orbit (LEO) frequently approach a one-meter resolution, those in Geostationary Orbit (GEO) typically yield much coarser data ranging from 500m to 1km. This disparity stems from divergent mission requirements and the physical distance from observed targets. GEO platforms are primarily utilized for meteorological and environmental monitoring, where wide-area framing of entire continents takes precedence over granular detail. Furthermore, the onboard sensor architecture dictates specific capabilities. Within the LEO segment, the drive toward higher precision has established the categories of Very High Resolution, covering imagery under 30cm, and Ultra High Resolution (UHR), which provides approximately 10cm resolution. Currently, European sovereign capabilities lack UHR assets, a gap reflected by their omission from the subsequent data visualization. Nevertheless, European governmental users may still access UHR data via American commercial providers, exemplified by the Albedo Space Clarity-1 satellite (eoPortal, 2025b).

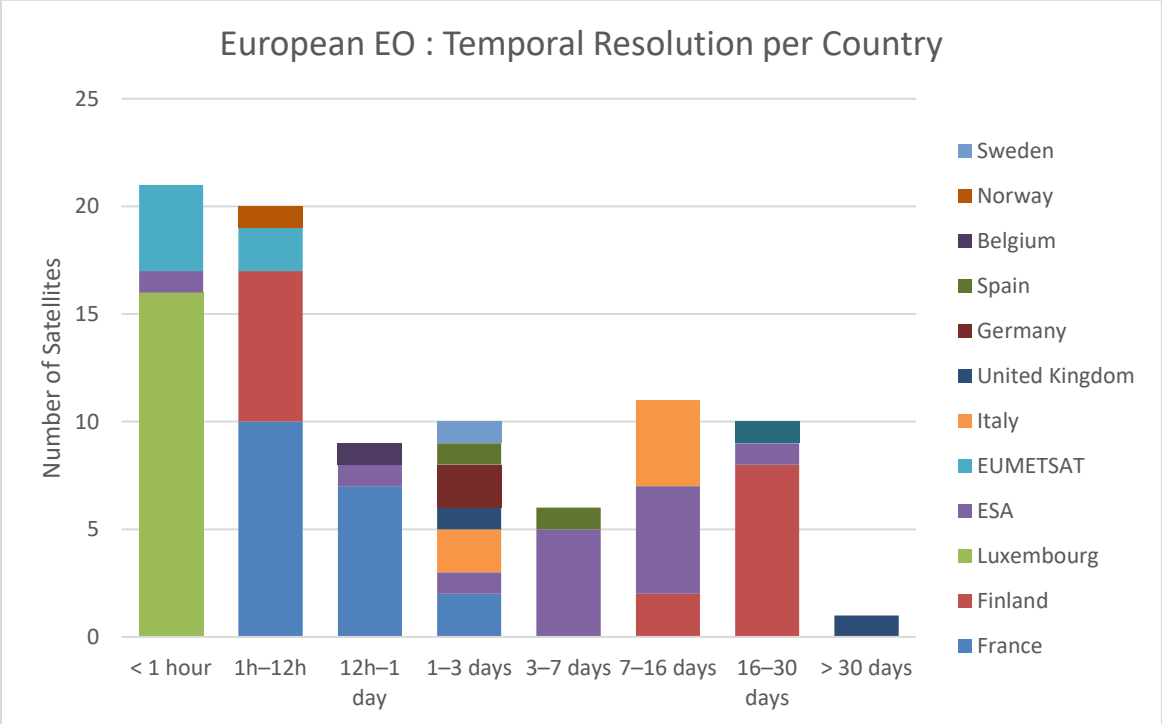


Data: (Lin et al., 2024)

European space assets exhibit a pronounced strategic polarization, favouring high-precision imaging with more than 35 satellites operating at sub-one-meter resolution. This dominance, largely spearheaded by French investments in the Pléiades series and Finnish advancements with the ICEYE constellation, underscores a concerted focus on intelligence, surveillance, and high-fidelity mapping. A distinct capability gap appears in the mid-resolution range between 5m and 100m, suggesting that operators prioritize either Very High Resolution (VHR) for tactical military and commercial applications or coarser coverage for environmental monitoring. A secondary cluster subsequently emerges in the 500m to 1km range, driven primarily by EUMETSAT and ESA. These organizations rely on Geostationary (GEO) assets to capture continental-scale data essential for global meteorological forecasting. Such a distribution highlights a bifurcated European strength: the maintenance of elite VHR reconnaissance capabilities alongside a robust infrastructure for large-scale Earth observation. While the mid-range remains less prevalent than VHR, it is still utilized by ESA to facilitate open data through the Copernicus constellation, a strategy that potentially mitigates the risk of providing overly precise actionable intelligence to adversarial actors or commercial competitors.

4.3.2. Temporal Resolution

The temporal resolution of European space assets reveals a strategic emphasis on rapid revisit capabilities, evidenced by a high concentration of satellites in the <1 hour and 1–12-hour categories. Such prioritization of near-real-time data appears essential for mission-critical applications including infrastructure monitoring, disaster response, and military intelligence, surveillance, and reconnaissance (ISR). Data suggests that EUMETSAT maintains a dominant role within the fast-revisit sector; its geostationary meteorological satellites offer continuous coverage, ensuring a robust presence in the <1 hour bracket. In contrast, a notable gap emerges in the medium revisit range of 3–16 days. This vacuum potentially indicates a capability shortfall for sectors such as agricultural monitoring and land-use change detection, which typically rely on consistent weekly observations rather than hourly updates.



Data: (Lin et al., 2024)

Temporal dynamics within the European space sector indicate that revisit frequencies of under one hour are generally the domain of meteorological or specialized sensors, whereas traditional high-resolution optical platforms typically necessitate longer intervals between successive passes. This accelerated temporal coverage increasingly relies on the proliferation of satellite into a so-called constellation, a structural shift where multiple small or medium-sized assets operate in a coordinated

fashion to minimize the latency between data captures. Although France and Finland demonstrate significant capacity within the 1–12-hour range, a granular analysis of the data suggests that European operators face lingering gaps in high-frequency temporal resolutions, particularly as aggregate figures appear skewed by the large-scale deployments of ICEYE, BRO, and Lemur-2. Such multi-satellite networks facilitate a level of persistent overhead presence that remains unattainable for legacy single-platform missions. The integration of these capabilities is best observed through the Copernicus Contributing Missions (CCM) framework, which aggregates diverse European Earth Observation data to ensure that institutional users can access the specific resolutions deemed most critical to their operational requirements.

Table 6. European EO Constellations

Constellation	*Temporal Resolution*
Lemur-2 (Spire)	<12h
BRO (UnseenLabs)	<12h
ICEYE	1 day
CSO	1 day
Pléiades	1 day
Copernicus	1–3 days
COSMO-SkyMed	1–3 days
CERES	1–3 days
Deimos	1–3 days

Data: (Lin et al., 2024)

The case of Lemur is interesting, as Luxembourg's prominence in high temporal resolution data is the result of a deliberate, decade-long national strategy to transform the country into a global "New Space" hub. By utilizing the LEMUR constellation, Luxembourg benefits from international capacities because Spire Global a US based company operates over 100 active nano satellites, that can achieve a high revisit rate, passing over specific geographic areas multiple times per day. In comparison, Unseenlabs with their Breizh Reconnaissance Orbiter (BRO) constellation, achieves high temporal resolution primarily through their important constellation and its technologies reducing the need for multiple satellites to detect an RF signal. By eliminating the need for formation flying, they can spread their constellation across diverse orbits to maximize coverage frequency. This, combined with a sensor that has massive swath regardless of cloud cover or daylight, ensures that they can provide

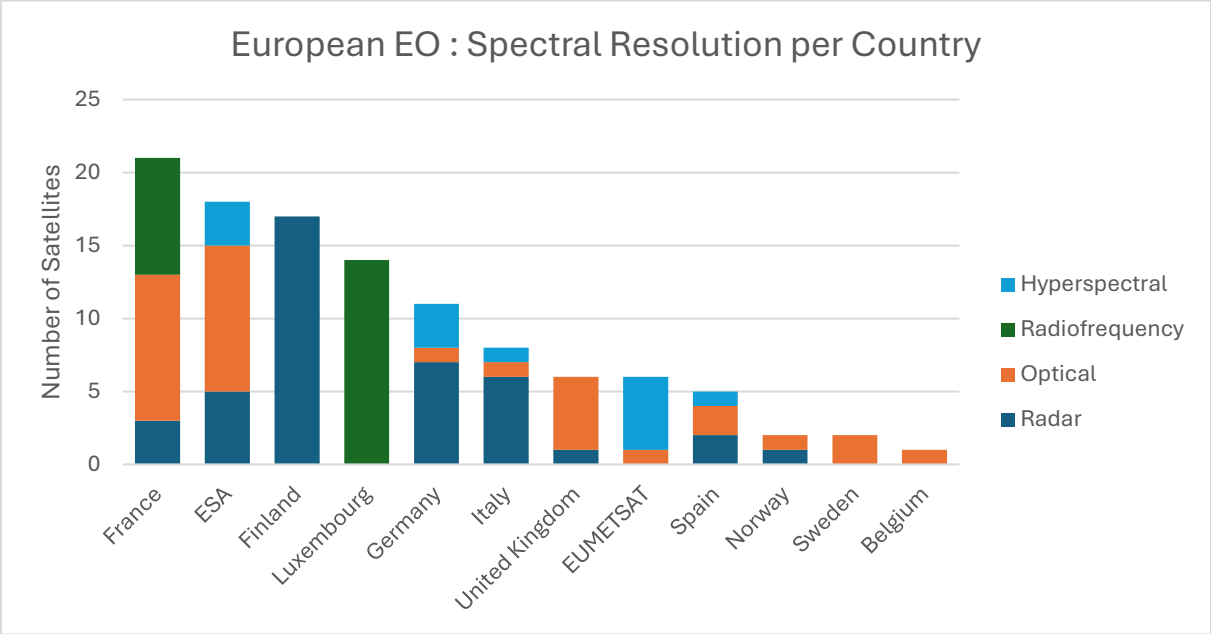
revisit times of less than an hour for any point on the globe. The latter position itself like an autonomous French and European capacity, being a competitor to its American equivalent HawkEye 360.

The case of the LEMUR constellation is particularly instructive, as Luxembourg's prominence in high temporal resolution data reflects a deliberate, decade-long national strategy to establish the Grand Duchy as a global "New Space" hub. Through the integration of the LEMUR fleet, Luxembourg leverages significant international capacities; Spire Global, a United States-based firm, operates a network of over 100 active nanosatellites that achieve a high revisit rate by passing over specific geographic coordinates multiple times daily (eoPortal, 2025c). In contrast, the French firm Unseenlabs utilizes its Breizh Reconnaissance Orbiter (BRO) constellation to secure high temporal resolution through a proprietary technological approach that minimizes the hardware traditionally required for radio frequency (RF) signal detection. By dispensing with the necessity for formation flying or tri-satellite clusters, Unseenlabs can distribute individual satellites across diverse orbits to optimize coverage frequency. This architectural efficiency, paired with a sensor capable of maintaining a massive swath regardless of cloud cover or diurnal cycles, enables revisit times of under one hour for any location on Earth (eoPortal, 2025a). Consequently, Unseenlabs represents an autonomous French and European capability, positioning itself as a strategic competitor to the American equivalent, HawkEye 360 (Bataille, 2026).

4.3.3. Spectral Resolution

The distribution of sensor types suggests distinct strategic specializations among European space actors, with France maintaining the most diversified sovereign portfolio. French assets appear balanced across optical, radiofrequency, and radar technologies, a configuration that aligns with its pursuit of strategic autonomy and comprehensive security applications. Conversely, nations such as Finland and Luxembourg have adopted highly specialized infrastructure models. The Finnish fleet remains exclusively focused on Synthetic Aperture Radar (SAR) via the ICEYE constellation, while Luxembourg concentrates its national capabilities on radiofrequency monitoring through Lemur-2 satellites integrated into the Spire network. These diverging paths indicate a European landscape bifurcated between broad

multispectral architectures and niche technological concentrations often driven by the presence of a single dominant domestic firm.



Data: (Lin et al., 2024)

The European Space Agency, primarily through the Copernicus constellation, maintains a central position in Earth Observation data acquisition, particularly within the optical sector where it leads via specific Sentinel satellites and specialized scientific missions like EarthCare designed for cloud and aerosol atmospheric monitoring (ESA, 2024). ESA further demonstrates substantial technical breadth through its deployment of Synthetic Aperture Radar and hyperspectral sensors. Given the high capital requirements and the necessity of a sophisticated industrial base, hyperspectral capabilities remain concentrated among a select group of actors, including Germany, Italy, and EUMETSAT, for targeted monitoring objectives. Conversely, for nations with nascent space sectors and more limited satellite fleets, such as Norway, Sweden, and Belgium, strategic priorities typically gravitate toward standardized optical and radar applications. These technologies continue to function as the essential pillars for smaller-scale national space programs. Consequently, these states appear to rely on broader European programs to address specific deficiencies in spectral resolution.

4.3.4. How Autonomous is Europe in its Defence Against Hybrid Threats

Utilizing the diagnostic framework established by the GMES Working Group on Security (2003), this section correlates existing European space-based capabilities with the requirements of various security applications, many of which prove central to countering hybrid threats. Previous analysis indicates that specific deficiencies persist regarding spatial resolution at the Ultra High-Resolution level, temporal resolution for sub-daily revisit frequencies, and spectral resolution, specifically concerning hyperspectral sensors. Nevertheless, the current European architecture appears sufficient to support the full range of security applications identified by the working group.

Table 7. Diagnostic Framework with Countries Capabilities

Task	**Main Sensor(s)**	**Resolution (m)**	**Revisit Time**	**Countries with Capable Satellites**
Industrial plant analysis	Optical, Thermal, Multispectral	0.5 - 2 2 - 10 1 - 4	Mthly, Qtly	France, Spain
Airfield analysis	Optical	1 - 2	Possibly	France, Spain
Barracks analysis	Optical	1	Possibly	France, Spain
Port analysis	Optical	1 - 5	Possibly	France, Spain
Aircraft identification	Optical	1	Not necessary	France, Spain
Missile identification	Optical	0.7	Not necessary	France
Radar identification	Optical	0.4	Not necessary	France
Treaty verification	Optical, Multispectral	0.5 - 2 1 - 4	Possibly	France, Spain
Crisis management	Optical, Radar	1 - 5 1 - 5	Frequent	ESA, Finland, France, Germany, Italy, Spain
Flood analysis	Radar, Optical	2 - 15 2 - 10	Frequent	ESA, Finland, France, Germany, Italy, Spain
I&W monitoring	Optical, Radar	0.5 - 1 1 - 3	Frequent	ESA, Finland, France, Germany, Italy, Spain
Camouflage detection	Multispectral	1 - 2	Not necessary	France, Spain
Terrain analysis	Optical, Multispectral	3 – 10 5 - 15	Not necessary	ESA, France, Spain
Coastal monitoring	Radar, Optical	2 - 15 2 - 10	Frequent	ESA, Finland, France, Germany, Italy, Spain
Route study	Optical	0.7 - 5	Not necessary	France, Spain
Evacuation planning	Optical	0.7 - 5	Not necessary	France, Spain
Humanitarian intervention	Optical	1 - 5	Frequent	France, Spain
Damage assessment	Optical, Multispectral	0.5 - 2 1 - 4	Frequent	France, Spain

Oil spill monitoring	Radar, Optical, Multispectral	2 - 15 2 - 10 2 - 10	Frequent	ESA, Finland, France, Germany, Italy, Spain
Peace keeping	Optical, Radar	0.5 - 2 1 - 8	Frequent	ESA, Finland, France, Germany, Italy, Spain
Peace enforcing	Optical, Radar	0.5 - 1 1 - 8	Very frequent	Finland, France, Germany, Italy
Point Location DGI	Optical	0.7 - 1	Not necessary	France, Spain
Local DGI	Optical	1 - 2	Not necessary	France, Spain
Regional DGI	Optical	5 – 10	Not necessary	ESA, France, Spain
Wide Area DGI	Optical	10 – 30	Not necessary	ESA, France, Spain, United Kingdom
Technical intelligence	Optical, Hyperspectral	0.10 – 0.30 1 - 3	Required	France

Data: (GMES Working Group on Security, 2003; Lin et al., 2024)

Data provided by the working group identifies France and Spain as the primary drivers of European military and dual-use space capabilities. France maintains its regional leadership through an assertive defence posture, utilizing the Pléiade, CERES, and CSO constellations to deliver Very High Resolution optical and radar imagery on a daily revisit schedule. While Spain possesses a numerically smaller fleet, its Deimos optical sensors and PAZ radar satellite offer the requisite resolution for a diverse array of security applications. Other actors, including ESA, Finland, Germany, Italy, and the United Kingdom, contribute capabilities better suited for civil-security intersections; these assets often prioritize environmental monitoring, maritime modelling, or the technical requirements of peace operations. Collectively, these national contributions from the industrial and technological foundation of European strategic autonomy. By strengthening sovereign Intelligence, Surveillance, and Reconnaissance (ISR) capabilities, these states ensure that Europe functions as a peer partner to the United States rather than a subordinate entity.

The strategic utility of European Earth Observation (EO) assets becomes evident when analysing the security applications discussed above. European Space Agency (ESA) officials highlight the 2014 investigation into the Malaysia Airlines flight over Ukraine as a definitive case study for the Copernicus program's role in facilitating unclassified data dissemination. While the Dutch-led criminal investigation relied heavily on high-resolution imagery provided by the United States, the restrictive classification of those American assets hindered broader information sharing. In this context, independent

European data capacity proved essential; unclassified Copernicus imagery provided a verifiable visual baseline that complemented the sensitive analysis produced by US authorities. Such contributions allowed Europe to integrate its sovereign technical capabilities into a unified situational awareness framework. By establishing a paradigm where open EO data functions as a credible source for international crisis fact-finding, the EU moves toward a model of technical autonomy. This ensures that European institutions remain primary contributors to global security dialogues instead of functioning as mere consumers of third-party intelligence.

4.3.5. Comparison with Europe's competitors

Contemporary space dynamics reveal that over 30 states have matured significant indigenous space capabilities, contributing to a global landscape where approximately 84 countries currently manage satellite operations. Beyond the established Western hegemony of the United States and Europe, the largest remote sensing satellite fleets are maintained by China, India, and Russia. Additionally, these countries, "are reportedly capable of employing their respective civil and commercial remote sensing satellites to supplement military-dedicated capabilities."(NASIC, 2018)

China maintains a sophisticated architecture of optical and radar Earth Observation (EO) satellites, providing a consistent, very high-resolution (sub-metric) monitoring capacity regardless of weather conditions. This reconnaissance and remote sensing infrastructure comprises over 230 satellites across diverse orbits, serving a triad of civil, commercial, and military functions. Notably, the People's Liberation Army (PLA) reportedly operates approximately half of this fleet, leveraging these assets to enhance the monitoring, tracking, and targeting of adversarial forces(Funaiole et al., 2026). Such a robust orbital presence grants the PLA significant situational awareness over regional competitors, specifically India and Japan, and facilitates persistent surveillance of geopolitical flashpoints like the Korean Peninsula, Taiwan, and the East and South China Seas.

The structural backbone of this capability includes the Fengyun meteorological series, Haiyang for maritime observation, Ziyuan for natural resources, and Gaofen for near real-time surveying, alongside the Yaogan and Tianhui mapping constellations. With more than 100 additional EO satellites scheduled for launch, Beijing is prioritizing the

expansion of multifunctional, high-resolution platforms tailored for security applications. Chinese research and development in this sector have been particularly aggressive, yielding breakthroughs in geostationary (GEO) high-resolution observation. This evolution is evident in the transition from the Gaofen-4 optical satellite, launched in 2015 with a 50-meter resolution, to the Gaofen-13, which achieved 15-meter resolution. Projections suggest the upcoming Yaogan-41 may reach a 2.5-meter resolution in GEO (Smid, 2022), a threshold sufficient for identifying individual aircraft in flight. Parallel advancements in Synthetic Aperture Radar (SAR) include the Ludi Tance-4, recognized as the inaugural geosynchronous SAR satellite with a 20-meter resolution (Jones, 2023). These GEO-stationed assets provide the high temporal persistence and video-like monitoring capabilities essential for modern strategic oversight.

A significant portion of these Earth Observation assets remains integrated into the High-resolution Earth Observation System (CHEOS), a framework inherently designed for dual-use applications. Parallel to state initiatives, the Chinese commercial sector actively develops expansive constellations; Changguang Satellite Technology, for instance, aims to deploy a mega constellation by 2030 capable of achieving a ten-minute temporal resolution. This ecosystem is defined by the profound integration of governmental and commercial interests, a structural alignment suggesting that Beijing maintains seamless access to data harvested by private entities (Swope, 2024). Beyond domestic consolidation, China has fostered multinational EO partnerships, including projects with ESA member states such as the CFOSat oceanographic mission with France and the Zhangheng-1 meteorological satellite developed alongside Italy.

