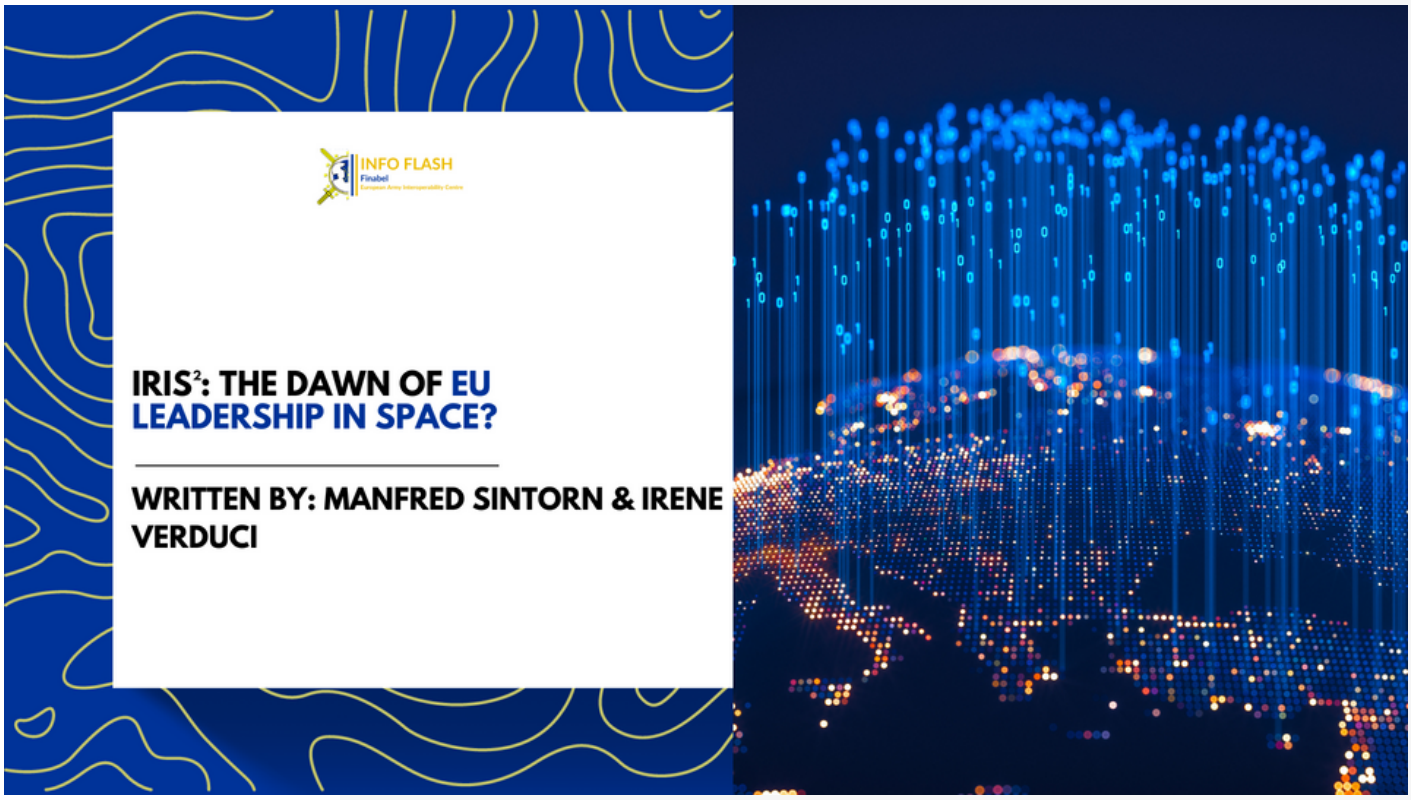
INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

DECEMBER 2023



WRITTEN BY

MANFRED SINTORN & IRENE VERDUCI

EDITED BY

CLELIA VETTORI

SUPERVISED BY

EMILE CLARKE

Introduction

As great power politics returns to the world stage, so does space policy. States that can afford to are funnelling money into their space programmes in pursuit of everything from space-based weaponry to technological development, research, and communications. The European Union, in a bid to become the leading space actor, has also launched a flurry of projects and established both an operational agency and a specialised directorate-general for its space policy. One of the many lessons from the war in Ukraine is the importance of resilient and secure satellite internet during times of crisis. In setting up such a capability, the EU is establishing the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), which will be fully operational by 2027 (Regulation 2023/588).