India maintains an extensive civilian remote sensing infrastructure through the Indian Remote Sensing (IRS) program, which provides critical data for agriculture, forestry, and disaster management. While the IRS serves broad developmental goals, the CARTOSAT series focuses on high-resolution cartography and strategic imaging, directly supporting military requirements. The inclusion of the RISAT series, equipped with Synthetic Aperture Radar, further expands India's all-weather surveillance capabilities. Recent advancements under the EOS designation continue this trajectory; for example, the LEO-based EOS-1 supports diverse sensing applications, while the geostationary EOS-3 and EOS-5 (GISAT-1 and GISAT-2) provide 50m multispectral resolution for real-time monitoring of weather and terrestrial resources. These systems

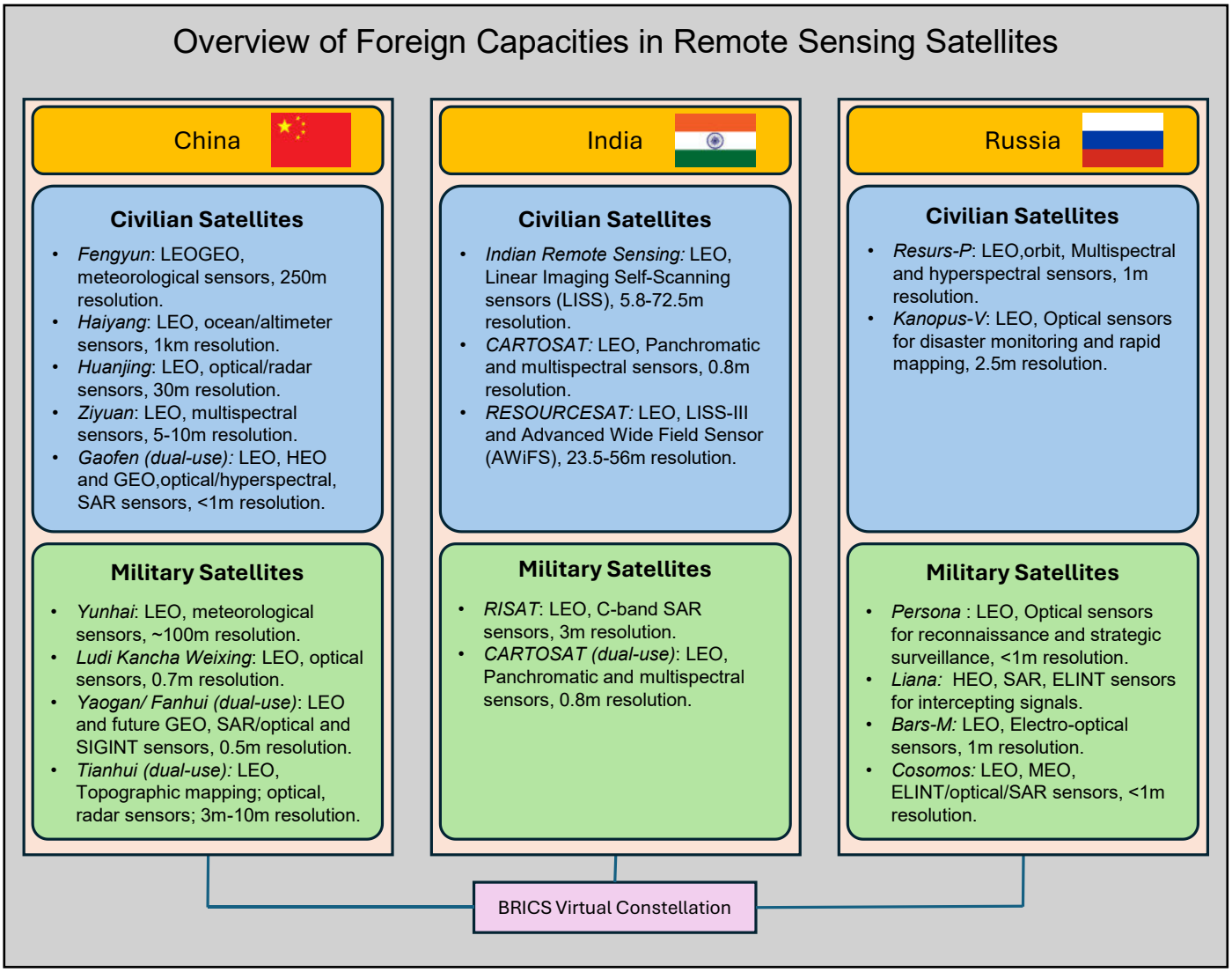
possess significant dual-use potential, effectively bridging the gap between civilian requirements and national security imperatives (Jaiswal, 2022).

The Resourcesat series represents a fundamental pillar of India’s Earth observation architecture, functioning as a high-fidelity multispectral system. Beginning with Resourcesat-1, the program was engineered to deliver granular data for agricultural oversight, forestry, and disaster mitigation, a legacy sustained by the subsequent Resourcesat-2 which provides critical inputs for national sustainable development and environmental governance. Notably, the latter also functions within the Copernicus Contributing Missions framework. Beyond state-led initiatives, India’s commercial space ecosystem has emerged as a formidable actor. Private entities now operate sophisticated assets including Pixxel’s hyperspectral constellation, ABA’s multispectral optical platforms, and TATA’s sub-meter resolution EO satellites (Krebs, n.d.). These commercial ventures augment governmental programs, effectively expanding India’s strategic depth in remote sensing.

Russia's remote sensing infrastructure has undergone significant maturation to address a dual-use spectrum of civilian and military requirements. This capability is anchored by diverse satellite families, including the Resurs, Kanopus-V, Persona, Bars-M, and Liana series. While Resurs-P units provide high-resolution hyperspectral imagery for resource management, the Kanopus-V constellation utilizes medium-resolution optical sensors tailored for land use and disaster monitoring. Conversely, the Persona series, deployed between 2008 and 2015, facilitates high-resolution optical reconnaissance for the defence sector, complemented by the Bars-M system’s focus on electro-optical cartography. The Liana electronic intelligence (ELINT) architecture remains indispensable for signal interception, providing vital situational awareness for ongoing military operations (Innoter, 2024; NASIC, 2018). Current trajectories in Russian R&D reflect an intensified focus on security-centric applications, emphasizing enhanced spatial accuracy and the integration of commercial data streams. The 2022 launch of Kosmos 2553, potentially the inaugural unit of the Neitron radar reconnaissance series, signals a shift in orbital strategy. Unusually, this platform operates at an altitude of approximately 2000 km, positioning it within Medium Earth Orbit (MEO) rather than the conventional LEO environment (Clark, 2022).

Initial cooperation was catalysed in 2015 when the China National Space Administration launched the BRICS Remote Sensing Satellite Constellation Cooperation Initiative. By August 2021, the space agencies of the five member states formalized this partnership through an agreement detailing the six satellites and five stations framework. This existing orbital infrastructure integrates diverse national assets, specifically the Chinese Gaofen-6 and Ziyuan III 02, the joint Sino-Brazilian CBERS-4, the Russian Kanopus-V, and the Indian RESOURCESAT-2 and 2A platforms. Development of this remote sensing architecture follows a bifurcated progression. The primary phase focuses on synthesizing these disparate Earth observation assets into a virtual constellation, while the subsequent stage envisions the deployment of a dedicated, unified constellation. By establishing this virtual network and its accompanying data-sharing protocols, the BRICS space agencies prioritize civil applications such as climate observation, disaster mitigation, and environmental surveillance (López, 2023).

Fig 12. Graphical Summary of the Relevant International Remote Sensing Capabilities



5. Case Studies

5.1. Protecting Critical Infrastructure

5.1.1. Classification of the Hybrid Threat

The 2022 sabotage of the Nord Stream pipelines serves as a primary case study for examining the role of Earth Observation (EO) data in identifying and monitoring hybrid threats. The incident began on September 26, 2022, when operators of the Nord Stream 2 link between Russia and Germany detected a precipitous drop in gas pressure, leading to the initial discovery of a leak Roke (n.d.). Shortly thereafter, a parallel pressure loss was recorded on Nord Stream 1, signifying a synchronized second strike. Confirmations followed within days as a total of four rupture sites were located near the island of Bornholm, identified through a combination of coast guard aerial patrols and both optical EO and Synthetic Aperture Radar (SAR) satellite imagery (Roke, n.d.). While the specific attribution of these acts remains contested, the event offers a quintessential illustration of a hybrid threat targeting European critical infrastructure.

Classification of the hybrid threat according to the “Landscape of Hybrid Threats” conceptual model developed by Giannopoulos et al. (2021).

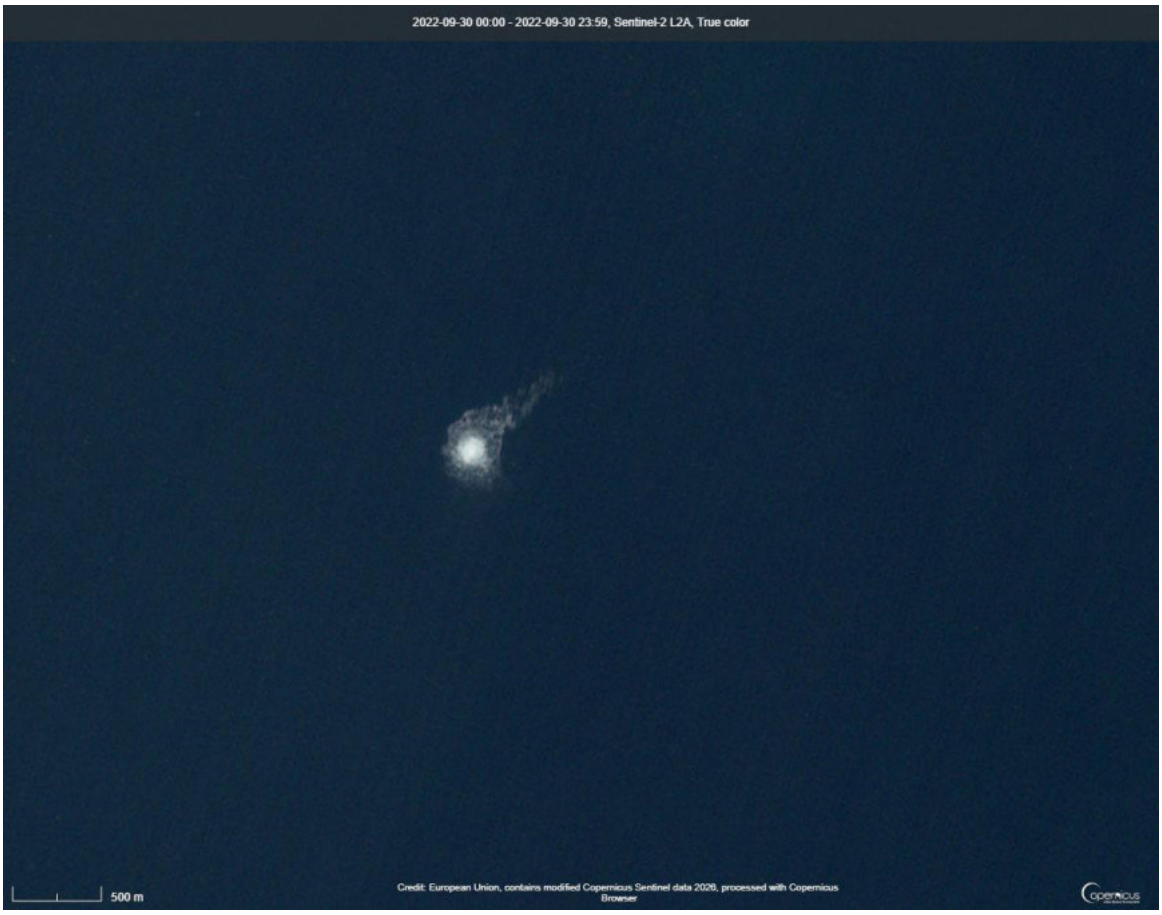
Dimension	Classification
Actor	Attribution remains unfruitful with conclusions that vary depending on the actors. - **Pro- Ukrainian Group**: Over a hypothesis including a Ukrainian citizen commanding the attack made from the yacht *Andromeda* seen hovering on top of the leak areas.(Hommerich et al., 2023) - **Russian Naval Presence:** Confirmed presence of the Russian salvage ship SS-750, equipped with a mini-submarine, near the site four days prior (The Guardian, 2023)
Tools	- **Physical operations to infrastructure**: Attack to a critical infrastructure with the use of high-yield explosives to damage the Nordstream 1 and 2 pipelines causing 4 leaks. Estimates vary from 100kg to 200kg of TNT equivalent (Lund et al., 2023) - **Creating or exploiting infrastructure dependency and economic dependency**: Nordstream was a critical supply of gas to Germany and Europe, representing two third of German importations in 2021.(Gross & Stelzenmüller, 2024) - **Territorial water violation**: The physical attacks on the pipelines happened within Danish Exclusive Economic

	Zone, resulting in a breach of sovereignty and a direct attack.(Braw, 2025)
Domains	- **Infrastructure**: Total destruction of three out of four strings of one of the most important Gaz pipelines in Europe, considered as a critical infrastructure by dependent countries. - **Economy**: Trigger a permanent separation of Europe from Russian gas, shifting towards other supply sources in the U.S., the Middle East and the Caucasus. Creating a deep energy crisis within Europe having important inflationary impacts. - **Political**: The motivation of the attack for both plausible actors was to create a Political reaction in Europe, that ultimately led towards a push for more important energy security.
Activity	This attack clearly sits in the **Coercion** phase at a level between **Operation** and **War/Warfare** as no clear attribution was made and the situation did not escalate strongly after this sabotage action.

5.1.2. Detection

Regarding detection capabilities, both radar and optical datasets were disseminated to security providers and subsequently the public to illustrate the consequences of this hybrid event. European assets remained prominent throughout this period, specifically through the Copernicus Sentinel constellation, which supplied medium-resolution imagery. This analysis highlights the discrepancies in spatial resolution when compared to commercial or non-European capabilities. The following figure, retrieved via the Copernicus EO Browser, a free, open-access portal for Sentinel data, demonstrates these technical parameters. Acquired on 30 September, the image captures a specific leak with sufficient clarity to determine its coordinates and magnitude. Such data serves as a critical mechanism for early detection and warning, facilitating the coordination of mitigation efforts by the Danish and Swedish coast guards.

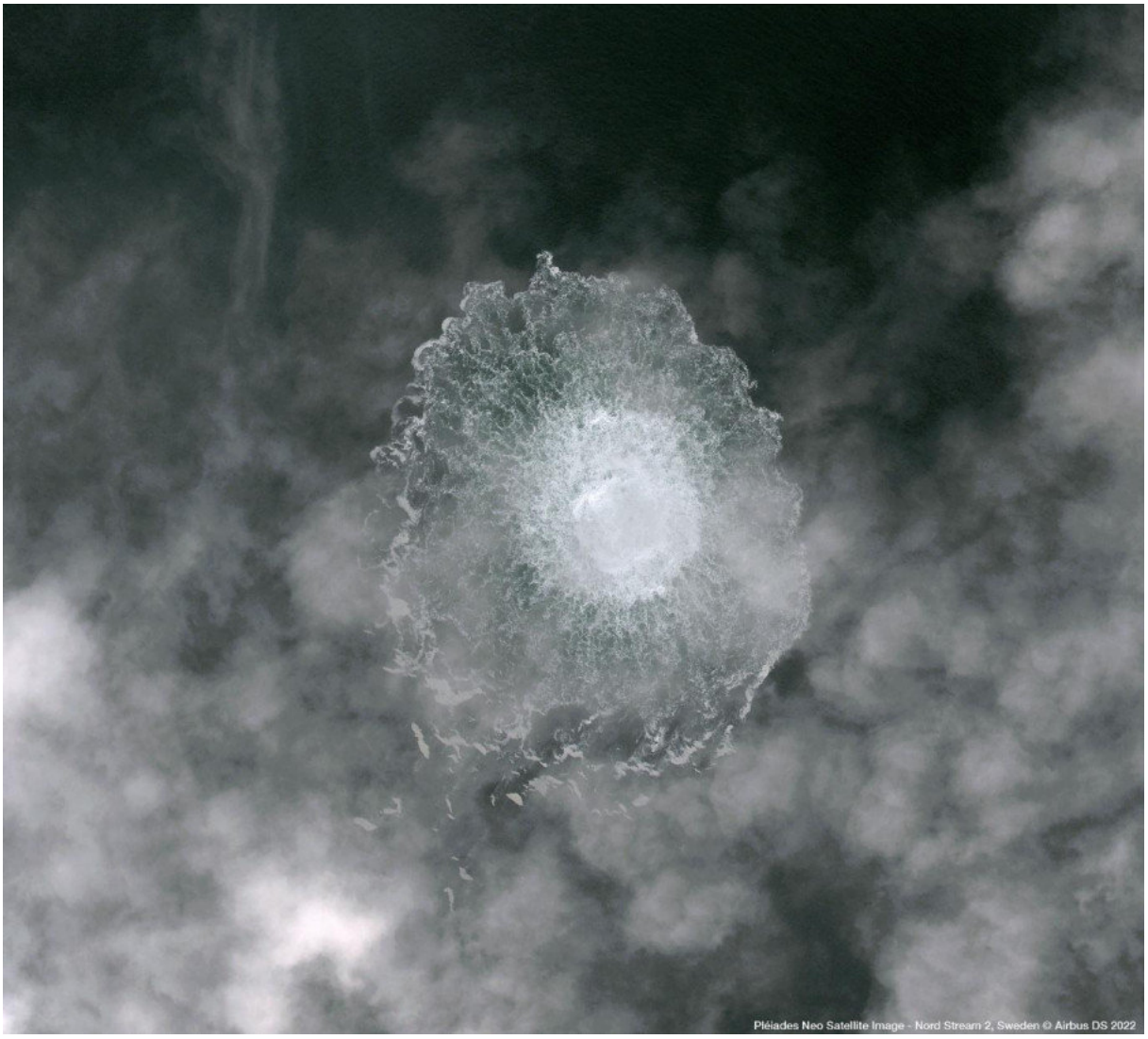
Image 1. Nordstream Leak in Mid Resolution Optical



Source: Copernicus Sentinel-2 data, Optical 10m, 30.09.2022, processed by Alexandre Touati, retrieved via Copernicus Browser

To illustrate the impact of varying resolutions, the following image provides a comparison using Very High Resolution (VHR) data captured by the French Pléiades Neo constellation on 29 September (Airbus Defence and Space, 2022). These high-precision assets demonstrate the extensive capabilities of modern Earth Observation satellites and the granular level of detail available to security providers engaged in maritime surveillance. While the Pléiades Neo imagery offers a significantly more detailed view of the surface disturbance, the specific nature of the leak, which spanned between 500m and 700m, suggests that extreme resolution was not strictly necessary for basic detection. Nevertheless, the 30cm precision remains vital for the identification of smaller tactical elements, such as nearby vessels or debris, which might otherwise remain obscured in coarser imagery.

Image 2. Nordstream Leak in Very High Resolution Optical

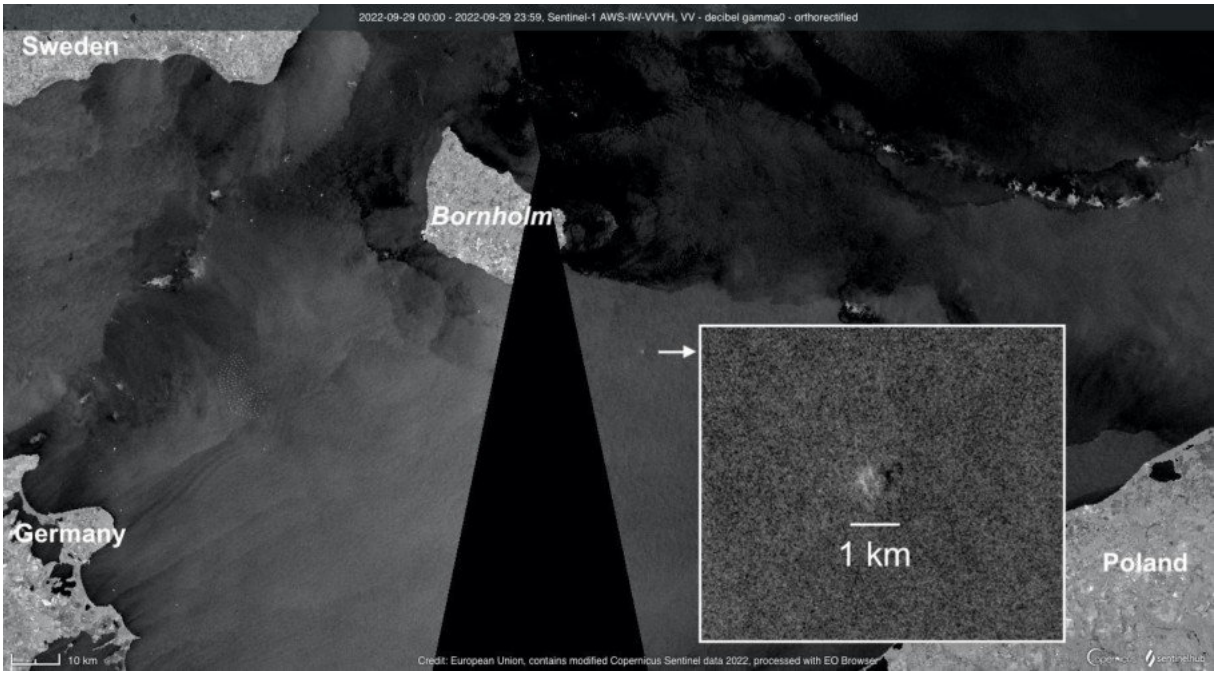


Source: Pléiades Neo data, Optical 30cm, 29.09.2022, processed by Airbus Defence and Space, retrieved via Airbus Defence and Space (2022).

Given the persistent cloud cover characteristic of the Baltic region, which often obscures traditional optical sensors, the integration of radar capabilities proved instrumental for effective monitoring (ESA, 2022b). Synthetic Aperture Radar (SAR) systems are uniquely suited for such environments, as their active sensors emit microwaves that are highly sensitive to variations in sea surface roughness. In the context of the Nord Stream incident, the turbulent bubbling caused by high-pressure gas escaping the pipelines created significant surface disturbances. These anomalies altered the radar backscatter, allowing for the precise detection of the leak sites regardless of atmospheric conditions. The following mid-resolution visualization

illustrates these specific SAR-detected signatures, mapping the various rupture points across the pipeline infrastructure.

Image 3. Nordstream Leak in Mid Resolution SAR



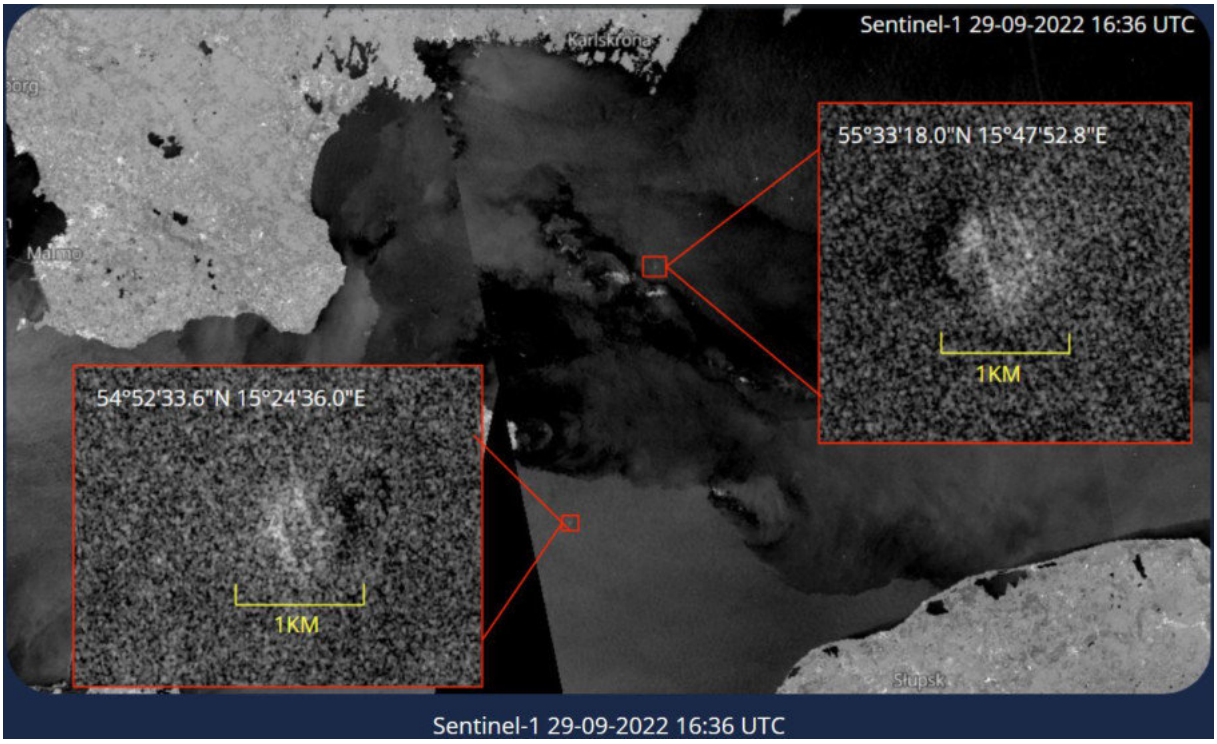
Source: Copernicus Sentinel-1 data, SAR 5m, 29.09.2022, processed by Hagolle (2022), retrieved via Copernicus Browser

Interpretations of the imagery necessitate a technical understanding of the dark cones, which represent the specific swath width captured by the Sentinel constellation. Data acquisition occurs through concrete bands following the orbital trajectory, a process that occasionally results in uncomplete information or the exclusion of specific geographic features as seen in this instance. Because these swaths might inadvertently obscure an object of interest, the necessity for high temporal resolution, specifically frequent revisit rates, becomes apparent, alongside the requirement for wide swath coverage and off-nadir pointing capabilities that allow sensors to tilt toward a prioritized target.

The second image, processed by Roke (n.d.), depicts two separate leaks within the Nord Stream pipeline infrastructure, though the raw spatial resolution poses significant challenges for manual human detection. To address these visual limitations, sophisticated algorithms and automated prompts are deployed to process vast

quantities of Synthetic Aperture Radar data, identifying minute anomalies that would otherwise remain invisible. These computational tools effectively flag areas of recent change, thereby streamlining the task for the human analyst who must interpret these complex radar returns.

Image 4. The Various Nordstream Leak in Mid Resolution SAR



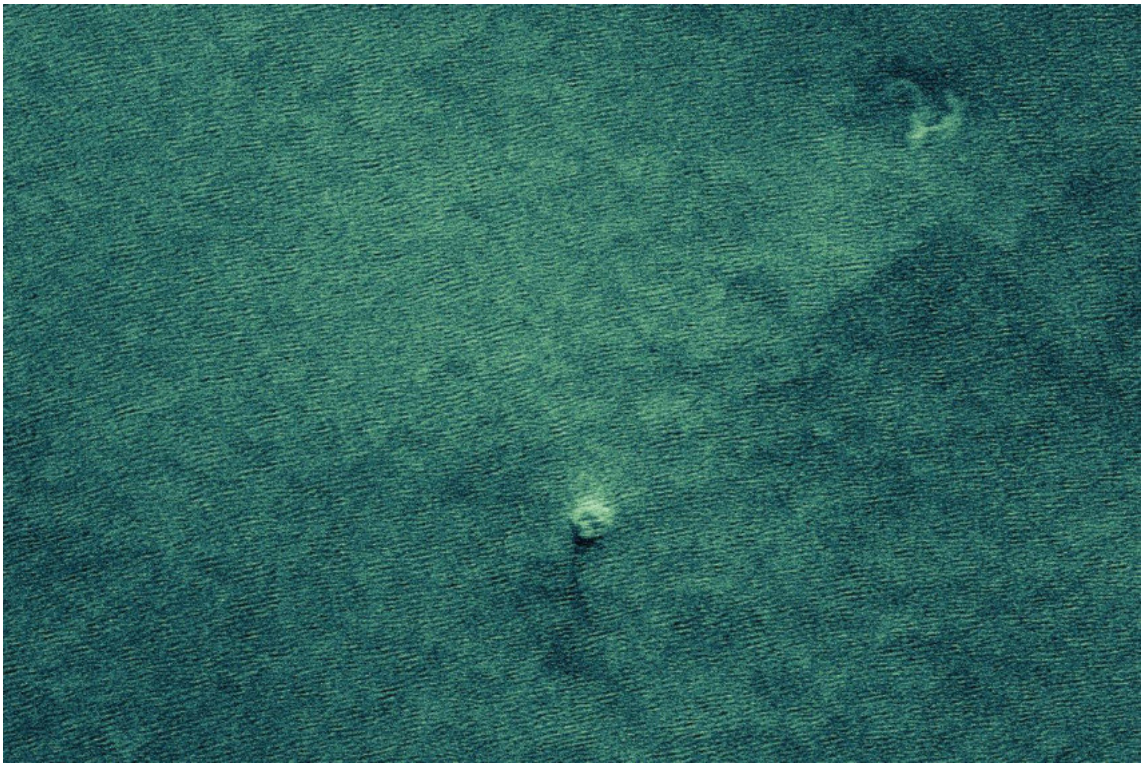
Source: Copernicus Sentinel-1 data, SAR 5m, 29.09.2022, processed by Roke, retrieved via Copernicus Browser

The final two images illustrate the same phenomenon as the previous data set, depicting the leaks on 29 September within a few hours of one another; this demonstrates how the Copernicus program, through its contributing missions, effectively achieves operational synergy. Such a federation of diverse data sources appears to mitigate gaps in temporal resolution, thereby facilitating more consistent imagery.

The subsequent open-source image with the highest available resolution originated from an ICEYE satellite passing over the region on the evening of 28 September, capturing the surface disturbance caused by the gas leaks. This specific imagery is of particular analytical interest due to a spatial resolution that permits the identification of

finer structural details. While Sentinel-1 resolution typically ranges between 1m and 10m, the ICEYE constellation offers VHR 30cm resolution, yet both systems successfully detected the leaks given that the disturbances spanned approximately 1km.

Image 5. Nordstream Leak in Very High Resolution SAR



Source: ICEYE data, SAR 1m, 28.09.2022, retrieved via ESA (2022b)

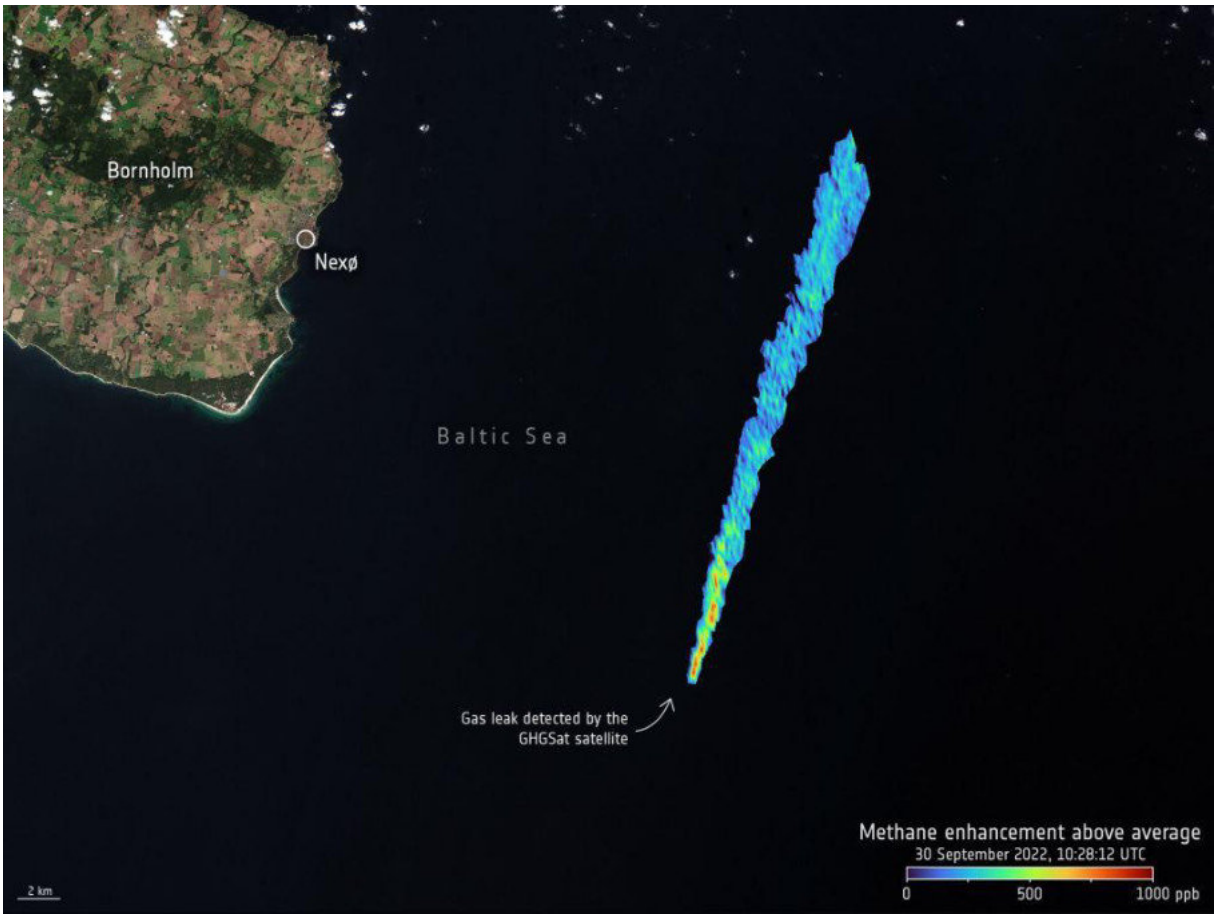
5.1.3. Attribution and Response

To identify the perpetrators behind this maritime sabotage, researchers at Roke synthesized AIS monitoring data with Radio Frequency signals to track vessels navigating in proximity to the leak coordinates. This methodology allowed for the subsequent monitoring of these ships during calls at Russian ports or the identification of direct links to Russian entities, highlighting anomalous manoeuvres and suspicious loitering patterns. Specifically, Roke (n.d.) identified a Greek cargo ship and three Polish yachts behaving erratically near the affected areas, which underscored the inherent risks of such illicit maritime activity. While this technical analysis did not yield an absolute attribution, it provides a vital evidentiary framework for identifying the attack's origin and represents a sophisticated intelligence source for monitoring high-risk

vessels (Roke, n.d.). Such data enables more effective subsequent investigations, allowing coast guards or deployed naval forces to engage vessels identified as components of the Russian shadow fleet within critical maritime zones.

Beyond the immediate repercussions of reputational damage, energy security vulnerabilities, and economic losses for Germany and the broader European Union, the most profound threat was environmental. Methane (CH4), among the most potent greenhouse gases, was discharged directly into the atmosphere. Because methane is partially absorbed by water, its detection remains technically arduous; nevertheless, an image released by ESA (2022b) utilizing data from the Canadian firm GHGSat succeeded in quantifying the leak. This satellite-derived intelligence was instrumental in determining the scale of the emission as well as the atmospheric trajectory of the methane trace.

Image 6. The Methane Emissions on the Nordstream Leaks



Source: GHGSat data, Multispectral 25m, 30.09.2022, retrieved via ESA (2022b)

Utilizing a satellite constellation with a spatial resolution of approximately 25m, investigators obtained precise measurements of the atmospheric discharge. These observations encompassed the entire duration of the gas leak; notably, data captured on 30 September indicated a methane release of roughly 79,000kg (ESA, 2022b) from a single site. This figure represents a significant environmental impact, particularly as the measurement occurred four days after the initial breach and accounted for only one of the four identified leak locations. Such satellite imagery provided European authorities with the necessary situational awareness to mandate the closure of relevant valves. Despite this tactical response, the subsequent release of high-resolution data appears to have prompted limited environmental risk mitigation efforts in the immediate aftermath.

5.1.4. Way forward

Strategic responses to these security challenges culminated in January 2025, when NATO and the European Union inaugurated the Baltic Sentry mission to bolster resilience against hybrid threats and safeguard critical infrastructure. This initiative operates in tandem with Task Force X Baltic in Germany, which serves as a coordination hub for force integration and the deployment of advanced technological sensors for threat detection. Analysis of this task force (NATO ACT, 2025) highlights the integration of Finnish ISR satellite capacity, suggesting that the ICEYE constellation is being leveraged for the persistent surveillance of suspicious maritime vessels and sensitive underwater assets.

Practical application of this enhanced maritime domain awareness is evident in recent investigations conducted by Unseenlabs using radiofrequency (RF) satellite clusters. By correlating AIS data transmitted from ship transponders and captured by terrestrial radars with RF signals intercepted by BRO satellites, analysts have successfully mapped the dark fleet operating within the Baltic Sea. These vessels frequently navigate with mandatory AIS systems deactivated, yet their electronic signatures remain detectable. Such persistent monitoring reveals a significant concentration of shadow ships near St. Petersburg, which likely facilitate activities ranging from sanctions evasion to potential kinetic sabotage of subsea cables. This hybrid tactical approach appears not to be exclusive to Russian operations, as Chinese actors

similarly employ these maritime assets in broader Gray-zone campaigns against European interests.

Image 7. Traffic in the Baltic Sea, RF vs AIS

Source: BRO data, RF, August 2024, retrieved via Unseenlabs (2024)

This clear visualization coupled via sub daily revisit times, allow for the European Unseenlabs to guarantee persistent security and transmission to European security providers. To have a constant and clear vision of the threats they are facing to augment European general resilience against hybrid threats.

5.2. Weaponised Migration

5.2.1. Classification of the Hybrid Threat

In examining additional dimensions of hybrid threats, this case study analyses the instrumentalization of migration as a coercive tool within Russian and Belarusian strategic frameworks aimed at destabilizing Europe and fostering systemic uncertainty.

The 2021 crisis at the Polish border serves as a primary example, where approximately 30,000 individuals attempted irregular crossings over the course of the year, an influx that arguably heightened localized tensions and catalysed domestic volatility within Polish society (Boyse, 2026). Similar patterns emerged in Lithuania and Latvia, both of which experienced a rapid surge in arrivals that peaked at roughly 4,500 border crossings during the same period (Boyse, 2026). These instances are particularly salient because, while the geographical origin of the migrant flows from Belarus makes the technical attribution process relatively transparent, the legal and political categorization of these events as a deliberate weaponization of human mobility remains a complex challenge for international observers.

Classification of the hybrid threat according to the "Landscape of Hybrid Threats" conceptual model developed by Giannopoulos et al. (2021).

Dimension	Classification
Actor	The actor is clearly identified as a state actor: - **Belarussian State**: Investigations point to high-level coordination with Russian logistics and support, even if the territory used for these operations, is Belarus. (RÁCZ, 2022)
Tools	- **Migration as a bargaining chip in international relation**: Creating extreme pressure on European borders by artificially creating waves of migration forcing a reaction by the affected states. (DG Migration and Home Affairs, 2024) - **Exploiting immigration for political influencing**: Further objective of using the migrants as a political force within the countries of arrival to create destabilisation. - **Manipulating discourses on migration**: Creating negative narratives to discredit European answer to the weaponised migration attacks to influence negatively the public opinion.
Domains	- **Social/Societal**: Exploiting internal European polarization over refugee quotas to create stress on European cohesion. - **Political**: Testing the trust of the polish and Baltic population towards their government in handling this crisis. - **Legal**: Exploiting the commitment to Human Rights by European democracies, in particular the non-refoulement principle to create a dilemma between legal obligations and national security. - **Information**: Using pro-Russian media platforms and social media to spread disinformation to shift the blame on the defender countries.

Activity	This attack sits in the **Destabilisation** phase at the **Operation** level. However, the death of a polish border guard and the supply of non-lethal weapons such a as laser to the migrants by Belarus brings it close to the threshold.

5.2.2. Detection

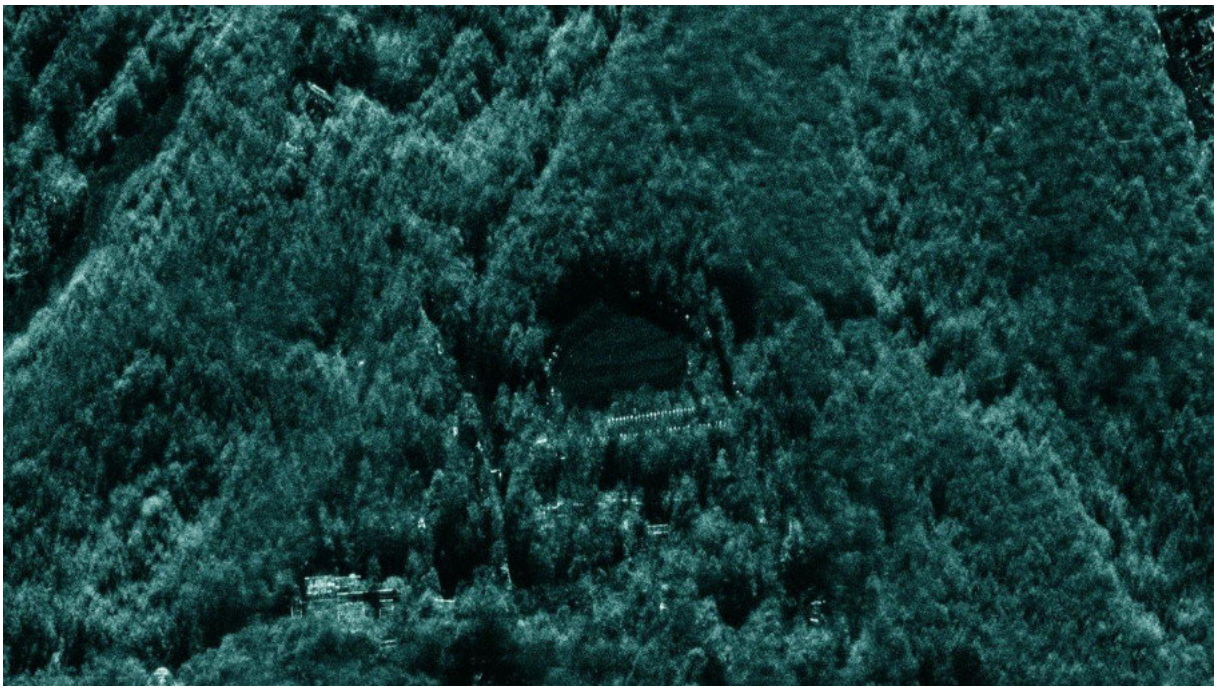
European security providers, most notably Frontex, have increasingly integrated satellite imagery to transform the execution of land border management. These orbital assets provide a persistent, wide-angle sensing capability that surpasses the reach of traditional ground patrols; by enabling remote observation, they reduce the necessity for direct resource engagement and mitigate operational risks. Through the simultaneous scanning of hundreds of kilometres along European frontiers, data processed via SatCen allows national agencies and Frontex to transition from reactive patrolling, which necessitates an immediate response to disruptive events, toward a strategic, data-driven model of anticipatory surveillance. Monitoring these borders remains an arduous task, as they frequently traverse isolated regions characterized by dense forests, rugged terrain, or other natural obstructions. The high-level visibility inherent to remote sensing proves essential for identifying human activity hotspots, including encampments, vehicle movements, and emerging transit paths in remote sectors (Frontex, 2025). Consequently, these tools assist authorities in optimizing physical interventions by directing resources to precise locations where unauthorized activities, such as subterranean tunnels along the Belarusian Polish border or the formation of large groups, are detected.

Border surveillance via Earth Observation (EO) satellites presents significant operational challenges, necessitating persistent monitoring through nocturnal cycles and adverse meteorological conditions. The interplay between spatial, temporal, and spectral resolutions remains fundamental to ensuring high-fidelity change detection, often achieved through the synthesis of orbital data with terrestrial or aerial sensors like unmanned aerial vehicles and ground-based cameras (Frontex, 2025). To achieve this continuous coverage, Synthetic Aperture Radar (SAR) platforms emerge as a critical solution due to their capacity to penetrate cloud cover and operate without solar illumination. Within the European EO architecture, these assets provide high revisit frequencies and fine resolutions, enabling the identification of subtle physical

signatures such as nascent footpaths or soil compaction indicative of human movement or vehicular tracks on soft terrain.

The imagery provided by ICEYE (n.d.) demonstrates this capability by clearly identifying vehicles and infrastructure within dense forest canopies, marked by high-backscatter points that remain invisible to conventional optical sensors.

Image 8. ICEYE Detection Capacities in a Dense Forest

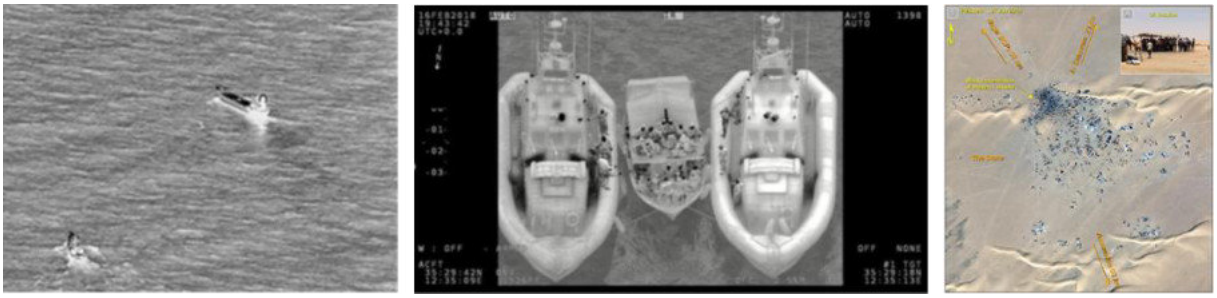


Source: ICEYE data, SAR 1m, retrieved via ICEYE (n.d.)