IRIS² aims to develop a reliable satellite-based internet system for European, invited, and allied use. The intent is to cover the EU, its delegations, member state embassies, and strategic areas for both civilian and military applications. In a context where the only existing alternative, Starlink, is privately owned, US-based, and has restricted the connection for a Ukrainian drone strike after its CEO was contacted by Russian officials (Brunnstrom, Landay, Stewart & Popeski, 2023), IRIS²'s necessity cannot be overstated. Recent experiences such as the suspected sabotage of undersea cables in the Gulf of Finland show that the EU's telecommunications infrastructure is vulnerable to hybrid attacks, stressing the need for alternative networks (Kauranen & Solsvik, 2023). IRIS²'s ramifications for strategic autonomy, redundancy in communications and military capacity are all significant (European Commission, 2023a). Further, in establishing the first publicly controlled satellite service of its kind, the EU is seeking a leading role in space technology and policy (European Commission, 2023a).

Therefore, it is worthwhile to review what IRIS² will accomplish and how it will function. With this aim, the paper analyses IRIS² in relation to its context, functioning, launch, control structure, necessity, applications, and implications for European security. After providing a general background on EU space strategy, attention will be devoted to the context of the war in Ukraine and the lessons learned in how space-based internet affects modern warfare.

The EU's Space Strategy

Space policy has always been an interest of the European Union, but cooperation has mainly been driven by single member states and has also been rather inconsistent, as continuous supranational elements are a recent addition. Because the space domain is an important enabler for EU strategic autonomy, the space realm has grown increasingly relevant (Cellerino, 2023). As per Article 4 of Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the Union, the aerospace sector has long been considered strategic, motivating a decision to designate foreign investments into the sector as a possible risk to security and public order. In the same vein, Directive 2022/2557 on the resilience of critical entities classifies space service operators as critical entities.

Acknowledging the importance of space as a critical asset for societal needs, the EU has, and is, trying to secure its own space infrastructure. The growing space-related private sector is a considerable commercial opportunity while the Union's freedom of action in this domain is dependent on its ability to achieve safe, secure, and autonomous access to space (Celerino, 2023). It is also worth noting that the space sector is essential for a wide range of policies and aims that are not limited to security and defence, such as for GPS and satellite imagery. Further, the space sector is becoming increasingly congested, which in tandem with increased global attention to space creates a clear need to act fast (European Commission, 2022).

Aware of both needs and advantages, the EU is structuring a space policy with tools capable of addressing its security, defence, public, and commercial interests. This task becomes more complex as the Union has to address certain specific matters, such as the role of the European Space Agency [ESA] in what is seemingly becoming an EU competency. The prime example of member state cooperation in space is ESA, which is not an EU structure, has non-EU participants and is mainly concerned with ensuring steady public investments in the space sector and providing technical expertise for its members' space programmes. While security and defence are exclusive member state competencies under Article 4(2) TEU, space policy is not. Hence, EU space policy has traditionally been considered a supranational EU competency and, even as it is entangled with defence, it has usually been placed among TFEU competencies, eventually falling under civil control (Reillon, 2017).