Synthetic Aperture Radar (SAR) data proves instrumental for change detection, yet its true utility emerges when integrated with high-resolution optical imagery or ground-based sensors to facilitate the identification and quantification of human gatherings at border crossings. This multi-sensor approach allows analysts to identify vulnerabilities in security infrastructure, such as fence breaches, in a resource-effective manner that mitigates the risk of undetected movement. Such data also serves to validate ground-based motion detectors, ensuring that alerts are not triggered by false positives like local wildlife (Frontex, 2025).

Regarding the monitoring of irregular migration, particularly across Mediterranean routes, satellites offer critical forward intelligence that supports more proactive humanitarian and security interventions. European Earth Observation (EO) services extend their reach beyond continental limits to monitor departure points in North Africa, such as Libya, which frequently serve as the primary staging grounds for maritime crossings (Copernicus, 2019). The sophistication of these orbital assets now permits the tracking of small vessels constructed from materials that often evade traditional maritime radar systems. Frontex employs a search and task methodology (Frontex, 2025) by initially utilizing wide-area SAR imagery to flag anomalies before refined VHR optical satellites zoom in to provide granular detail. This process of sensor fusion, often enhanced by automated data processing, enables authorities to map movement patterns across the Mediterranean and concentrate assets on established transit corridors. These space-based layers are ultimately complemented by aerial surveillance from manned aircraft and remotely piloted systems to maintain oversight before migration flows reach formal borders.

Fig. 13 Copernicus Border Surveillance Service (illustration)

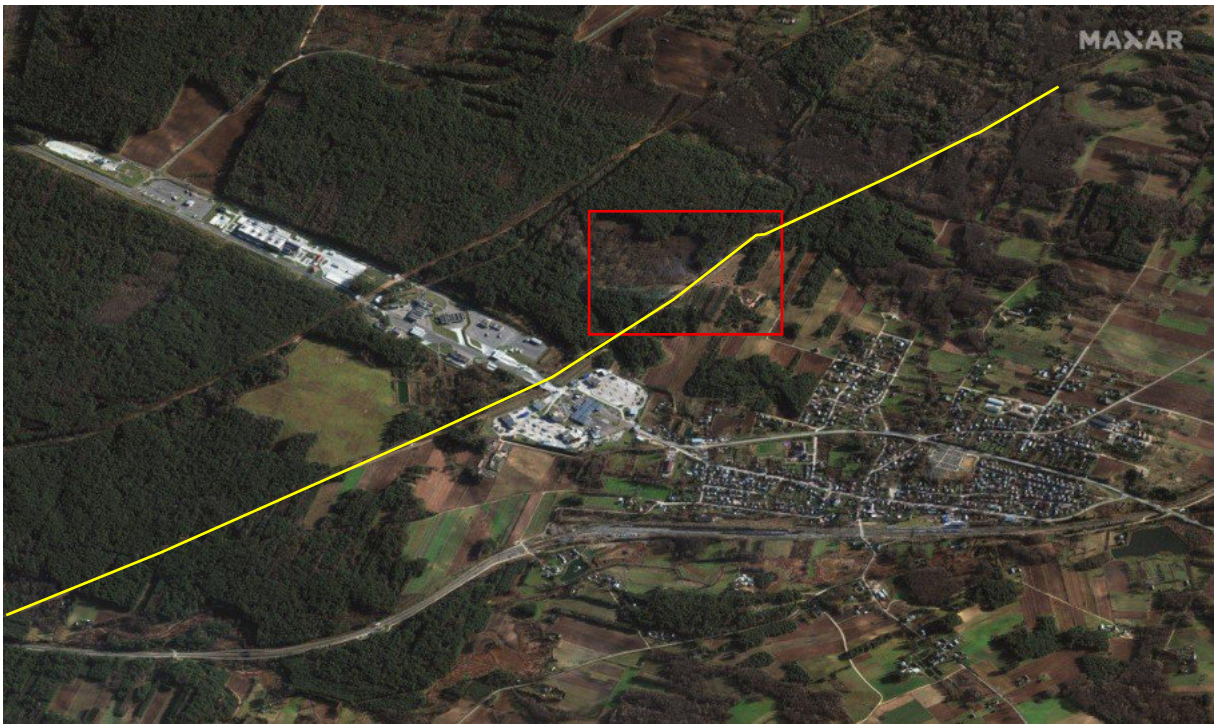


Source: (Copernicus, 2019)

Regarding the November 2021 incident, which saw approximately 4,000 Iraqi refugees directed toward Poland from the Belarusian Bruzgi-Kuznica border crossing, VHR imagery proved remarkably abundant. Under optimal meteorological conditions and during daylight hours, standard optical imagery, such as the data acquired by Rushton (2021) from Maxar, an American commercial provider subsequently acquired by Microsoft, effectively illustrates the intelligence tools potentially available to the Polish Border Guard and Frontex. This imagery assists in analysing the response to a hybrid threat reportedly orchestrated by the Russian and Belarusian administrations. In the

initial VHR optical samples distributed to various news outlets to document the border crisis, the spatial arrangement of the transit point is clearly discernible. The physical fencing, visible within the designated red sector on the map, highlights the infrastructure intended to deter irregular migration through the surrounding forested terrain. Such high-resolution data underscores both the geographical scale of the nearby village and the strategic isolation of the border post, factors that appear to exacerbate its inherent security vulnerabilities.

Image 9. Bruzgi-Kuznica Border Crossing



Source: Maxar data, Optical 30cm, 2021, retrieved via Rushton (2021)

Examination of the second image, specifically the magnified red square, reveals a distinct gathering of individuals situated along a roadway adjacent to the border post. Such aerial perspectives enable an assessment of migrant density and their primary direction of movement. The presence of smoke plumes suggests the establishment of semi-permanent encampments, potentially indicating an intent to remain for a prolonged duration to exert sustained pressure on the Polish frontier. This level of granular intelligence serves as a critical tool in countering hybrid threats, particularly disinformation, by providing the general public with empirical evidence regarding the

reality of the situation and the nature of the institutional response. Without such verification, these humanitarian vulnerabilities remain susceptible to instrumentalization by Russian state media entities like TASS. Such outlets frequently manipulate border dynamics to critique European migration management while obscuring the strategic intent behind the orchestration of migrant surges designed to generate external political pressure.

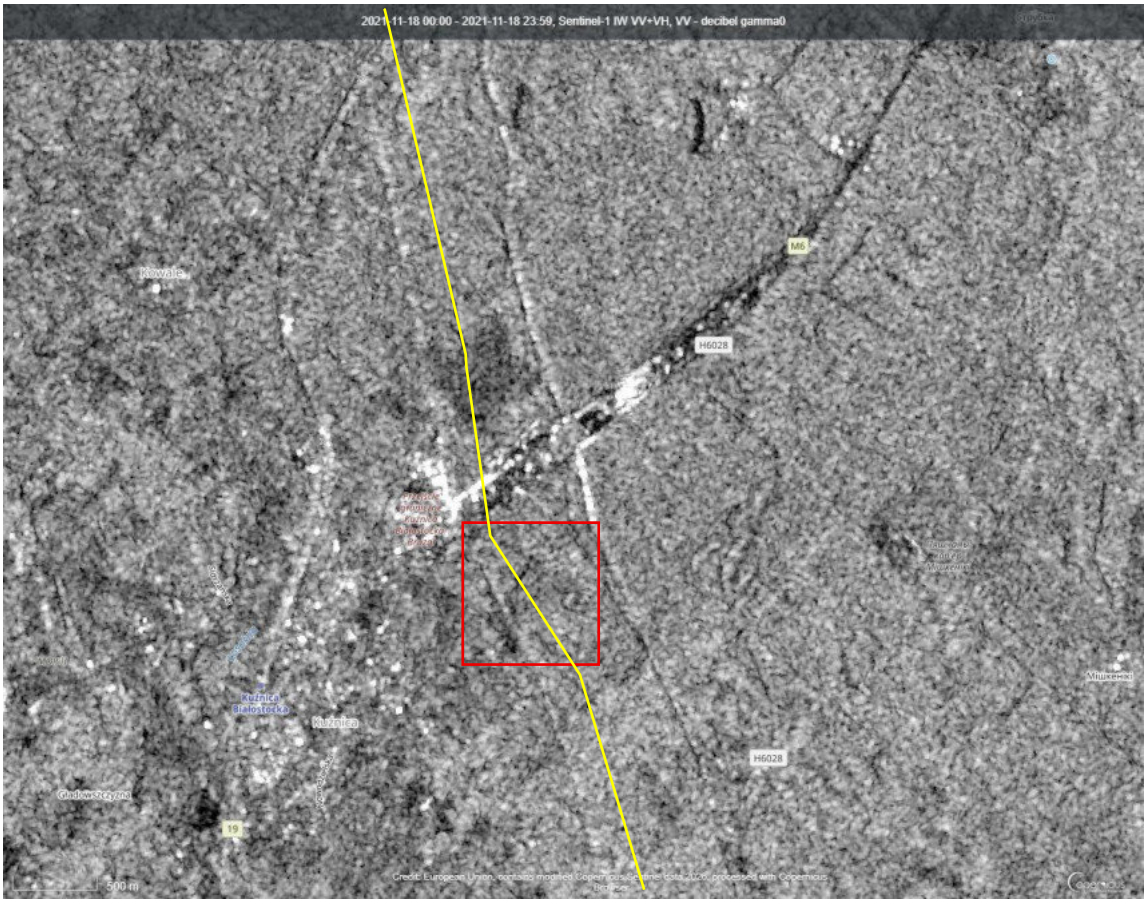
Image 10. Bruzgi-Kuznica Border Crossing (Zoomed on Migrants Positions)

Source: Maxar data, Optical 30cm, 2021, retrieved via Rushton (2021)

The integration of heterogeneous sensor suites within Frontex methodologies, specifically the reliance on Synthetic Aperture Radar (SAR), indicates a potential for European Earth Observation (EO) solutions to detect large-scale human movements and reconstruct the historical presence of migrant groups. Within such operational contexts, Very High Resolution (VHR) data appears essential to distinguish authentic terrestrial movements from environmental noise, yet the inherent political and humanitarian sensitivity of these scenarios often restricts imagery dissemination. To provide a comparative baseline, an open-source SAR acquisition from the Sentinel-1 mission was extracted via the Copernicus EO Browser to simulate the limitations of mid-resolution data in this specific geographical theatre. By transposing the identical

red square and yellow delineations onto this SAR dataset, the visual output demonstrates the specific observational capabilities and constraints inherent to LEO-based radar sensing at this scale.

Image 11. Bruzgi-Kuznica Border Crossing SAR Imagery



Source: Copernicus Sentinel-1 data, SAR 5m, 18.11.2021, processed by Alexandre Touati, retrieved via Copernicus Browser

Given the lack of publicly available satellite imagery regarding this specific instance of weaponized migration, the utility of border monitoring via Earth Observation is better illustrated by the 2020 Turkey-Greece border crisis. High-resolution imagery from Maxar at the Pazarkule crossing clearly identifies vehicular patterns and personnel movements, providing a granular view of the situation. Such Very High-Resolution data enables an assessment of the logistical capacity of the migrant groups, including their equipment and duration of stay, which in turn allows security forces to calibrate the resources required for border control and develop long-term mitigation strategies for

similar asymmetric threats. If temporal resolution is sufficient, European security providers can achieve the situational awareness necessary for early detection of events that carry significant regional security implications. Conversely, Frontex has faced rigorous scrutiny regarding its management of migrant flows, particularly concerning alleged human rights violations. In these contexts, remote sensing data provides a critical evidentiary basis for civil society organizations to conduct independent investigations into state and institutional conduct (Human Rights Watch, 2022).

Image 12. Pazarkule crossing (Greece -Türkyie)

Source: Maxar data, Optical 30cm, 2020, retrieved via Getty Images (2020)

5.2.3. Attribution and Response

The crisis documented along the Polish Belarusian frontier serves as a primary example of state-sponsored weaponized migration. Evidence indicates that the Belarusian administration orchestrated this influx to destabilize neighbouring states, specifically Poland and the Baltic nations, thereby presenting a multifaceted security threat to the European Union (European Commission, 2025). Investigations suggest that starting in June 2021, Minsk systematically doubled air traffic from the Middle East, utilizing state-run travel agencies in Iraq and Syria to market package deals that bundled visas with transit to the European border (Boyse, 2026). Rather than a

spontaneous humanitarian movement, this appeared to be a calibrated operation involving the recruitment of individuals from countries such as Libya, Turkey, and Iran. On the ground, the presence of personnel in unmarked uniforms, a tactic frequently associated with Russian "Gray zone" operations to obscure attribution, facilitated these crossings. To maximize the tactical nuisance, migrants were reportedly equipped with lasers to disorient Polish border guards through non-kinetic means (Boyse, 2026). Such coordination likely aligned with Russian strategic interests, coinciding with the Zapad 2021 military exercises (Boyse, 2026). This timing forced European security providers to focus on the migration emergency while Moscow executed a significant show of conventional force.

Responding to this hybrid offensive necessitated a significant reallocation of national security assets by Poland, Lithuania, and Latvia. By November 2021, Warsaw had deployed 15,000 troops to the border, a manoeuvre that diverted personnel from standard defence missions (Montgomery, 2026). In an effort to deter future provocations, Poland invested roughly €350 million into the construction of a 400-kilometer border wall and an adjacent buffer zone (European Commission, 2025). These defensive infrastructure projects were mirrored by parallel fortification efforts in Lithuania and Latvia (Montgomery, 2026). At the height of the crisis, approximately 30,000 illegal crossing attempts were recorded annually (Boyse, 2026). This sustained pressure led to volatile escalations on the ground, ultimately resulting in the death of a Polish border guard.

5.2.4. Way forward

The Frontex (2025) report on Earth Observation for Border Management introduces several critical pathways for the evolution of EO applications in this sector. Given that Frontex already relies heavily on the Copernicus Border Surveillance Service (CBSS), these innovations will likely be integrated under European frameworks to bolster capabilities and solidify the continent’s strategic autonomy in the space domain. Practical implementation focuses on adopting satellites with enhanced spatial, temporal, and spectral resolutions alongside the fusion of satellite data with aerial and ground-based sensor networks. On the analytical side, progress mirrors broader digital economic trends, specifically the development of sophisticated AI models and algorithms designed to accelerate and refine data processing.

The paradigm of border security is increasingly shifting toward more intimate and persistent orbital configurations, characterized by the emergence of Very Low Earth Orbit (VLEO) constellations. By operating at altitudes significantly lower than traditional LEO satellites, these platforms markedly enhance spatial resolution and minimize signal latency for rapid data delivery. This proximity not only improves image clarity but also mitigates LEO congestion and reduces launch costs, as delivery vehicles are not required to reach higher orbital planes (EDA, 2024b). Beyond orbital shifts, the sector anticipates a transition toward Ultra-High Resolution (UHR) imagery, where commercial standards are expected to migrate from the 1m–30cm range to a 10cm benchmark. While this may reduce the total area covered per pass, the resulting precision allows analysts to identify specific vehicle types, detect minute breaches in border fencing, and provide high-confidence forensic evidence for criminal proceedings. Though UHR remains a nascent commercial offering, its adoption is already a priority for military institutions, particularly in China and the United States. To counter the limitations of surveillance in regions with dense vegetation, Foliage-Penetration (FOPEN) technology is proving transformative (Frontex, 2025). By utilizing P-band SAR and hyperspectral sensors, these systems can penetrate thick canopies to detect human activity on the forest floor that remains invisible to standard optical cameras (Frontex, 2025).

Complementing these low-orbit assets are High Altitude Platform Systems (HAPS), which function as pseudo-satellites stationed in the stratosphere at approximately 18km (Frontex, 2025). Unlike traditional satellites constrained by orbital mechanics, which prevents geostationary positioning at lower altitudes and creates gaps in revisit times, these solar-powered HAPS and fixed-wing aircraft can hover over specific border hotspots for weeks (Frontex, 2025). This persistent, stationary surveillance effectively bridges the capability gap between the broad coverage of EO satellites and the localized, short-term deployment of drone technology.

5.3. Jamming and Spoofing (EW)

5.3.1. Classification of the Hybrid Threat

Following the outbreak of hostilities in Ukraine, numerous maritime and aerial assets have encountered significant disruption of GNSS signals, specifically involving the jamming or spoofing of GPS and Galileo constellations. These electronic interference activities, concentrated primarily along Europe's eastern frontier and the Kaliningrad exclave, have severely impacted Baltic shipping lanes and Polish aviation hubs. Several ITU member states and Russia have formally denounced these manoeuvres, which many observers now categorize as malicious hybrid attacks against European infrastructure (Höller, 2025). Technically, the execution of GNSS jamming is not resource-intensive; because these satellites operate in high orbits, they transmit relatively weak signals that terrestrial emitters can easily overpower (Höller, 2025). While the strategic intent behind such interference remains opaque, the operational consequences for neighbouring states are tangible, effectively compromising routine civilian activities and regional safety protocols.

Classification of the hybrid threat according to the "Landscape of Hybrid Threats" conceptual model developed by Giannopoulos et al. (2021).

Dimension	Classification
Actor	The actor is clearly attributed to a state actor: - **Russia**: specifically originating from the Kaliningrad exclave and the St. Petersburg/Leningrad region (Höller, 2025)
Tools	- **Electronic operations (GNSS jamming and spoofing)**: Jamming and spoofing of navigation system provided via satellite by using sophisticated jammers. - **Clandestine Operations**: Denial of GNSS data to European states to create confusion and deny situational awareness for these states potentially leading to escalation.
Domains	- **Space:** Disrupting the delivery of PNT data from satellite constellations such as Galileo and GPS to ground/air receivers, however without conducting a direct attack on space infrastructure. - **Cyber**: Attack on the Electromagnetic domain, exploiting the inherent vulnerability of unencrypted civilian GNSS signals to flood or hijack the signal. - **Infrastructure:** Compromising the central importance of PNT data on supporting transportation, telecommunications, timing, power grids, and bank transactions.

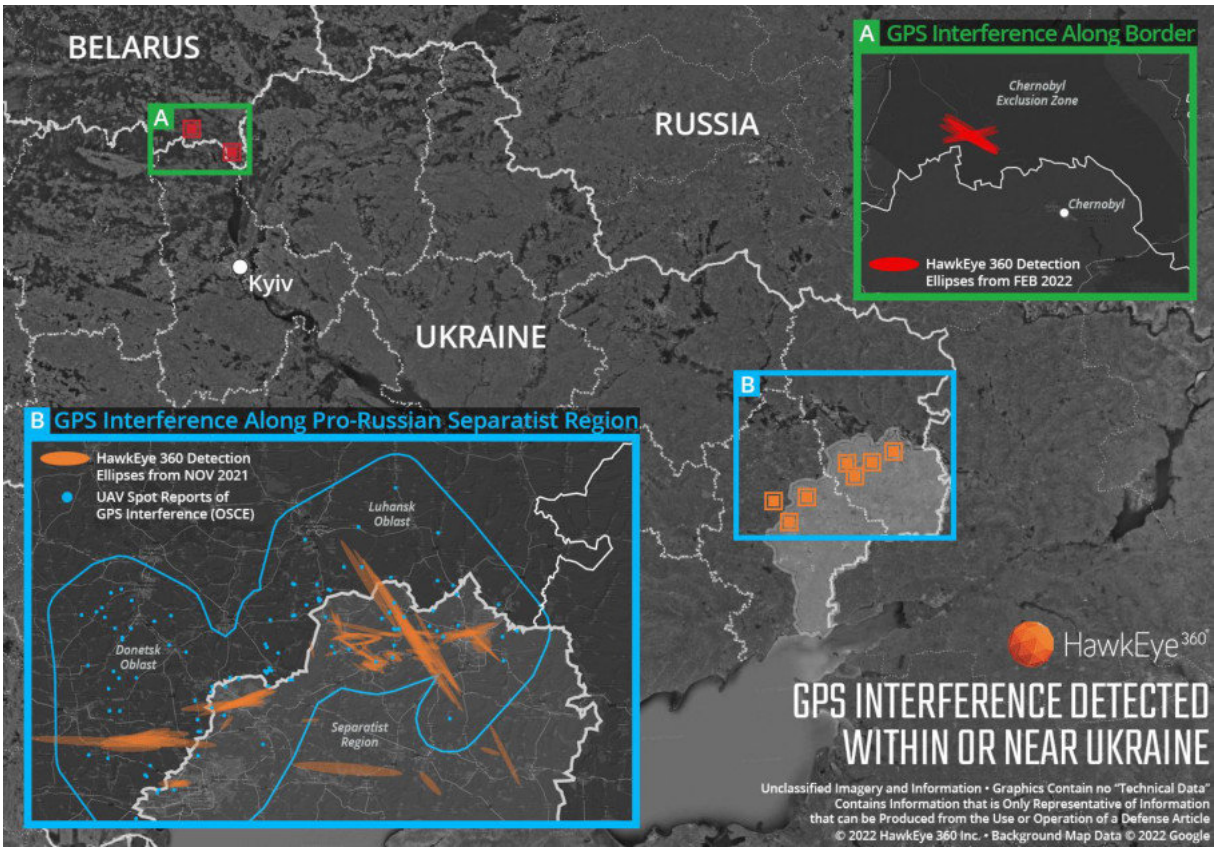
Activity	These actions are situated in the **Destabilisation** phase situated at the **Operation** level as these acts have real physical consequences and a potential for disruptions that is non negligible.

5.3.2. Detection

Detecting electronic warfare incidents involves a range of terrestrial sensors, including radars, Automatic Identification System (AIS) platforms, and various GNSS software suites. To map the source and intensity of jamming and spoofing, private actors such as Flightradar24 (n.d.) provide resources like the GPS jamming and interference map, which aids in pinpointing approximate locations where these disruptions impact civilian infrastructure, particularly maritime traffic and civil aviation. Space-based remote sensing offers a sophisticated alternative through two distinct technologies: Radio Frequency (RF) monitoring and Synthetic Aperture Radar (SAR) imagery. When these detections are correlated with optical imagery, analysts can potentially identify the specific hardware or installations causing the interference.

The significance of this capability was highlighted by numerous news outlets in 2022, demonstrating how the American firm HawkEye 360 utilized its RF satellite constellation to detect ellipses of GNSS interference along the Russian-Ukrainian border during the initial phases of the invasion (Goward, 2022). These measured interferences in Russian-occupied regions prior to the full-scale assault suggest a deliberate effort to mask troop movements and disrupt civilian transportation networks, thereby destabilizing the social sphere in preparation for kinetic action. Because these jamming activities served as direct precursors to conventional warfare, they may transcend the definition of a hybrid threat, instead illustrating the tactical maturation of electronic signal denial. While HawkEye 360 remains the leader in this field, the European counterpart Unseenlabs does not publicly showcase equivalent operational outputs. This discrepancy suggests a potential capability gap that could impact European strategic autonomy in the space domain.

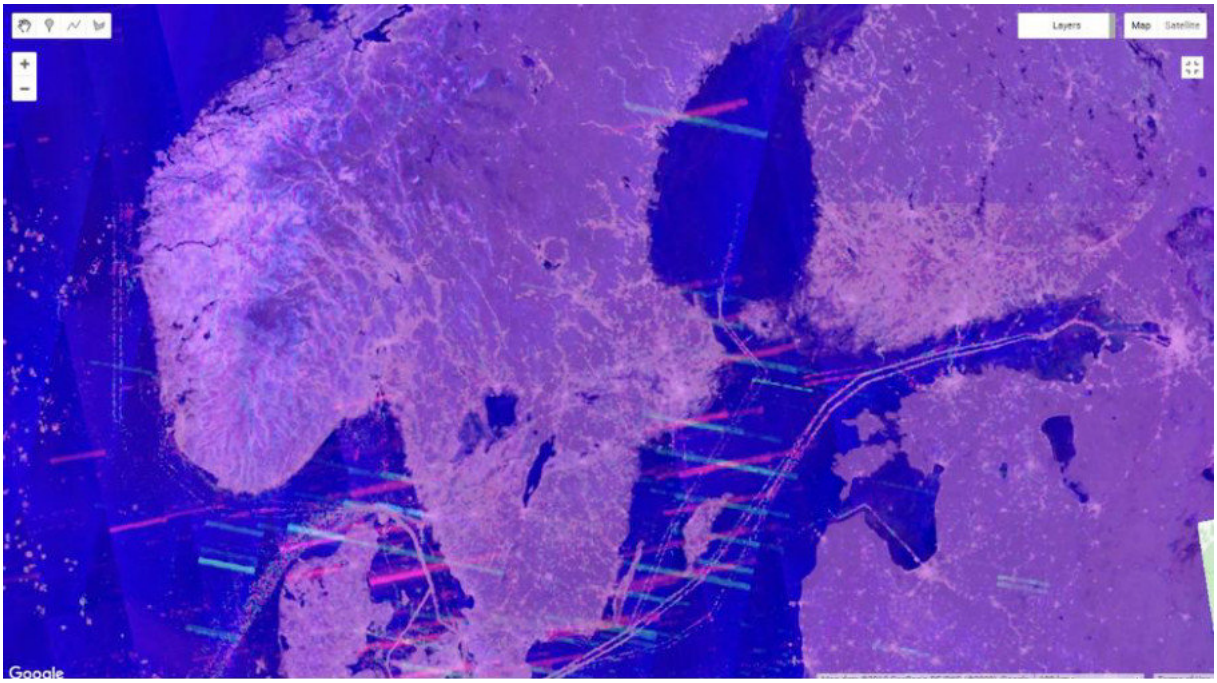
Image 13. GPS Interference Near Ukraine



Source: HawkEye 360 data, RF, November 2021, processed by Goward (2022).

To address existing gaps in dedicated Radio Frequency (RF) capabilities, research conducted by Ballinger (2022) demonstrates how radio frequency interference (RFI) can be identified using standard Synthetic Aperture Radar (SAR) imagery from Sentinel-1, the flagship radar satellite of the Copernicus programme. Leveraging this open-access data allowed for the detection of RFI across various European conflict zones and strategic sectors populated by high-power transmitters. A notable instance involves a distinct X-shaped interference pattern appearing on SAR imagery along the Baltic littoral, which Ballinger (2022) attributed to powerful radio emissions from the Swedish STRIL ballistic missile defence system, an early-warning installation monitoring potential Russian missile launches. By synthesizing SAR imagery with Very High-Resolution optical data and open-source intelligence, the researcher successfully identified specific emitters in these contexts. This methodology was subsequently extended to the Black Sea and the Middle East, illustrating the capacity for SAR technology to supplement limited RF assets in the precise detection of GNSS jammers.

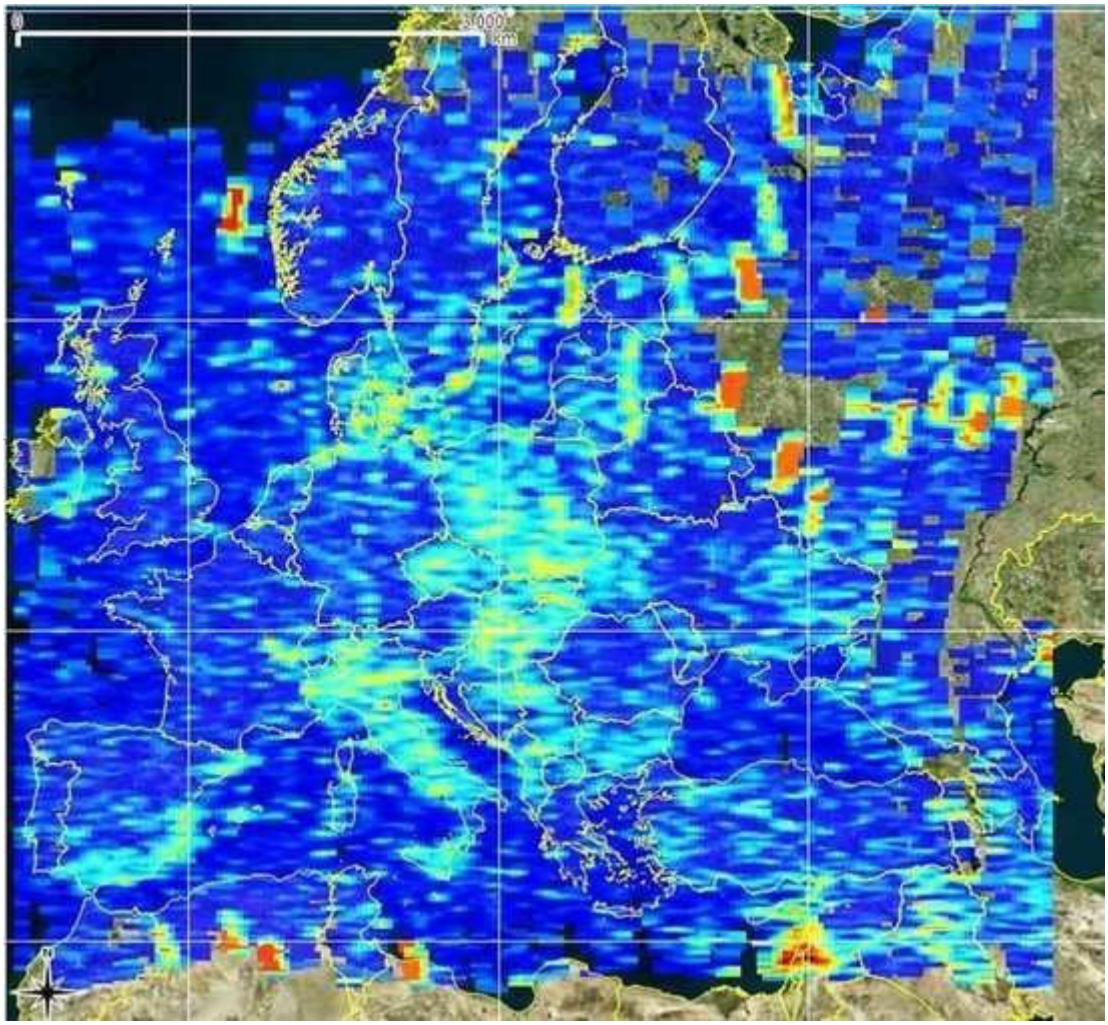
Image 14. Interference on Sentinel 1 in the Baltic Sea



Source: Copernicus Sentinel-1 data, SAR 5m, processed by Ballinger (2022)

Complementary research conducted by Monti-Guarnieri et al. (2017) presents an alternative methodology for identifying Radio Frequency Interference (RFI) within the C-band, which remains the primary frequency for Synthetic Aperture Radar (SAR) technology. By utilizing Sentinel-1 data, the authors employ computational techniques to isolate geographic clusters characterized by high interference levels. While the original study does not explicitly address defence or security applications, it highlights the utility of such mapping for policymakers seeking to comprehend the European electromagnetic landscape. This spatial identification of RFI suggests a foundational step for broader regulatory oversight and frequency management across the continent.

Image 15. Interference on Sentinel 1 in Europe

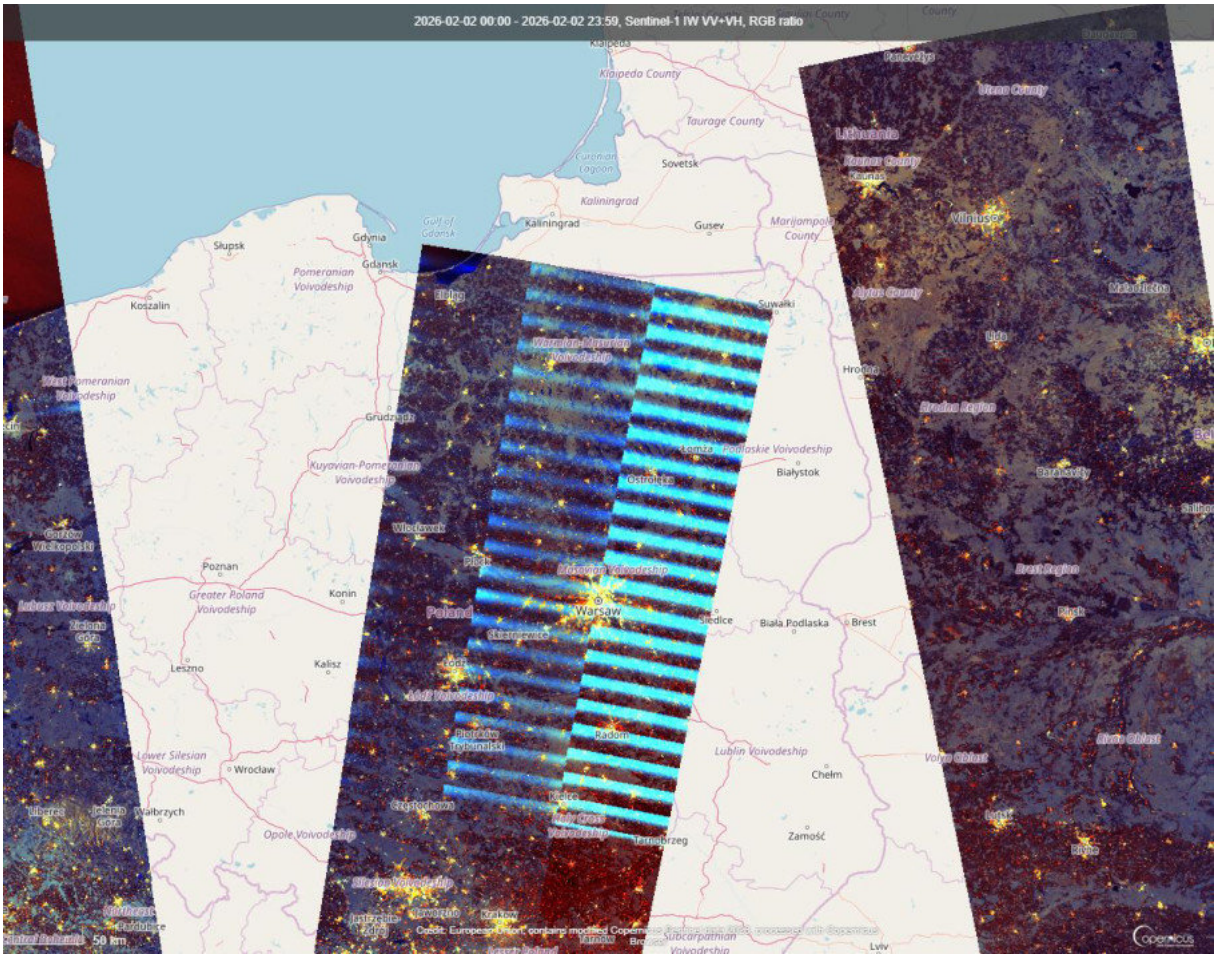


Source: Copernicus Sentinel-1 data, SAR 5m, processed by Monti-Guarnieri et al. (2017)

By applying both theoretical frameworks, this case analysis replicates the methodology for identifying Radio Frequency Interference (RFI) linked to suspected jamming and spoofing activities across Europe. Such occurrences are increasingly categorized as hybrid threats orchestrated by adversaries to compromise critical infrastructure and transportation networks. Sentinel-1 imagery retrieved via the Copernicus EO browser on 2 February, focusing on the European eastern flank, demonstrates the feasibility of RFI detection through civilian assets. The prominent blue artifacts cantered over Warsaw illustrate how these tools facilitate the detection and subsequent attribution of electronic interference. Given that the satellite swath was positioned to capture imagery of the Russian exclave of Kaliningrad, a preliminary hypothesis regarding the origin of these disruptions appears plausible.

Regarding technical capacity, while dedicated RF detection via satellite remains in a developmental phase within the European civilian sector, sensor fusion potentially addresses existing capability gaps. It remains probable that such sophisticated detection is already integrated into European sovereign systems managed by military operators or accessible through Copernicus contributing missions. This intelligence is increasingly available to civilian stakeholders and European authorities through integrated EO technology databases (Space Daily, 2023).

Image 16. Interference on Sentinel 1 on the Eastern Border



Source: Copernicus Sentinel-1 data, SAR 5m, 02.02.2026, processed by Alexandre Touati, retrieved via Copernicus Browser

5.3.3. Attribution and Response

Electronic interference, specifically jamming and spoofing, has transitioned from sporadic occurrences to a daily reality, particularly following the escalation of the conflict in Ukraine. Attribution of such hybrid threats often relies on sensor fusion, an analytical process that integrates radar and optical imagery with diverse intelligence streams to pinpoint the origins of an attack. This methodological approach allowed Polish researchers to identify a radar installation in Kaliningrad as the primary source of GNSS jamming across the Baltic region, utilizing Sentinel-1 radar data to detect the interference patterns (Höller, 2025). By corroborating these findings with optical imagery from Planet Labs, investigators successfully identified a transmission station equipped with specific antenna arrays at Okunevo in March 2025 (Höller, 2025). Identified as the Baltic Jammer, this system has consistently disrupted civil aviation navigation services throughout the Baltic states, with signals originating directly from the Kaliningrad exclave (Jonsson, 2024).

Image 17. Supposed Location of the Baltic Jammer

Source Google Earth, processed by Höller (2025)

5.3.4. Way forward

To mitigate the pervasive threat of GNSS jamming along the Ukrainian front, drone operators have pioneered various technological adaptations to bolster the resilience of Unmanned Aerial Vehicles against electronic warfare. Perhaps the most prominent

improvisation involves tethering platforms via fibre-optic cables, which facilitates secure remote command-and-control immune to signal interference. Such a solution appears unsustainable, however, as the accumulation of discarded cabling presents long-term environmental hazards and represents a localized tactical stopgap rather than a strategic resolution to systemic jamming. Exploring more sophisticated alternatives, Maxar introduced the Raptor system to enable navigation in environments compromised by spoofing or signal denial (Erwin, 2025). By utilizing VHR optical imagery to construct a synthetic visual map, the system allows a drone to orient itself through the correlation of the Maxar Earth Observation database with real-time data from onboard camera sensors. This approach facilitates genuine operational autonomy, allowing for pre-tasked missions that bypass the requirement for continuous human intervention or vulnerable datalinks (Vantor, 2025) . These advancements hold significant potential for transfer into the civilian sphere, particularly within commercial aviation, to fortify critical infrastructure against state-sponsored hybrid threats and electronic interference.

The provided visualization illustrates the efficacy of Raptor technology; the erratic red line denotes the inaccurate GNSS-based positioning, whereas the yellow and green trajectories accurately track the actual location and projected heading of the drone (Vantor, 2025).

Fig. 14 Maxar Raptor Technolgy (illustration)

Source: (Vantor, 2025)

This technological transition reflects the American dual-use philosophy embedded within these solutions to foster greater systemic and technological autonomy. Evidence presented in preceding sections suggests that Europe has yet to secure a leadership position in space-based solutions, continuing to face challenges regarding specific operational applications. Integrating Space as a Service (SaaS) models could provide a viable pathway to catalyse private sector investment, thereby ensuring that the European New Space ecosystem secures the requisite capital to achieve its broader innovation objectives (Golovtchenko, 2026).

6. Conclusion

This research was designed to address a primary research question rooted in a discernible literature gap regarding the practical application of Earth Observation (EO) and broader space technologies in countering hybrid threats. Specifically, the investigation centres on Europe and its evolving concerns regarding strategic autonomy, both in defence contexts and within emerging technological sectors like space. Initial chapters delineated the conceptual boundaries of strategic autonomy with a focus on the European space sector, while the second component defined the

pervasive impact of hybrid threats on continental security, highlighting how these challenges deviate from kinetic, traditional warfare. Within the third theoretical section, the study detailed space-based technologies and the specificities of EO science, mapping a trajectory for Europe to leverage these assets to bolster resilience. To facilitate a quantitative assessment of European EO capacity, a diagnostic framework was introduced to evaluate real-world applications.

To evaluate strategic autonomy in the space domain, this study utilized the three levelled theoretical framework established by Fiott (2020), which categorizes autonomy into the branches of "for," "to," and "from." The first phase of this analysis scrutinized European political will concerning EO for security, identifying clear incentives from the European Space Agency (ESA), the European Union, and NATO to prioritize space-based security in both strategic planning and budgetary allocations. Findings indicate a decisive pivot in European policy toward security-centric EO applications. Notably, the ESA Agenda 2025 (ESA, 2025) urges a move toward security-oriented research, marking a departure from the organization’s historical emphasis on civilian and purely scientific activities. This shift raises complex questions regarding the agency's membership, which includes neutral states like Switzerland and non-European observers such as Canada. On the regulatory front, recent European Parliament elections and Commission initiatives signal a robust political drive to empower strategic autonomy through space. The publication of the EUSSSD (European Union Space Strategy for Security and Defence, 2023) formally categorizes space as a contested domain with tangible defence applications. Furthermore, the development of the Earth Observation Governmental Service (EOGS) reflects an urgent requirement for sovereign Intelligence, Surveillance, and Reconnaissance (ISR) capabilities to serve both EU and national security providers. This initiative underscores the growing complementarity between the EU and ESA, with EUSPA functioning as a vital intermediary to reduce sectoral fragmentation. Finally, following the evolution of American doctrine and the formal recognition of space as a distinct operational domain alongside land, sea, air, and cyber, NATO has intensified its focus on defence applications through its overarching space policy (NATO, 2019). This doctrinal transition toward Multi-Domain Operations (MDO) mandates the synergistic use of all five domains. Concretely, the APSS initiative (NATO, 2023) demonstrates the critical nature of EO for ISR and the necessity of pooling capabilities between NATO allies, the EU, and the ESA.

Regarding the assessment of European sovereign capabilities, the second analytical pillar focuses on the robustness of the domestic space industry. This evaluation initially examines European space market health before scrutinizing financial investment data specifically within the earth observation (EO) sector; subsequently, it maps key industrial actors and their respective technological capacities. Data concerning the broader European market illustrates a diverse array of satellite technologies, where EO maintains high visibility, yet communication satellites continue to dominate the portfolios of less mature space nations. Cases such as Luxembourg, which allocates a disproportionate share of its GDP to space technologies to leverage a distinct comparative advantage, further highlight these shifting dynamics. Public markets clearly emerge as primary catalysts for industrial development, representing the vast majority of infrastructure investment. Within this framework, the military applications serves as a critical driver for innovation, particularly in military earth observation, which remains essential for maintaining national situational awareness and ensuring access to cutting-edge surveillance assets. Market analysis confirms a heavy reliance on institutional funding for EO technologies, with the European Space Agency accounting for a significant percentage of industry sales. This structural dependence likely stems from a combination of high market entry costs, a reliance on subsidized funding, and a relatively late pivot toward defence-oriented applications. While the New Space ecosystem acts as a fragmented yet promising engine for innovation, challenging the global dominance of traditional players like Airbus Defence and Space. Despite holding strong actors across optical, SAR, infrared, hyperspectral, and radio frequency domains with clear security applications, European firms often struggle with domestic procurement and financing gaps that slow long-term innovation.

The third dimension of strategic autonomy entails European Earth Observation (EO) capabilities categorized by spatial, temporal, and spectral resolutions. Regarding image precision, Europe maintains highly competitive assets distributed across member states, particularly in Very High Resolution (VHR) sensors that ensure technological sovereignty. Temporal resolution presents a further challenge, currently, few European constellations provide revisit times under twenty-four hours, a limitation that renders persistent surveillance impossible and creates gaps in situational awareness. While the prevailing trend toward building larger constellations offers a

potential remedy, it simultaneously encourages orbital congestion. The European Space Agency has countered this by fostering a federation of missions under the Copernicus Contributing Missions framework, which appears to provide a viable pathway for addressing temporal deficiencies. In terms of spectral resolution, while radar and optical systems remain well established across the continent, certain gaps persist in hyperspectral and radiofrequency (RF) sensing. Nevertheless, recent French and Luxembourgish RF initiatives suggest a narrowing of these disparities.

The second component of this analysis applies the GMES Working Group on Security (2003) diagnostic framework to evaluate the capacity of specific nations to fulfil security-related tasks. Quantitative assessments indicate that while most requirements can be met through the collective spatial and temporal capabilities of France and Spain, this validates the fact that Europe possesses sufficient strategic autonomy to avoid total dependence on foreign entities for core security needs. This autonomy is, however, relative. When measured against groundbreaking Chinese innovations, such as GEO-based high-resolution optical imagery, spectral diversity, and constellations with 10min revisit times, Europe is behind. Despite these specific technological dependencies, Europe is not being left behind in terms of sovereign capability. Instead, it effectively harnesses the shift toward pooling resources as a strategic mechanism to combat the inherent fragmentation of its decentralized space architecture.