Since the 1980s, space policy has been an EU interest. As the Union did not have the technical capacity to carry out programmes on its own, it collaborated with ESA in establishing, for instance, the Copernicus and Galileo programmes, among others. Non-EU participation in ESA poses issues in regard to sensitive information since ESA, along with all its members, has complete access to all data and is also the only actor with the technical capabilities necessary to operate the programmes (Celerino, 2023). In addressing this issue, the Council and the Commission acted to adapt ESA to European security requirements and allow the Union to fully pursue its needs. This eventually resulted in the 2011 administrative agreement between ESA and the European Defence Agency [EDA], allowing the Union to develop a full range of space capabilities together with ESA (Oikonomou, 2012). Recently, the EU has further developed its capacity to handle space-related matters through the launch of the Directorate-General for Defence Industry and Space [DG DEFIS] and the EU Agency for the Space Programme [EUSPA].

In this context, the EU has developed two space capabilities with notable strategic implications: Space Situational Awareness [SSA] and Governmental Satellite Communication [GOVSATCOM]. The former aims to network national Space Surveillance and Tracking assets monitoring space debris, while the latter aims to provide EU institutions and member states' authorities with resilient and robust governmental satellite communications capacities (Celerino, 2023).

With a view directed towards internalization and the pursuit of strategic autonomy, the EU has increasingly allocated more political and security aspects on EUSPA's shoulders while establishing the EU Space Programme to enhance the Union's space components (Celerino, 2023). This has recently led to the launch of several new initiatives, including IRIS², which the following section deals with in depth.

IThe Avant-garde IRIS² and its Advantages

IRIS² is to be a multiorbital internet connectivity network of satellites. Demystified, this means an extensive network of satellites in different orbits that provide continuous low-latency satellite internet coverage worldwide (European Commission, 2023b). The concept is not new and is currently commercially available, albeit not using multi-orbital satellites and with other slight differences (Starlink, 2023). The system is intended to merge public, private, and defence interests by ensuring that the infrastructure is available to all actors.

From a defence perspective, the main benefit is to allow for satellite internet communication, which is highly versatile, difficult to trace, and comparatively hard to disrupt (Kim, Pérez-Peña & Kramer, 2023; Khurana et al., 2023). A unique benefit for satellite communications is that the signal is difficult to jam, even in the case of Starlink, which is a civilian product with no intended protection against jamming (Withington, 2023). Additionally, if the latency is low enough and the communication is hard enough to trace, it also allows drone operators to work far from the front regardless of whether the operating side has air superiority. As for public interests, the main benefit is for the satellite network to provide redundancy should standard internet infrastructure be disabled by deliberate action or catastrophe (European Commission, 2023a). Further, it would provide internet access to operations in areas where internet infrastructure is unreliable, as well as provide more secure and stable internet access to EU delegations and member state embassies (European Commission, 2023a). Lastly, the private interests raised refer to the provision of mass-market broadband access and communications systems for long-range commercial transport (European Union, 2023).

The project appears to heed lessons learned from the Russo-Ukrainian war, where the destruction and sabotage of physical infrastructure has forced essential services, citizens, and armed forces to switch to space-based internet (Kim, Pérez-Peña & Kramer, 2023). The conflict has shown that this is both feasible and a boon for resilience but has also drawn attention to the need for political ownership of the system. This is because, as mentioned earlier, a lack of viable alternatives to Starlink has left Ukraine beholden to private interests which have already led to service restrictions due to the company's CEO being pressured by the Russian government (Brunnstrom, Landay, Stewart & Popeski, 2023). The satellite system's vulnerabilities and resilience in a state of war vis-à-vis a space-capable state actor will be expanded in the subsequent section.

Recent experiences, such as the suspected sabotage of undersea cables in the Gulf of Finland (Kauranen & Solsvik, 2023), have shown that the EU's internet infrastructure is susceptible to hybrid attacks, stressing the need for EU action. As for the system's security, it is powered by a quantum key distribution system developed through EuroQCI, which is a sub-project of IRIS². The system uses quantum mechanics to create and transmit encryption keys that cannot be intercepted without being changed, as observing the photons en route alters their properties (European Commission, 2023c). The encryption keys are thereby distributed in a way that makes eavesdropping render the key invalid and alerts the receiver of the interception (European Commission, 2023c).