Following the definition of European strategic autonomy in space, this second research phase evaluates the core hypothesis regarding the enhancement of resilience against hybrid threats through three distinct case studies chosen to highlight capabilities in detection, attribution, response, and deterrence. These cases are analysed via the conceptual framework established by Giannopoulos et al. (2021) to facilitate empirical comparison. Selection was predicated on the intensity levels defined within the activity pillar of said model. The 2022 sabotage of the Nord Stream 1 and 2 pipelines represent a clear act of coercion situated near the threshold of open warfare. Conversely, the repeated weaponization of migrants at the borders of Poland, Lithuania, and Latvia by Belarus serves as a secondary case, positioned at the destabilization phase and operational level. Finally, the persistent GNSS jamming and spoofing originating from the Kaliningrad exclave reflects a less intense but more enduring threat, categorized within the destabilization phase at a lower operational level.

Analysis of the Nord Stream sabotage indicates that detection via optical imagery provided significant clarity, though results varied based on the spatial resolution required for specific applications. Synthetic Aperture Radar (SAR) imagery proved vital in mitigating the persistent cloud cover of the Baltic Sea, ensuring continuous monitoring regardless of weather conditions. In the subsequent attribution and response phases, Radio Frequency (RF) data and Automatic Identification System (AIS) tracking were deployed to investigate the actors involved, while specialized atmospheric sensors identified methane leaks to quantify the resulting environmental degradation. To bolster future deterrence, enhanced surveillance was established utilizing European SAR assets and RF detection through the Unseenlabs constellation. This technical versatility suggests that European security authorities possess a high degree of autonomy, even if certain methane emission data relied on Canadian partners. Ultimately, the pooling and federation of Earth observation data appears to be a viable pathway for constructing strategic autonomy through institutional cooperation.

In the second instance concerning the weaponization of migration by Belarus, satellite imagery proved instrumental for detection by integrating Synthetic Aperture Radar (SAR) data with very high-resolution optical products. Frontex and national border patrols from Poland and the Baltic states utilized these assets to monitor evolving situations and calibrate their responses based on the perceived scale of the threat. Regarding the data source, the political sensitivity of this case complicates the access to open imagery. While space-based capabilities played a secondary role in direct attribution, they facilitated the evaluation of migrant flows, helping authorities gauge the necessary infrastructure to counter such threats and maintain deterrence through persistent surveillance. Augmenting ground-based sensors with orbital platforms ensures a superior data baseline for the future of border security. Emerging technologies such ultra-high-resolution sensors or advanced SAR variants may offer more comprehensive monitoring to better anticipate the fallout from such hybrid actions.

For the last case, on the detection of GNSS jamming and spoofing, it may be achieved through radio frequency (RF) monitoring satellites, a capability currently dominated by American commercial providers. Such interference can also be identified by correlating SAR imagery with optical data, employing innovative scientific methodologies to

pinpoint the origins of radio frequency disturbances. Attributing these disruptions in satellite navigation is vital, as they threaten civilian transportation and critical services like financial market timing. To mitigate these vulnerabilities, new frameworks are being developed to fuse Earth Observation data directly into autonomous transport systems. This integration aims to bolster resilience against spoofing or jamming by providing alternative positioning verification that does not rely solely on traditional GNSS signals.

Synthesizing these empirical findings allows for a nuanced resolution to the primary research question, suggesting that while European strategic autonomy in space appears comprehensive regarding spatial and spectral resolutions, a significant gap remains in temporal resolution. Addressing this shortfall requires investment in innovation and the promotion of space as a service business models. Such initiatives would ensure that both institutional and private actors grasp the inherent utility of space-based assets, potentially allowing the sector to achieve the same transformation that what is observed in artificial intelligence. Beyond technical specifications, Earth observation technologies offer a robust framework for augmenting regional resilience against hybrid threats. This includes the persistent surveillance of maritime corridors and critical infrastructure, as well as the monitoring of sensitive border zones. Such capabilities facilitate early risk detection and the anticipation of adversary manoeuvres during periods of escalation. Additionally, innovative EO-integrated solutions could mitigate the disruptive impacts of GNSS jamming and spoofing. This rapid expansion nonetheless necessitates a careful evaluation of Low Earth Orbit congestion, even as it opens novel avenues for lunar observation satellites. By applying terrestrial monitoring techniques to the lunar environment, Europe might effectively pre-empt the various geopolitical and safety risks associated with the next era of deep space exploration.

Bibliography

A Strategic Compass for Security and Defence, European Commission (2022).

Agreement Between the UNITED STATES OF AMERICA and OTHER GOVERNMENTS, Pub. L. (80 Stat. 271; 1 U.S.C. 113), TREATIES AND OTHER INTERNATIONAL ACTS SERIES 11-1212 (2004).

Airbus Defence and Space. (2022). *Nord Stream 2, Sweden high quality satellite image | Pleiades Neo*. https://space-solutions.airbus.com/resources/satellite-image-gallery/pleiades-neo/pleiades-neo-nord-stream-2/

Albani, S., Lazzarini, M., Saameno, P., Luna, A., & Barrilero, O. (2022). NEW SCENARIOS SHAPING A DIGITAL TWIN EARTH FOR SECURITY. *European Union Satellite Centre* . www.ec-better.eu

Allen, M. (2025). Guarding Europe's hidden lifelines: how AI could protect subsea infrastructure A wake-up call in the Baltic. *Horizon, The EU Research & Innovation Magazine*.

Almäng, J. (2019). War, vagueness and hybrid war. *Defence Studies*, *19*(2), 189–204. https://doi.org/10.1080/14702436.2019.1597631

Anghel, S., Immenkamp, B., Lazarou, E., Saulnier, J. L., & Wilson, A. B. (2020). On the path to 'strategic autonomy' The EU in an evolving geopolitical environment. *European Parliamentary Research Service*.

Ballinger, O. (2022). Radar Interference Tracker: A New Open Source Tool to Locate Active Military Radar Systems . *Bellingcat*. https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-tool-to-locate-active-military-radar-systems/

Bartóki-Gönczy, B., & Malinowska, K. (2025). Paradigm shift in the European Union's space policy: institutional restructuring and its possible consequences for the CEE region. *Frontiers in Political Science*, *7*. https://doi.org/10.3389/fpos.2025.1536170

Bataille, M. (2026, February 12). *Interview conducted by Alexandre Touati: European strategic autonomy in Earth observation?*

Baumann, M., & Pynnöniemi, K. (2025). European Security in the Era of Hybrid Warfare, Active Measures in Russia's Confrontation with Europe. *DGAP Policy Brief*. https://www.iiss.org/research-

Bişag, R.-C., & Ilinca, D. (2025). Enhancing Security Through Earth Observation: The Role of Copernicus in Monitoring Emerging Threats. *Land Forces Academy Review*, *30*(2), 321–332. https://doi.org/10.2478/raft-2025-0031

Bo Lillis, K., Bertrand, N., & Atwood, K. (2022, February 11). How the Biden administration is aggressively releasing intelligence in an attempt to deter Russia. *CNN Politics*. https://edition.cnn.com/2022/02/11/politics/biden-administration-russia-intelligence

Borrell, J. (2020). *Why European strategic autonomy matters* . EEAS. https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en

Boyse, M. (2026). Weaponized Mass Migration: A Security Risk to Europe and the United States . *Hudson Institute*. https://www.hudson.org/regulation/weaponized-mass-migration-security-risk-europe-united-states-matt-boyse

Braw, E. (2025). *How the Baltic Sea nations have tackled suspicious cable cuts*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/

Brennan, L. (2019). How Luxembourg is positioning itself to be the centre of space business. *The Conversation*. https://doi.org/10.64628/AB.twua5aqcx

Breton, T. (2022). *Speech by Commissioner Breton at the 14th Space Conference*. https://ec.europa.eu/commission/presscorner/detail/es/speech_22_561

Caliskan, M., & Liégeois, M. (2021). The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars and Insurgencies*, *32*(2), 295–319. https://doi.org/10.1080/09592318.2020.1860374

Capaul, I. (2024). A Taxonomy of Hybrid Threats. *CSS Analyses in Security Policy*, *352*.

Cellerino, C. (2023). *EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the 'Security and Defence Dimension of the Union in Space'*. *8*(2), 487–501. https://doi.org/10.15166/2499-8249/669

Chabert, V. (2023). NATO looking up: the relevance of outer space in a changing security environment. *Futuri*.

Chapman, Bert. (2025). *Space Strategy and Military Doctrine*. Bloomsbury Academic.

Clark, S. (2022). *Soyuz launches Russian military spy satellite*. Spaceflight Now. https://spaceflightnow.com/2022/02/07/soyuz-launches-russian-military-spy-satellite/

Copernicus. (2019). *OBSERVER: Copernicus - Eyes on the EU's external borders*. https://www.copernicus.eu/en/observer-copernicus-eyes-on-EU-external-borders

Crosetto, G. (2025). *Countering Hybrid Warfare: An Active Strategy*.

Cross, M. K. D. (2022). Space Security and the Transatlantic Relationship. *Politics and Governance*, *10*(2), 134–143. https://doi.org/10.17645/pag.v10i2.5061

CSpOC. (2026). *Objects in Orbit*. Space-Track.Org. https://www.space-track.org/basicspacedata/query/class/satcat/predicates/OBJECT_ID,OBJECT_NAME,NORAD_CAT_ID,COUNTRY,PERIOD,INCLINATION,APOGEE,PERIGEE,RCS_SIZE,RCSVALUE,LAUNCH,COMMENT/DECAY/null-val/CURRENT/Y/orderby/NORAD_CAT_ID%20desc/format/csv/emptyresult/show

Czulda, R. (2024). The EU's space strategy for security and defence. *ESD*.

De Man, P., & Wouters, J. (2025). Global Policy EU Space Governance at the Threshold of A New Era. *Global Policy*, *0*, 1–5. https://doi.org/10.1111/1758-5899.70030

Defence Intelligence Agency. (2022). *Challenges to Security in Space*. www.dia.mil/Military-Power-Publications

Devlin, K., Metzlerand, B., & Nguyen, K. (2025). Dozens of sanctioned Russian tankers navigate Channel despite UK vow of 'assertive' action. *BBC*. https://www.bbc.com/news/articles/c2d77rr51rko

DG Migration and Home Affairs. (2024). *Commission issues Communication countering the weaponisation of migration and provides funding to enhance border surveillance capabilities*. European Commission. https://home-affairs.ec.europa.eu/news/commission-issues-communication-countering-weaponisation-migration-and-provides-funding-enhance-2024-12-11_en

Divišová, V., Frank, L., Hanzelka, J., Novotný, A., & Břeň, J. (2021). "The Whole is Greater than the Sum of the Parts". Towards Developing a Multidimensional Concept of Armed Forces' Resilience Towards Hybrid Interference. *Obrana a Strategie*, *21*(2), 3–20.

Draghi, M. (2024). *The Future of European Competitiveness—A Competitiveness Strategy for Europe.*

EARSC. (2023). Industry views on the EU Space Strategy for Security and Defence. *Position Paper from the European Earth Observation Downstream Services Industry*.

EDA. (2024a). EDA's contribution to the EU Space Programme mid-term review. *European Commission*. https://doi.org/10.1080/14702436.2023.2277440

EDA. (2024b). *European satellite constellation for very low earth orbit to launch in two years*. https://eda.europa.eu/news-and-events/news/2024/03/06/european-satellite-constellation-for-very-low-earth-orbit-to-launch-in-two-years

Edwards, C., & Seidenstein, N. (2025). The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. *The International Institute for Strategic Studies*.

EEAS. (2016). *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*.

eoPortal. (2025a). *BRO (Breizh Reconnaissance Orbiter) / Unseenlabs*. https://www.eoportal.org/satellite-missions/unseenlabs

eoPortal. (2025b). *Clarity (Albedo Space)*. https://www.eoportal.org/satellite-missions/clarity#spaceandhardwarecomponents

eoPortal. (2025c). *Spire Global Nanosatellite Constellation*. https://www.eoportal.org/satellite-missions/spire-global#ads-b-automatic-dependent-surveillance-broadcast

Erwin, S. (2024). *Planet signs deal with NATO to supply satellite imagery*. SpaceNews. https://spacenews.com/planet-signs-deal-with-nato-to-supply-satellite-imagery/

Erwin, S. (2025). Maxar launches GPS-alternative navigation system for drones . *SpaceNews*. https://spacenews.com/maxar-launches-gps-alternative-navigation-system-for-drones/

ESA. (2002). *The European Union and ESA: the need for closer working relations*. https://www.esa.int/About_Us/Corporate_news/The_European_Union_and_ESA_the_need_for_closer_working_relations

ESA. (2013). *Copernicus, Satellites Help to Monitor Infrastructure Stability*. www.esa.int/copernicus

ESA. (2020a). *ESA and EDA joint research: advancing into the unknown*. https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_and_EDA_joint_research_advancing_into_the_unknown

ESA. (2020b). *Types of orbits*. https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

ESA. (2022a). *Civil security from space*. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Civil_security_from_space

ESA. (2022b). *Satellites detect methane plume in Nord Stream leak*. https://www.esa.int/Applications/Observing_the_Earth/Satellites_detect_methane_plume_in_Nord_Stream_leak

ESA. (2024). *EarthCARE*. https://www.esa.int/Applications/Observing_the_Earth/FutureEO/EarthCARE

ESA. (2025). *ESA Agenda 2025, Make space for Europe*. www.morganstanley.com/ideas/investing-in-space.

ESA, & ESPI. (2021). 1st ESA Security Conference, Proceedings. *PROCEEDINGS*. https://www.google.com/search?q=1st+ESA+Security+Conference%2C+Proceedings%2C+(2021)&oq=1st+esa+&gs_lcrp=EgRlZGdlKgkIABBFGDsY-QcyCQgAEEUYOxj5BzIGCAEQRRg5MggIAhAAGBYYHjIICAMQABgWGB4yCAgEEAAYFhgeMgcIBRAAGO8FMgoIBhAAGIAEGKIEMgcIBxAAGO8FMgcICBAAGO8FMggICRDpBxj8VdIBCDM0NzdqMGoxqAIAsAIA&sourceid=chrome&ie=UTF-8

ESA, & ESPI. (2023). 2nd ESA Security Conference. *PROCEEDINGS*.

ESPI. (2020). Europe, Space and Defence From ‘Space for Defence’ to ‘Defence of Space’. In *ESPI Report 72-Europe, Space and Defence-Full Report"*. www.espi.or.at

ESPI. (2023). High time for an EU Space Strategy for Security and Defence. *Brief No. 63*.

ESPI. (2024a). ESPI contribution to the EU Space Programme mid-term review. *European Commission*. https://www.espi.eu/wp-content/uploads/2023/11/ESPI_Evaluation_EUSpaceProgramme-1.pdf

ESPI. (2024b). *ESPI2040: Space for Prosperity, Peace and Future Generations*. https://www.espi.eu/espi-2040/

ESPI. (2024c). *Will Space Sit in The European Parliament?* www.espi.or.at

European Commission. (2021a). *2021 Strategic Foresight Report*.

European Commission. (2021b). Action Plan on synergies between civil, defence and space industries. *COM(2021) 70 Final*.

European Commission. (2021c). *European Space Programme*. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/european-space-programme_en#budget-and-performance

European Commission. (2022). *Commission contribution to European defence*. COM(2022) 60 Final. https://commission.europa.eu/system/files/2022-02/com_2022_60_1_en_act_contribution_european_defence.pdf

European Commission. (2023). *Copernicus Security Services Strategic Research Agenda*.

European Commission. (2024a). Indicative multiannual perspective 2024-2027 . *European Defence Fund*.

European Commission. (2024b). Proposal for a Regulation of the European Parliament and of the Council establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products ('EDIP') . *COM(2024) 150 Final*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024PC0150

European Commission. (2025). The European Annual Asylum and Migration Report . *COM 795*. http://data.europa.eu/eli/reg/2024/1349/oj.

European Council. (2016). Implementation Plan on Security and Defence. *High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, and Head of the European Defence Agency* .

European Council. (2024). Strengthening Europe's competitiveness through space: Council conclusions . *Document 10142/24*. https://data.consilium.europa.eu/doc/document/ST-10142-2024-INIT/en/pdf

European Parliament. (2021). *Regulation - 2021/696 - EN - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2021/696/oj/eng

European Union Space Strategy for Security and Defence (2023).

Eurospace. (2024). *28th edition of the annual facts and figures report*.

Eurospace. (2025). 29th edition of the annual facts and figures report. *ASD*.

Evroux, C. (2024). EU space policy: State of play. *European Parliamentary Research Service*.

Evroux, C. (2025). EU space act. *European Parliamentary Research Service*.

Fabbrini, S. (2017). Intergovernmentalism in the European Union. A comparative federalism perspective. *Journal of European Public Policy*, *24*(4), 580–597.

https://doi.org/10.1080/13501763.2016.1273375;WEBSITE:WEBSITE:TFOPB;PAGEGROUP:STRING:PUBLICATION

Fiott, D. (2018). Strategic autonomy: towards ‘European sovereignty’ in defence? *EUISS*.

Fiott, D. (2020). The European space sector as an enabler of EU strategic autonomy . *Policy Department for External Relations*. https://doi.org/10.2861/983199

Fiott, D. (2021a). *How can space support the EU’s Strategic Compass? SECURING THE HEAVENS*.

Fiott, D. (2021b). Strategic Sovereignty: Three Observations About a New and Contested Term. In D. Fiott (Ed.), *European Sovereignty, Strategy and interdependence* (Vol. 169, pp. 7–15). EU Institute for Security Studies. https://doi.org/10.2815/649889

Flightradar24. (n.d.). *GPS jamming & interference map*. Retrieved 16 February 2026, from https://www.flightradar24.com/data/gps-jamming

Franzoso, M. (2024). Navigating the Tensions: ESA, EU, the Geographical Return Principle, and Competitiveness in the European Ambit. *Business Law Review*, *45*(Issue 2), 36–40. https://doi.org/10.54648/BULA2024005

Frontex. (2025). *Earth Observation for Border Management*. www.frontex.europa.eu

Funaiole, M. P., Hart, B., & Power-Riggs, A. (2026). *In China’s Orbit: Beijing’s Space Diplomacy in the Global South*. CSIS. https://features.csis.org/hiddenreach/china-space-diplomacy-global-south/

Galeotti, M. (2016). ‘Hybrid War or Gibridnaya Voina? Getting Russia’s non-linear military challenge right’. In *Post-Soviet Armies Newslette*. Mayak Intelligence.

Gannon, A. J., Gartzke, E., Lindsay, J. R., & Schram, P. (2022). The Shadow of Deterrence: Why capable actors engage in contests short of war. *Center for Peace and Security Studies* . https://github.com/CenterForPeaceAndSecurityStudies/GrayZone.

Gartzke, E., & Lindsay, J. R. (2024). Elements of Deterrence : Strategy, Technology, and Complexity in Global Politics. In *Elements of Deterrence*. Oxford University Press. https://doi.org/10.1093/OSO/9780197754443.001.0001

Getty Images. (2020). *5 Satellite Image Border Refugee Europe Stock Photos, High-Res Pictures, and Images - .* Maxar. https://www.gettyimages.ch/search/2/image?phrase=satellite%20image%20border%20refugee%20europe&sort=mostpopular&license=rf%2Crm

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). The landscape of Hybrid Threats : a conceptual model. *Publications Office of the European Union*. https://doi.org/10.2760/44985

Giegerich, B. (2007). Cambridge Review of International Affairs Navigating differences: transatlantic negotiations over Galileo Navigating differences: transatlantic negotiations over Galileo. *Cambridge Review of International Affairs*, *20*(3), 491–508. https://doi.org/10.1080/09557570701574196

GMES Working Group on Security. (2003). *The security dimension of GMES :*

Golovtchenko, V. (2026, February 17). *Interview conducted by Alexandre Touati: European strategic autonomy in Earth observation?*

González Muñoz, R., & Portela, C. (2023). The EU Space Strategy for Security and Defence: Towards Strategic Autonomy? *Non-Proliferation and Disarmament Papers*, *83*.

Goward, D. (2022). *Why isn't Russia doing more to jam GPS in Ukraine?* C4ISRNET. https://www.c4isrnet.com/opinion/2022/07/22/why-isnt-russia-jamming-gps-harder-in-ukraine/

Gray, C. S. (2012). *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*. US Army War College Press. https://press.armywarcollege.edu/monographs/561

Gross, S., & Stelzenmüller, C. (2024). *Europe's messy Russian gas divorce*. Brookings. https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/

Hagolle, O. (2022). *First satellite images of Nord Stream leaks*. CESBIO. https://www.cesbio.cnrs.fr/multitemp/first-satellite-images-of-nord-stream-leaks/

Hainaut, B. (2024). *NATO's New Ambitions for Space*. www.nato.int.

Hartmann, U. (2017). The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. *Research Paper NATO Defence College*, *139*. https://facebook.com/NDC_Research

Helwig, N., & Sinkkonen, V. (2022). *Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_645

Hennig, S. (2013). Exploring the Benefits of Active vs. Passive Spaceborne Systems. *Earth Imaging Journal*. https://eijournal.com/print/articles/exploring-the-benefits-of-active-vs-passive-spaceborne-systems

Hoffman, F. G. (2007). *The Rise of Hybrid Wars*. http://www.potomacinstitute.org/

Höller, L. (2025). *Researchers home in on origins of Russia's Baltic GPS jamming*. DefenseNews. https://www.defensenews.com/global/europe/2025/07/02/researchers-home-in-on-origins-of-russias-baltic-gps-jamming/

Hommerich, L., Stark, H., & Zimmermann, F. (2023). *Nord Stream Pipeline Attack: Who Blew up Nord Stream?* DIE ZEIT. https://www.zeit.de/politik/2023-09/nord-stream-pipelines-attack-anniversary-english/komplettansicht

Höyhtyä, M., & Uusipaavalniemi, S. (2023). The space domain and the Russo-Ukrainian war: Actors, tools, and impact. *Hybrid CoE Working Paper 21*. https://www.researchgate.net/publication/367008350_The_space_domain_and_the_Russo-Ukrainian_war_Actors_tools_and_impact

Human Rights Watch. (2022). *Airborne Complicity: Frontex Aerial Surveillance Enables Abuse*. Border Forensic. https://www.hrw.org/video-photos/interactive/2022/12/08/airborne-complicity-frontex-aerial-surveillance-enables-abuse

ICEYE. (n.d.). *SAR border monitoring*. Retrieved 15 February 2026, from https://www.iceye.com/sar-border-monitoring

ICEYE. (2026). *Ukraine expands partnership with ICEYE*. https://www.iceye.com/newsroom/press-releases/ukraine-expands-partnership-with-iceye

Innoter. (2024). *Remote Sensing in Russia. Myths of the past, harsh present, unrealistic future*. https://innoter.com/en/articles/remote-sensing-in-russia-myths-of-the-past-harsh-present-unrealistic-future/

Jaiswal, R. (2022). *Updates on Indian Space Programme – 2022*.

Joint Research Centre. (2025). *Earth Observation for security*. European Commission. https://joint-research-centre.ec.europa.eu/projects-and-activities/earth-observation-security_en

Jones, A. (2023). *China launches first geosynchronous orbit radar satellite*. SpaceNews. https://spacenews.com/china-launches-first-geosynchronous-orbit-radar-satellite/

Jones, S. G. (2025). Russia's Shadow War Against the West. *CSIS*.

Jones, S., Hollinger, P., & Bott, I. (2026, February 4). Russian spy spacecraft have intercepted Europe's key satellites, officials believe. *Financial Times*. https://www.ft.com/content/cd08c49c-658e-49c9-9a15-234f2bfc2074

Jonsson, M. (2024). *Thread by @auonsson on Thread Reader App – Thread Reader App*. X Thread Reader. https://threadreaderapp.com/thread/1776701617842073956.html?utm_campaign=topunroll

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., & Giannopoulos, G. (2023). *Hybrid threats : a comprehensive resilience ecosystem*. Publications Office of the European Union.

Kahan, J. H., Allen, A. C., & George, J. K. (2009). An Operational Framework for Resilience. *Journal of Homeland Security and Emergency Management*, *6*(1). www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

KEFM, & UFM. (2024). *Strategy for space research and innovation Strategy for space research and innovation* .

Kotaridis, I., & Benekos, G. (2023). Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: A case study of the Ukraine–Russia war. *Security and Defence Quarterly*, *43*(3), 1–21. https://doi.org/10.35467/sdq/170901

Kramer, F. D., Dailey, A. M., & Brodfuehrer, J. (2024). *NATO multidomain operations: Near- and medium-term priority initiatives*.

Krebs, G. D. (n.d.). *Spacecraft: Earth Observation - India*. Gunter's Space Page. Retrieved 14 February 2026, from https://space.skyrocket.de/directories/sat_eo_ind.htm

Lewis, J. A. (2004). *Galileo and GPS: From Competition to Cooperation*.

Libek, E. (2019). European Strategic Autonomy: A Cacophony of Political Visions - International Centre for Defence and Security. *RKK ICDS*. https://icds.ee/en/european-strategic-autonomy-a-cacophony-of-political-visions/

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies*, *46*(4), 858–880. https://doi.org/10.1080/01402390.2023.2177987

Lieberman, S., & Hoerber, T. (2024). Finding space for the European Space Agency. *Space Policy*, *69*. https://doi.org/10.1016/j.spacepol.2024.101637

Lin, M., Jin, M., Li, J., & Bai, Y. (2024). GEOSatDB: global civil earth observation satellite semantic database. *Big Earth Data*, *8*(3), 522–539. https://doi.org/10.1080/20964471.2024.2331992

Lindström, G., & Gasparini, G. (2003). The Galileo satellite system and its security implications . *Occasional Papers N°44*. www.iss-eu.org

Linkov, I., Baiardi, F., Florin, M.-V., Greer, S., Lambert, J. H., Pollock, M., Rickli, J.-M., Roslycky, L., Seager, T., Thorisson, H., & Trump, B. D. (2019). Applying Resilience to Hybrid Threats. *Resilient Security*, 78–83. https://www.academia.edu/118987755/Applying_Resilience_to_Hybrid_Threats

Lionnet, P. (2023). *The Earth Observation infrastructure landscape*. Eurospace. https://eurospace.org/the-earth-observation-infrastructure-landscape/

López, L. D. (2023). BRICS+ from Above: Why the Space Dimension of the Expanded Alliance Matters. *CSIS*.

Lund, B., Eggertsson, G. A., Schmidt, P., Roth, M., Voss, P., Larsen, T. B., Dahl-Jensen, T., Rinds, N., Köhler, A., Goertz-Allmann, B. P., Alvizuri, C., Dando, B., Schweitzer, J., Oye, V., Dunham, E. M., Steinberg, A., Gestermann, N., Ceranna, L., Hartmann, G., … Weidle, C. (2023). Seismic Analysis of the Nord Stream Underwater Explosions. *AGUFM*, *2023*, S52A-06. https://ui.adsabs.harvard.edu/abs/2023AGUFM.S52A..06L/abstract

Lynch, M. (2025). From the Last Frontier to the Final Frontier: The Polar Regions and Space Security. *Space and Defense*, *16*(1). https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1307&context=spaceanddefense

Macchiarulo, V., Milillo, P., Blenkinsopp, C., & Giardina, G. (2022). Monitoring deformations of infrastructure networks: A fully automated GIS integration and analysis of InSAR time-series. *Structural Health Monitoring*, *21*(4), 1849–1878. https://doi.org/10.1177/14759217211045912

McDowell, J. (2026). *Space Activities in 2025*.

Monaghan, S. (2019). Countering Hybrid Warfare. *PRISM*, *8*(2), 82–99. https://doi.org/10.2307/26803232

Montgomery, M. (2026). *Weaponized Mass Migration*. FDD. https://www.fdd.org/analysis/2026/02/10/weaponized-mass-migration/

Monti-Guarnieri, A., Giudici, D., & Recchia, A. (2017). Identification of C-Band Radio Frequency Interferences from Sentinel-1 Data. *Remote Sensing 2017, Vol. 9, 9*(11). https://doi.org/10.3390/rs9111183

Mumford, A., & McDonald, J. (2014). *Ambiguous Warfare*.

Murphy, M., Hoffman, F. G., & Schaub, G. (2016). *Hybrid Maritime Warfare and the Baltic Sea Region*. http://cms.polsci.ku.dk/.

Muti, K., & Nones, M. (2024). European Space Governance and Its Implications for Italy edited by Karolina Muti and Michele Nones. *Documenti IAI*, (24).

NASIC. (2018). Competing in Space. *USAF*.

NATO. (n.d.). *What DIANA offers*.

NATO. (2019). *NATO's overarching Space Policy*. NATO Official Text. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/06/27/natos-overarching-space-policy

NATO. (2023). Alliance Persistent Surveillance from Space (APSS) Overview. *NATO Factsheet*. www.nato.int

NATO. (2025). *NATO's approach to space*. Nato.Int. https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-approach-to-space

NATO ACT. (2025). *Task Force X Baltic: Denmark and Finland Advance NATO's Maritime Vigilance Through Innovation* . https://www.act.nato.int/article/tfx-denmark-finland/

NATO, & EU. (2023). *3rd Joint Declaration on EU-NATO Cooperation*. https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

NATO STO. (2020). *Science & technology trends: 2020-2040*. https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NOAA. (2024). *What is remote sensing?*

OECD. (2021). Evolving Public-Private Relations in the Space Sector, Lessons Learned for the Post-COVID-19 Era. *OECD Science, Technology and Industry*, *114*. http://www.oecd.org/termsandconditions.

OECD. (2023). *The Space Economy in Figures: Responding to Global Challenges*. https://doi.org/https://doi.org/10.1787/fa5494aa-en

Olech, A. (2025). Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses. *Terroryzm*, *2025*(Special Issue), 133. https://doi.org/10.4467/27204383ter.25.017.21520

Omand, D. (2005). Developing national resilience. *RUSI Journal*, *150*(4), 14–18. https://doi.org/10.1080/03071840508522884

Onoda, M., & Young, O. R. (2017). Satellite Earth Observations in Environmental Problem-Solving. In M. Onoda & O. R. Young (Eds.), *Satellite Earth Observations and Their Impact on Society and Policy* (pp. 3–30). Springer Nature.

Ortega, A. A. (2023). Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems. *Lawfare*. https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems

Palmer, C. (2025). Very Low Earth Orbit Satellites Promise Greater Resolution…and Less Privacy. *Engineering*, *46*, 6–8. https://doi.org/10.1016/J.ENG.2025.01.009

Patarin-Jossec, J. (2020). Materialising sovereignty: European space industries in the Europeanisation-nationalism nexus. *Journal of Contemporary European Studies*, *28*(2), 257–268. https://doi.org/10.1080/14782804.2020.1734551

Peerboom, F. (2022). Protecting Borders or Individual Rights? A Comparative Due Process Rights Analysis of EU and Member State Responses to 'Weaponised' Migration. *European Papers - A Journal on Law and Integration*, *2022 7*(2), 583–600. https://doi.org/10.15166/2499-8249/580

Pellegrino, M., & Stang, G. (2016). Space security for Europe. *EUISS, ISSUE*, *29*.

Pillai, H. (2023). *Protecting Europe's critical infrastructure from Russian hybrid threats*.

Pischedda, C., Cheon, A., & Moller, S. B. (2024). Can you have it both ways? Attribution and plausible deniability in unclaimed coercion. *European Journal of International Security*, *9*(4), 493–510. https://doi.org/10.1017/eis.2024.14

Poirier, C., Bataille, M., & Petzold, L. (2023). EU space policy and the involvement of civil society. *Foresight, Studies and Policy Assessment Unit, EESC*.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Safety, Resilience and Sustainability of Space Activities in the Union, COM/2025/335 final (2025). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0335

RÁCZ, A. (2022). *An Orchestrated Crisis Misplayed - Belarus, Russia, and the Weaponisation of Migration*. PISM. https://pism.pl/publications/an-orchestrated-crisis-misplayed-belarus-russia-and-the-weaponisation-of-migration

Ravichandran, A. (2021). *The European NewSpace Ecosystem*. Medium. https://aravind-ravichan.medium.com/the-european-newspace-ecosystem-c5dec4f3b686

Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? . *Norwegian Institute for International Affairs (NUPI)*, *1*.

Reillon, Vincent. (2017). *European space policy : historical perspective, specific aspects and key challenges : in-depth analysis*. European Parliament.

Reis, J. C. G. dos. (2025). European Union's Space Security and Defense: Strategy Against Hybrid Threats. *Astropolitics*, *23*(1), 30–52. https://doi.org/10.1080/14777622.2025.2498474

Remuss, N.-L. (2009). Space and Internal Security - Developing a Concept for the Use of Space Assets to Assure a Secure Europe. *ESPI Report 20*. http://www.espi.or.atTel.:+4317181118-0Fax-99

Retter, L., Pezard, S., Flanagan, S., Germanovich, G., Clement, S. G., & Paille, P. (2021). *European Strategic Autonomy in Defence: Transatlantic visions and implications for NATO, US and EU relations*. www.rand.org/about/principles.

Roke. (n.d.). *Nord Stream: What We Know*. Retrieved 15 February 2026, from https://storymaps.arcgis.com/stories/2f82f339b8c14681b39eab649a4f9ac9

Roulette, J., & Taylor, M. (2024). *Exclusive: Musk's SpaceX is building spy satellite network for US intelligence agency, sources say*. Reuters. https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/

Rushton, S. (2021). *Satellite images reveal scale of migrants massed on Belarus-Poland border*. The National. https://www.thenationalnews.com/world/uk-news/2021/11/11/satellite-images-reveal-scale-of-migrants-massed-on-belarus-poland-border/

Safran. (n.d.). *Renseignement géospatial par IA*. Retrieved 13 February 2026, from https://www.safran-group.com/fr/produits-services/renseignement-geospatial-ia

Sagath, D., Papadimitriou, A., Adriaensen, M., & Giannopapa, C. (2018). Space strategy and governance of ESA small member states. *Acta Astronautica*, *142*, 112–120. https://doi.org/10.1016/J.ACTAASTRO.2017.09.029

Schroefl, J. (2022). Geospatial Information to Tackle Hybrid Threats. *Geospatial World Magazine*.

Shevchenko, V. (2014). 'Little green men' or 'Russian invaders'? *BBC Monitoring*. https://www.bbc.com/news/world-europe-26532154

Smid, H. H. F. (2022). *The Space Review: An analysis of Chinese remote sensing satellites*. The Space Review. https://www.thespacereview.com/article/4453/1

Space Daily. (2023). *New data platform to host Copernicus Earth observation datan data*. https://www.spacedaily.com/reports/New_data_platform_to_host_Copernicus_Earth_observation_data_999.html

Space Industry Database. (n.d.). *Space As A Service (SAAS) / Space Data As A Service (SDAAS)*. Retrieved 13 February 2026, from https://spaceindustrydatabase.com/directory/space-as-a-service

Space Strategy for Europe, Pub. L. COM/2016/0705 final (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478510570970&uri=CELEX:52016DC0705

Swope, C. (2024). *No place to hide: A look into China's geosynchronous surveillance capabilities*.

Taylor, P. (2022). *Running out of space: Addressing the growing threat of space debris*.

The Guardian. (2023). *Russian navy ship photographed near Nord Stream pipelines before blasts*. https://www.theguardian.com/world/2023/apr/28/russian-navy-vessel-seen-near-nord-stream-pipelines-days-before-blasts

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing Hybrid Threats. *Swedish Defence University*.

UK Ministry of Defence. (2023). Intelligence, Surveillance and Reconnaissance. *Joint Doctrine*.

UNIDIR. (2025). *Dual-Use - Terminology* . Outer Space Security Lexicon. https://spacesecuritylexicon.org/terminology/dual-use

Union of Concerned Scientists. (2023). *Satellite Database*. https://www.ucs.org/resources/satellite-database

Unseenlabs. (2024). *Unseenlabs Uncovers Threats to Subsea Cables*. LinkedIn. https://www.linkedin.com/pulse/unseenlabs-uncovers-threats-subsea-cables-unseenlabs-chfge/

USGS. (2025). *What is remote sensing and what is it used for?* . https://www.usgs.gov/faqs/what-remote-sensing-and-what-it-used

Van Camp, C., & Peeters, W. (2022). A World without Satellite Data as a Result of a Global Cyber-Attack. *Space Policy*, *59*. https://doi.org/10.1016/j.spacepol.2021.101458

Van, J. (2017). Tactics of Strategic Competition: Gray Zones, Redlines, and Conflict before War. *Naval War College Review*, *70*(3), 39–61. https://www.academia.edu/24643948/_Tactics_of_Strategic_Competition_Gray_Zones_Redlines_and_Conflict_before_War_Naval_War_College_Review

Vantor. (2025). *Maxar Launches Raptor, a First-of-its-Kind Software that Unlocks Next-Gen GPS Resilience for Autonomous Systems*. Maxar, Defense & Intelligence,

Press Releases, Commercial Technology. https://vantor.com/blog/maxar-launches-raptor-a-first-of-its-kind-software-that-unlocks-next-gen-gps-resilience-for-autonomous-systems/

Varma, T. (2024). European Strategic Autonomy: The Path to a Geopolitical Europe. *The Washington Quarterly*, *47*(1), 65–83. https://www.tandfonline.com/doi/pdf/10.1080/0163660X.2024.2327820

Veraverbeke, S., Harris, S., & Hook, S. (2011). Evaluating spectral indices for burned area discrimination using MODIS/ASTER (MASTER) airborne simulator data. *Remote Sensing of Environment*, *115*(10), 2702–2709. https://doi.org/10.1016/J.RSE.2011.06.010

Wang, Q., Tang, Y., Ge, Y., Xie, H., Tong, X., & Atkinson, P. M. (2023). A comprehensive review of spatial-temporal-spectral information reconstruction techniques. *Science of Remote Sensing*, *8*, 100102. https://doi.org/10.1016/J.SRS.2023.100102

Weeden, B., & Samson, V. (2023). *Global Counterspace Capabilities, An Open Source Assessment*.

Zancan, V., Paravano, A., Locatelli, G., & Trucco, P. (2024). Evolving governance in the space sector: From Legacy Space to New Space models. *Acta Astronautica*, *225*, 515–523. https://doi.org/10.1016/J.ACTAASTRO.2024.09.005

Zekulić, V., Godwin, C., & Cole, J. (2017). Reinvigorating Civil–Military Relationships in Building National Resilience. *RUSI Journal*, *162*(4), 30–38. https://doi.org/10.1080/03071847.2017.1380376

Annexes

Interview with Mathieu Bataille, ESPI and ESA

Semi-structured Interview conducted 12.02.2026 between Alexandre Touati (Interviewer) and Mathieu Bataille (Interviewee), DG Support and Member States Relations, Director General's Cabinet, European Space Agency.

The views and opinions expressed in this interview are those of the Interviewee and do not necessarily reflect the views of the European Space Agency.

Transcript generated via Zoom AI Companion translated from French

Interviewer: How would you characterize the current state of the European Earth observation market, particularly in relation to security and defence?

Mathieu Bataille: The war in Ukraine has significantly accelerated development opportunities for European Earth observation companies. A notable trend has been the strategic pivot of several firms from predominantly civilian applications toward military and security-oriented markets. Companies such as ICEYE and Constellr, the latter having raised €37 million, illustrate this transition. The conflict has provided armed forces with concrete operational evidence of the value of commercial satellite constellations. Commercial capabilities, particularly in synthetic aperture radar (SAR), have demonstrated their relevance for real-time intelligence and battlefield awareness. At the same time, there has been a marked expansion of the SAR market, alongside the emergence of new sensor modalities, including thermal imaging, hyperspectral sensors, and radiofrequency (RF) monitoring. These technologies broaden the range of detectable phenomena and enhance operational resilience. For example, Synspective is developing a second-generation system extending its focus from maritime to terrestrial monitoring. Overall, European Earth observation companies appear to have strong prospects in the security and defence sector, with sensor diversification becoming increasingly critical.

Interviewer: How can Earth observation contribute to addressing hybrid threats?

Mathieu Bataille: The usefulness of Earth observation varies depending on the nature of the threat. In the case of cyberattacks, its contribution is limited, as such threats primarily unfold within digital infrastructures. By contrast, Earth observation is highly relevant for detecting and monitoring physical sabotage, such as damage to pipelines

or submarine cables. The identification of “dark vessels” and suspicious maritime activities is particularly valuable in this regard. Persistent surveillance of manual sabotage operations remains constrained by current spatial and temporal resolution limits, although capabilities are progressively improving. In the domain of disinformation, satellite imagery can function as a verification and evidentiary tool. For example, imagery has been used to corroborate or refute claims concerning events in Malian villages.

Interviewer: There have also been cases of weaponized migration along the Polish and Finnish borders.
Mathieu Bataille: Indeed. Frontex integrates satellite data into its border management activities, demonstrating how Earth observation supports situational awareness and operational coordination in migration contexts.

Interviewer: What about the detection of jamming and spoofing activities, particularly in the Baltic region?
Mathieu Bataille: Innovative applications of SAR may allow for the detection of localized jamming activities, including around sensitive military installations such as missile defence bases. While Earth observation can reveal anomalies and support monitoring, attribution of intent remains challenging and requires complementary intelligence sources. More broadly, Earth observation tends to be more effective for situational management than for determining intent. Its utility is particularly high for sabotage monitoring, useful for migration management, valuable as evidentiary support in disinformation contexts, and comparatively limited in cyber domains.

Interviewer: What initiatives are underway to strengthen European strategic autonomy in Earth observation?
Mathieu Bataille: The Copernicus programme already includes a Security Service structured around three components: border surveillance, maritime surveillance, and support to external actions. Additionally, the Earth Observation Governmental Service (IOGS) is being developed to support Common Security and Defence Policy (CSDP) operations. The European Space Agency has proposed the Iris programme, European Resilience from Space, as a precursor to IOGS. Iris is structured around three pillars: Earth observation, satellite communications with contributions to Iris², and positioning,

navigation, and timing (PNT), including GNSS capabilities in low Earth orbit. The IRS-IO component envisions a system-of-systems architecture in orbit, designed to ensure rapid revisit rates and organized around multinational clusters. A central objective is to reduce dependence on U.S. institutional and commercial data sources. There is active cooperation between ESA and the European Union in developing a more autonomous European architecture, and several national and multinational clusters, including Atlantic and mountainous configurations, have already been validated.

Interviewer: From a capability standpoint, which dimension of resolution should be prioritized?

Mathieu Bataille: The principal challenge today concerns temporal resolution rather than spatial or spectral resolution. Operational users increasingly require updated information at intervals of 15 to 30 minutes. Europe already possesses a diverse array of sensors, including French optical systems, German and Italian radar satellites, and the Copernicus Sentinel constellation. French military satellites achieve spatial resolutions of approximately 30 centimeters or better. It remains an open question whether improving spatial resolution from 20 centimetres to 5 centimetres would produce proportionate operational benefits. Consequently, the priority lies in enhancing temporal resolution through the development of constellations, while spatial and spectral capabilities are already relatively advanced.

Interviewer: Could you elaborate on RF monitoring as an emerging technology?

Mathieu Bataille: RF monitoring was historically reserved for military powers such as the United States, Russia, China, and France. More recently, commercial actors such as HawkEye 360 in the United States and Unseenlabs in France have entered the field. Unseenlabs specializes primarily in maritime surveillance. RF monitoring provides a complementary observational capability that facilitates the detection of illicit or covert activities, particularly when vessels deactivate AIS transponders. However, the market is likely to remain limited and predominantly governmental rather than commercial. In a broader conceptualization, Earth observation should be defined inclusively, incorporating AIS and RF monitoring alongside optical and radar imagery.

Interviewer: What role does artificial intelligence play in Earth observation systems?

Mathieu Bataille: One major application of artificial intelligence lies in onboard data processing to reduce unnecessary data transmission. ESA's PhiSat-1 and PhiSat-2 missions illustrate the implementation of embedded image processing capabilities. For example, automatic cloud detection enables optical satellites to discard unusable images before downlink, thereby optimizing bandwidth and processing efficiency. Artificial intelligence also supports digital twin applications and advanced modelling. Upstream, AI contributes to the optimization of industrial processes across satellite manufacturing and operations. Although European space investments have declined since 2022 relative to AI-focused sectors, the integration of AI into space systems reflects convergence rather than competition, with AI progressively embedded across Earth observation architectures.