Resilient, Secure, Vulnerable?

While space systems are lauded as highly resilient, they have vulnerabilities that malignant or disruptive actors can exploit. Given the strategic relevance of space, some states already have and are developing counter-space asset arsenals that can disrupt, degrade or destroy space-based systems to disable the enemy's space-based capabilities (Harrison et al., 2022). As stated in the Combined Space Operations Vision 2031, which guides US, UK, Canadian, New Zealander, Australian, French, and German collaborative space operations, threats derive from "the lack of widely accepted norms of responsible behaviour" and historical practice that "increases the possibility of misperceptions and the risks of escalation" (Combined Space Operations, 2022, p. 1).

Physical anti-space weapons can be divided into kinetic and non-kinetic categories. Kinetic weapons, such as bullets and missiles, cause physical damage and are aimed at permanently disabling either ground stations or satellites in orbit (Harrison et al., 2022). Non-kinetic weapons damage the satellite or ground system without making physical contact, disabling them by blinding sensors, overheating components with lasers or using high-powered microwave or nuclear weapons to disrupt or even destroy systems (Harrison et al., 2022). While the former are generally visible and comparatively attributable, this is not necessarily true for the latter, which might also leave attackers unaware of their actions' efficacy.

Furthermore, there are two vectors of attack whose primary foci are not to cause physical damage but to electronically – and often temporarily – disable systems instead. The first is electronic weaponry, which disrupts radio signals used by space-based systems; this includes jamming and spoofing, which are both reversible and relatively easy to carry out (Harrison et al., 2022). Electronic attacks can also be difficult to detect and trace, which makes attribution and situational awareness challenging (Harrison et al., 2022). The second vector is cyber-attacks, which do not target signals but the software or data themselves. Targets for cyber operations include everything from space-based assets to ground stations, equipment, and command structures. Cyber-attacks can be carried out by a wide range of actors, such as firms, individuals, or states. Unique to cyber-attacks is that they are virtually free bar personnel and education costs and that vulnerabilities to these attacks are difficult to predict (Harrison et al., 2022). For example, Ukraine's wartime satellite internet was originally provided by Viasat, which was disrupted to the point of inoperability by cyber-attacks launched in tandem with the onset of the full-scale invasion (Khurana et al., 2023). The replacing service, Starlink, has not faced any considerable service disruptions, notwithstanding the self-inflicted interruptions of service over Russian-occupied territory (Srivastava, Olearchyk & Schwartz, 2022). Lastly, cyber-attacks are often deniable and rarely clearly attributable: even when an attack is traced, it can be difficult to ascertain whether it was state-sponsored

Conclusion

In evaluating IRIS² in the context of the EU's space policy, this paper finds that IRIS² addresses gaps in capability, strengthens European autonomy, and is both ambitious and going well. Notwithstanding, there are several issues concerning the capability which will be dealt with below.

The system is a breath of fresh air for military use: jointly controlled, not beholden to private interests, and secure. There are, however, two possible issues. The first is that EU ownership reduces certainty in the consequences of an attack on the system. An attack on a single state's military communications satellite is an act of war, but this is not necessarily clear when it is an EU satellite that is attacked. This uncertainty raises risks, as the hostile actor might under- or overestimate the response, which could have disastrous consequences. While the EU has a defined strategy for threats to EU space assets, actions taken are beholden to a unanimous council decision (Council of the European Union, 2021). This approach does not seem ideal considering the issues of reaching unanimous decisions in foreign policy without reducing them to the lowest common denominator (Biscop, 2019).

The second issue is that placing military communications infrastructure in space is, in effect, militarising space. This incentivises rivals to develop anti-satellite capabilities, which in turn further militarises space. However, the thinking here is abundantly clear: "The EU is committed to preventing such an arms race and has been actively advocating for reducing space threats through norms, rules, and principles of responsible behaviours. At the same time, the EU has to cope with new security challenges, including in the space domain" (European Commission, n.d.). In other words, the Union prefers a demilitarised space domain but is faced with the reality of that not being the case.