Interview with Valentin Golovtchenko, World Economic Forum

Semi-structured Interview conducted 17.02.2026 between **Alexandre Touati** (Interviewer) **and Valentin Golovtchenko** (Interviewee), Lead, Planetary Solutions Strategy, C4IR Physical Technologies, World Economic Forum.

The views and opinions expressed in this interview are those of the Interviewee and do not necessarily reflect the views of the World Economic Forum.

Transcript generated via Zoom AI Companion translated from French

Interviewer: How would you characterize the current state of the European Earth observation market, particularly in terms of spatial, temporal, and spectral resolutions?

Valentin Golovtchenko: The European Earth observation market is undergoing a significant transformation, marked by a renewed emphasis on governmental applications. Prior to the 2024 U.S. presidential election, the prevailing trend favoured an increase in private operators serving commercial clients in sectors such as insurance, agriculture, and supply chain management.

As of early 2026, the defining feature of the market is "dual use." Numerous European start-ups that initially focused on private environmental applications are now securing multi-billion-euro contracts with the European Commission and Member States for defence and intelligence purposes.

This shift is largely driven by the release of substantial defence budgets across Europe, particularly in Germany, which has undertaken a major strategic reorientation. In

addition, European sovereignty has become a central criterion in public procurement procedures. This development strengthens the competitive position of European operators relative to established U.S. actors such as Planet and Maxar.

Airbus Defence and Space remains a major European incumbent; however, the broader ecosystem is expanding as European preference policies are increasingly implemented in procurement processes.

Interviewer: How would you assess the technological trajectory of the sector?

Valentin Golovtchenko: Technological development is progressing in a steady and incremental manner rather than through disruptive breakthroughs. Temporal resolution continues to improve due to the growing number of satellites deployed in orbit, enabling more frequent revisit times.

Spatial resolution is also advancing as a result of continuous improvements in sensor technologies. Overall, technological evolution in the sector is gradual and cumulative rather than transformative.

Interviewer: Could you categorize the types of applications currently sought in dual-use calls for tenders?

Valentin Golovtchenko: My expertise is primarily focused on commercial and environmental applications within the private sector. Nevertheless, demand increasingly extends beyond the optical spectrum. While Europe possesses strong capabilities in optical imagery, current investments are not concentrated exclusively in this domain.

Alternative sensing modalities are gaining prominence, including multispectral, hyperspectral, radio frequency (RF), synthetic aperture radar (SAR), and thermal imaging technologies.

For example, the German company Constellr specializes in thermal imaging. It was initially established to address agricultural and urban planning use cases, such as detecting heat islands and areas experiencing water stress. The company has since secured significant contracts with the German military. Thermal imaging enables nighttime detection, identification of vessels in territorial waters even when tracking systems are deactivated, and detection of moving vehicles in conflict zones.

The company's leadership strategically positioned its technology to access defence markets while continuing to serve environmental applications. This illustrates how dual-use positioning enables companies to diversify revenue streams between environmental and security-related activities.

Interviewer: What is your assessment of the "Space as a Service" model and its implications?

Valentin Golovtchenko: "Space as a Service," often referred to as "Insight as a Service," consists of commercializing processed information derived from satellite imagery, typically through subscription-based models, rather than selling raw images.

Two principal categories of companies operate in this domain: vertically integrated firms that own and operate satellites alongside proprietary software platforms, and aggregators that compile data from multiple providers.

However, this model has not expanded as anticipated. The market remains largely dominated by direct image sales. One reason is incompatibility with governmental requirements for exclusivity. Governments are willing to pay premium prices for exclusive access to specific imagery, which conflicts with subscription-based distribution models.

A second challenge concerns pricing structures. Satellite imagery is generally required on a targeted and immediate basis rather than continuously, as is the case for cloud-based services. The concept of tasking, namely directing a satellite to capture imagery at a specific time and location, is central. Because users require precise and timely information, payment per task is often more appropriate than subscription-based pricing. As the proportion of revenues derived from governmental clients increases, the feasibility of the "as a service" model becomes more limited.

Interviewer: How can Earth observation capabilities address hybrid and non-kinetic threats such as GNSS jamming and spoofing?

Valentin Golovtchenko: Hybrid threats include non-kinetic actions such as GNSS jamming and spoofing, particularly along Europe's eastern borders. Optical sensors are not well suited to detecting such threats. More advanced technologies, especially RF sensing, are required. Applications for detecting jamming and spoofing signals are already available.

Hybrid threats also encompass disinformation campaigns and broader destabilization efforts. An emerging area of concern involves threats in orbit. Several nations possess capabilities to disrupt or potentially destroy rival space assets. This raises the possibility of a large-scale cyberattack in space and its implications for trust in space-based infrastructure.

Currently, satellite imagery and GNSS signals are widely regarded as reliable and difficult to falsify. Ensuring the resilience and cybersecurity of space systems will therefore become increasingly important.

Interviewer: What is your perspective on the convergence between artificial intelligence, quantum technologies, and space systems?

Valentin Golovtchenko: Edge computing is increasingly deployed in orbit, enabling onboard data processing and reducing the need for systematic data downlinks. Embedded artificial intelligence allows satellites to transmit only relevant information, thereby improving efficiency and lowering costs.

Quantum technologies are particularly relevant for encryption and may be integrated into orbital hardware to enhance secure communications. Although I am not a specialist in quantum technologies, their potential applications in cryptography are significant.

On the ground segment, artificial intelligence plays a crucial role in information processing, including pattern recognition and automation of previously manual analytical tasks. A particularly transformative development concerns user interaction through natural language processing and large language models.

An emerging field, often referred to as GeoAI, enables users to interact with historical imagery datasets, digital twins, or near-real-time imagery through natural language queries. This development has the potential to fundamentally simplify access to and interaction with satellite imagery.

Interviewer: How do you assess initiatives such as the Copernicus Contributing Missions within a fragmented European market?

Valentin Golovtchenko: Such initiatives are essential for building competitive capabilities. Europe cannot rely exclusively on large national prime contractors; private sector participation is necessary. A broader ecosystem increases the number of actors

contributing to innovation and enables access to non-strategic capabilities without direct public investment.

Most importantly, European governments face high levels of sovereign debt and constrained fiscal capacity. The private sector can therefore complement public efforts, particularly where governments lack the resources to deploy constellations independently. Public-private partnerships are essential for achieving sovereign and competitive Earth observation capabilities.

For example, thermal imaging capabilities at resolutions comparable to those provided by Constellr are not currently available within the core Copernicus satellites. By participating as a Contributing Mission, Constellr fills this technological gap.

Regarding transatlantic considerations, integrating U.S. companies into European sovereign capability frameworks may conflict with strategic autonomy objectives. Strengthening collaboration with European private companies is therefore crucial for developing a robust European New Space ecosystem. Europe possesses strong talent, established space agencies, and advanced training programs. Supporting European companies through public procurement and governmental contracts is necessary to consolidate and expand capabilities within Europe.

Data on European EO capabilities

Database Information

Compilation: Geosat Database & UCS Satellite Database (merged)
Source: European Space Agency (ESA), EUMETSAT, National Space Agencies, eoPortal, NY20,
Last Update: 15.févr.25
Total Satellites: 130 active European EO satellites

Geographic Coverage: Europe (ESA, EUMETSAT, individual nations)
Data Types: Optical, Radar, Multispectral, Hyperspectral, Meteorology

Mission Type Breakdown

- Earth Science: 41 satellites
- Optical Imaging: 24 satellites
- Radar Imaging (SAR): 33 satellites
- Meteorology: 9 satellites
- AIS/Maritime: 33 satellites
- Intelligence/Military: 11 satellites
- Other/Specialized :9 satellites

Important Notes

- Spatial Resolution: Measured in meters (m). Lower values = higher detail. Range: 0.2m to 170km
- Temporal Resolution: Revisit time in days. How often satellite can image same location.
- Spectral Bands: Wavelengths captured (UV, Visible, IR, Microwave, Radar frequencies)

Name of Satellite, Alternate Names	Country/Org of UN Registry	Users	Detailed Purpose	Class of Orbit	Type of Orbit	Spatial Resolution	Temporal Resolution	Spectral resolution
PVCC	Belgium	Commercial	Optical Imaging	LEO	Sun-Synchronous	100.0	1.0	Blue | Cyan | Visible | Viol
AAt-4	Denmark	Civil	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
GomX-4A	Denmark	Military		LEO	Sun-Synchronous			
Sternula-1	Denmark	Commercial	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
Aeolus	ESA	Government	Earth Science	LEO				
Cryosat-2	ESA	Government	Radar Imaging	LEO	Polar	250.0 | 5000.0	30.0	Microwave | Ku-Band
ESEO (European Student Earth Orbite	ESA	Civil		LEO	Sun-Synchronous			
PROBA-1	ESA	Government	Earth Science	LEO	Sun-Synchronous	8.0 | 18.0		Visible | Violet | Red | Near
PROBA-2	ESA	Government	Earth Science	LEO	Sun-Synchronous	2200000.0	0.00069444444	Ultraviolet
PROBA-3 OSC	ESA	Government	Earth Science	LEO	Sun-Synchronous			
Proba 5 (Project for On-Board Autono	ESA	Government	Earth Science	LEO	Sun-Synchronous	100.0	1.0	Blue | Cyan | Visible | Viol
Sentinel 1A	ESA	Government	Earth Science	LEO	Sun-Synchronous	4.0	5.0	Microwave | C-Band
Sentinel 1C	ESA	Government	Earth Science	LEO	Sun-Synchronous	1.0 | 4.0	5.0	Microwave | C-Band
Sentinel 2A	ESA	Government	Earth Science	LEO	Sun-Synchronous	10.0	5.0	Blue | Visible | Violet | Nea
Sentinel 2B	ESA	Government	Earth Science	LEO	Sun-Synchronous	10.0	5.0	Blue | Visible | Violet | Nea
Sentinel 2C	ESA	Government	Earth Science	LEO	Sun-Synchronous	10.0	5.0	Blue | Visible | Violet | Nea
Sentinel 3A	ESA	Government	Earth Science	LEO	Sun-Synchronous	300.0 | 20000.0 | 150.0 | 5000.0	10.0	Microwave | C-Band | Ku-I
Sentinel 3B	ESA	Government	Earth Science	LEO	Sun-Synchronous	300.0 | 20000.0 | 150.0 | 5000.0	10.0	Microwave | C-Band | Ku-I
Sentinel 5P (Sentinel 5 Precursor)	ESA	Government	Earth Science	LEO	Sun-Synchronous	3500.0	16.0	Ultraviolet | Visible | Violet
Sentinel 6	ESA	Government	Earth Science	LEO	Sun-Synchronous	25000.0 | 150.0 | 5000.0 | 3000.0	30.0 | 10.0	Microwave | K-Band | Ka-I
SMOS (Soil Moisture and Ocean Salini	ESA	Government	Earth Science	LEO	Sun-Synchronous	150.0 | 50000.0	3.0	Microwave | L-Band
SWARM-A	ESA	Government	Earth Science	LEO	Polar			
SWARM-B	ESA	Government	Earth Science	LEO	Polar			
SWARM-C	ESA	Government	Earth Science	LEO	Polar	150.0		
EARTHCARE	ESA	Government	Earth Science	LEO	Polar	500.0	16.0	Visible | Red | Near infrare
EDRS-C	ESA	Government	Earth Science	LEO	Polar			
Meteosat 10 (MSGalaxy-3,MSG 3)	EUMETSAT	Government/Civil	Earth Science/Meterology	GEO		39300.0 | 1000.0	0.01	Blue | Cyan | Green | Visib
Meteosat 11 (MSG 4)	EUMETSAT	Government/Civil	Earth Science/Meterology	GEO		39300.0 | 1000.0	0.01	Blue | Cyan | Green | Visib
Meteosat-12 (MTG-I1)	EUMETSAT	Government/Civil	Earth Science/Meterology	GEO		4500.0	0.006944444444444444	Near infrared | Blue | Visib
Meteosat 9 (MSGalaxy-2, MSG 2)	EUMETSAT	Government/Civil	Earth Science/Meterology	GEO		39300.0 | 1000.0	0.01	Blue | Cyan | Green | Visib
MetOp-B (Meteorological Operational	EUMETSAT	Government/Civil	Earth Science/Meterology	LEO	Sun-Synchronous	16000.0 | 150.0 | 12000.0 | 1090	0.5 | 1.5 | 29.0	W-Band | Thermal infrare
MetOp-C (Meteorological Operational	EUMETSAT	Government/Civil	Earth Science/Meterology	LEO	Sun-Synchronous	16000.0 | 150.0 | 12000.0 | 1090	0.5 | 1.5 | 29.0	W-Band | Thermal infrare
Meteosat 8 (MSGalaxy-1, MSG-1)	EUMETSAT/ESA	Government/Civil	Earth Science/Meterology	GEO				
ICEYE-X1 (ICEYE POC 1, XR1)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	10.0 | 3.0	20.0	Microwave | X-Band
ICEYE-X10 (ICEYE POC 10, XR1)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X11 (ICEYE POC 11, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X12 (ICEYE POC 12, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X13 (ICEYE POC 13, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X14 (ICEYE POC 14, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X15 (ICEYE POC 15, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X16 (ICEYE POC 16, XR1)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	0.5 | 1.0	1.0	Microwave | X-Band
ICEYE-X2 (ICEYE POC 2)	Finland	Commercial	Radar Imaging (SAR)	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X21	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	0.5 | 3.0	14.0	Microwave | X-Band
ICEYE-X27	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	0.5 | 3.0	14.0	Microwave | X-Band
ICEYE-X4 (ICEYE POC 4)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X5 (ICEYE POC 5)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X6 (ICEYE POC 6)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X7 (ICEYE POC 7)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X8 (ICEYE POC 8)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
ICEYE-X9 (ICEYE POC 9)	Finland	Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0 | 3.0	30.0	Microwave | X-Band
BRO-1	France	Commercial	Maritime Surveillance	LEO	Non-Polar Inclined	1000.0	0.125	Radio frequency | X-Band
BRO-2	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-3	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-4	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-6	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-7	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-8	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
BRO-9	France	Commercial	Maritime Surveillance	LEO	Sun-Synchronous	1000.0	0.125	Radio frequency | X-Band
CERES 1 (CapacitÉ de Renseignemen	France	Military	Electronic Intelligence	LEO	Polar	1.0	1.0	Microwave | X-Band
CERES 2 (CapacitÉ de Renseignemen	France	Military	Electronic Intelligence	LEO	Polar	1.0	1.1	Microwave | X-Band
CERES 3 (CapacitÉ de Renseignemen	France	Military	Electronic Intelligence	LEO	Polar	1.0	1.2	Microwave | X-Band
CSO-1 (Optical Space Component-1)	France	Military	Multispectral Imaging	LEO	Sun-Synchronous	0.2	1.0	Blue | Cyan | Green | Visib
CSO-2 (Optical Space Component-2)	France	Military	Multispectral Imaging	LEO	Sun-Synchronous	0.35	1.0	Blue | Cyan | Green | Visib
Pléiades HR1B	France	Commercial	Optical Imaging	LEO	Sun-Synchronous	0.7	1.0	Blue | Cyan | Green | Visib
Spot 6 (Système Probatoire d'Observ	France	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.5	1.0	Blue | Cyan | Green | Visib
Spot 7 (Système Probatoire d'Observ	France	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.5	1.0	Blue | Cyan | Green | Visib
Pléiades HR1A	France	Government	Optical Imaging	LEO	Sun-Synchronous	0.7	1.0	Blue | Cyan | Green | Visib
Pléiades Neo 3	France	Government	Optical Imaging	LEO	Sun-Synchronous	0.3	0.5	Visible | Violet | Blue | Cya
Pléiades Neo 4	France	Government	Optical Imaging	LEO	Sun-Synchronous	0.3	0.5	Visible | Violet | Blue | Cya
Helios 2B	France	Military	Optical Imaging	LEO	Sun-Synchronous			
UVSQ-SAT NG	France					2000.0		Near infrared | Short-wave
ENMAP	Germany					30.0		Blue | Cyan | Green | Visib
Bird 2 (Bispectral InfraRed Detector 2	Germany	Government/Civil	Optical Imaging	LEO	Sun-Synchronous	25.0		Blue | Cyan | Green | Visib
BIROS (Bispectral Infrared Optical Sys	Germany	Government	Optical Imaging	LEO	Sun-Synchronous	0.5		Blue | Cyan | Green | Visib
FLP (Flying Laptop)	Germany	Civil	Automatic Identification System (AIS)	LEO	Sun-Synchronous	0.5		
SAR-Lupe 1	Germany	Military	Radar Imaging	LEO	Non-Polar Inclined	0.5		Microwave | X-Band
SAR-Lupe 2	Germany	Military	Radar Imaging	LEO	Non-Polar Inclined	0.5		Microwave | X-Band
SAR-Lupe 3	Germany	Military	Radar Imaging	LEO	Non-Polar Inclined	0.5		Microwave | X-Band
SAR-Lupe 4	Germany	Military	Radar Imaging	LEO	Non-Polar Inclined	0.5		Microwave | X-Band
SAR-Lupe 5	Germany	Military	Radar Imaging	LEO	Non-Polar Inclined	0.5		Microwave | X-Band
TanDEM-X (TerraSAR-X add-on for Di	Germany	Government	Radar Imaging	LEO	Sun-Synchronous	1.0	2.5	Microwave | X-Band
TerraSAR-X 1 (Terra Synthetic Apertu	Germany	Government/Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0	2.5	Microwave | X-Band
COSMO-Skymed 1 (Constellation of si	Italy	Military/Civil	Radar Imaging	LEO	Sun-Synchronous	1.0	14.0	Microwave | X-Band
COSMO-Skymed 2 (Constellation of si	Italy	Military/Government	Radar Imaging	LEO	Sun-Synchronous	1.0	14.0	Microwave | X-Band
COSMO-Skymed 3 (Constellation of si	Italy	Military/Government	Radar Imaging	LEO	Sun-Synchronous	1.0	14.0	Microwave | X-Band
COSMO-Skymed 4 (Constellation of si	Italy	Military/Government	Radar Imaging	LEO	Sun-Synchronous	1.0	14.0	Microwave | X-Band
CSG-1 (COSMO-SkyMed Second Gen	Italy	Military/Government	Radar Imaging	LEO	Sun-Synchronous	0.35	1.5	Microwave | X-Band
CSG-2 (COSMO-SkyMed Second Gen	Italy	Military/Government	Radar Imaging	LEO	Sun-Synchronous	0.35	1.5	Microwave | X-Band
Optsat-3000	Italy	Military	Optical Imaging	LEO	Sun-Synchronous			
PRISMA (PRecursore IperSpettrale de	Italy	Government	Hyperspectral Imaging	LEO	Sun-Synchronous	10.0 | 5.0		Blue | Cyan | Green | Visib
D2/AtlaCom-1	Lithuania	Government	Optical Imaging	LEO	Sun-Synchronous	16.0	30.0	Microwave | C-Band | Ku-I
Lemur-2 Disclaimer (Lemur FM165)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Emmaculate (Lemur FM164)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 FuenteTaja-01 (FM169)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Mmolo (Lemur FM167)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 PhilAri (Lemur FM166)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 SteveAlbers (Lemur FM168)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 ChristinaHolt (Lemur 2F90)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 DaisyHarper (Lemur 2F95)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Djara	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Non-Polar Inclined	1000.0	0.0104	
Lemur-2 Elham (Lemur 2FM99)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Gustavo (Lemur 2F89)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 RemyColton (Lemur 2F88)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 SarahBettyBoo (Lemur 2F93	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Slicers (Lemur 2FM121)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 Susurrus (Lemur 2FM120)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Lemur-2 TinyKev (Lemur 2F92)	Luxembourg	Commercial	Meteorology, Automatic Identification System (AIS)	LEO	Sun-Synchronous	1000.0	0.0104	
Brik-II	Netherlands	Government	Signals Intelligence	LEO	Non-Polar Inclined			
Arctic Weather Satellite	Norway	Government	Earth Science			10000.0	0.20833333333333334	V-Band
NorSat-1	Norway	Government	Automatic Identification System (AIS)	LEO	Sun-Synchronous	1.0 | 1000		
NorSat-2	Norway	Government	Automatic Identification System (AIS)	LEO	Sun-Synchronous	1.0 | 1000		
NorSat-3	Norway	Government	Automatic Identification System (AIS)	LEO	Sun-Synchronous	10000.0		
NorSat-4	Norway	Government	Automatic Identification System (AIS)	LEO	Sun-Synchronous	10.0		
NorSat-TD	Norway	Government	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
FSSCAT-A	Spain	Government	Earth Science	LEO	Sun-Synchronous			
FSSCAT-B	Spain	Government	Earth Science	LEO	Sun-Synchronous			
AISTechSat-2	Spain	Commercial	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
AISTechSat-3	Spain	Commercial	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
Deimos 1	Spain	Government	Optical Imaging	LEO	Sun-Synchronous	22.0	3.0	Green | Visible | Orange |
Deimos 2	Spain	Government	Optical Imaging	LEO	Sun-Synchronous	1.0	4.0	Blue | Cyan | Green | Visib
Paz	Spain	Military/Commercial	Radar Imaging	LEO	Sun-Synchronous	1.0		Microwave | X-Band
Mats	Sweden	Government	Earth Science	LEO	Sun-Synchronous	200.0		Ultraviolet | Near infrared
Odin	Sweden	Government	Earth Science	LEO	Sun-Synchronous	1000.0 | 1500.0	3.0	Blue | Cyan | Green | Visib
AAC AIS-Sat1 (Kelpie 1)	United Kingdom	Commercial	Automatic Identification System (AIS)	LEO	Sun-Synchronous			
DMC 3-1 (Disaster Monitoring Constel	United Kingdom	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.0		Blue | Cyan | Green | Visib
DMC 3-2 (Disaster Monitoring Constel	United Kingdom	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.0		Blue | Cyan | Green | Visib
DMC 3-3 (Disaster Monitoring Constel	United Kingdom	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.0		Blue | Cyan | Green | Visib
NovaSAR-1	United Kingdom	Government/Commercial	Radar Imaging	LEO	Sun-Synchronous	6.0	365.0	Microwave | S-Band
SSTL-S1-4	United Kingdom	Commercial	Optical Imaging	LEO	Sun-Synchronous	1.0		Blue | Cyan | Green | Visib
UK-DMC-2 (BNSCSat-2, British Nation	United Kingdom	Government	Optical Imaging	LEO	Sun-Synchronous	22.0	3.0	Green | Visible | Orange |