As for commercial interests and how widespread usage of the system will be, some things remain less than obvious. While the mass-market component is evident (European Union, 2023), it is generally unclear how it would work and whether the EU would now become an internet service provider. The same questions reign when it comes to uptake as, although the system has far-reaching benefits, states have no obligation to use the system and might sectorally opt-out, for instance, if they want to retain control of their communications systems. In the same vein, questions arise about whether NATO forces can seamlessly adopt an EU-developed military communications system shared with non-members.

These issues are however far from insolvable. Strategic uncertainty can be reduced by a simple declaration from member states stating exactly how they would treat an attack on EU satellites and space infrastructure. Similarly, the mass-market component can be addressed by deciding the format in which it would occur, and the uptake can be foreseen by member states creating adaptation and implementation plans for the system as a redundancy. In gauging interest in its space policy, the EU has, in fact, been proactive. The most notable instance of this is the establishment of the EU Space Information Sharing and Analysis Centre (ISAC), a network of public entities and private enterprises with different backgrounds designed to strengthen and improve the security and resilience of the project's Members. In this context, the importance of Small and Medium Enterprises (SMEs) and start-ups has been particularly stressed, along with the benefits that could be derived (European Commission, 2023d).

The Centre's success will be reliant on how well it organises collaboration on cybersecurity, information sharing, and providing access to experts. It is still unclear, though, to what extent this network could generate economic benefits and who would receive said benefits. Regardless, with IRIS² the EU is making inroads to establish itself as a world leader in space policy, even surpassing the capabilities of all other actors. No matter how the project continues, its ambition is no small feat.

References

Biscop, S. (2019). European Strategy in the 21st Century: New Future for Old Power. Milton: Routledge.

Brunnstrom, D., Landay, J., Stewart, P., & Popeski, R. (2023, September 8). Musk says he refused Kyiv request for Starlink use in attack on Russia. Reuters. https://www.reuters.com/world/europe/musk-says-he-refused-kyiv-request-use-starlink-attack-russia-2023-09-08/

Celerino, 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'. European Papers Vol. 8, 2023, No 2, pp. 487-501. https://www.europeanpapers.eu/en/europeanforum/eu-space-policy-and-strategic-autonomy

Combined Space Operations. (2022). Combined Space Operations Vision 2031. https://media.defense.gov/2022/Feb/22/2002942522/-1/-1/0/CSPO-VISION-2031.PDF

Council of the European Union. (2021). COUNCIL DECISION (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0698

Directive 2022/2557. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. http://data.europa.eu/eli/dir/2022/2557/oj

European Commission. (2022). COM/2022/60 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: Commission Contribution to European Defence. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52022DC0060

European Commission. (2023a, March 24). IRIS²: the new EU Secure Satellite Constellation. https://defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en

European Commission. (2023b, March 31). IRIS² Industry Information Day - Presentation. https://defence-industry-space.ec.europa.eu/system/files/202303/IRIS2%20Industry%20Information%20Day%20-%2030%20March%202023.pdf

European Commission. (2023c, June 19). EuroQCI Concept of Operations (ConOps). https://digital-strategy.ec.europa.eu/en/miscellaneous/euroqci-conops-concept-operations

References

European Commission. (2023d, October 2). Call for Expression of Interest - EU Space ISAC. https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/call-expressions-interest-eu-space-isac_en

European Commission (n.d.). EU Space Strategy for Security and Defence for a stronger and more resilient European Union. Defence Industry and Space. Retrieved on 30 November 2023, from https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en

European Union. (2023). IRIS²: Infrastructure for resilience, interconnectivity and security by satellite [Fact Sheet]. https://defence-industry-space.ec.europa.eu/system/files/2023-03/IRIS%C2%B2_Factsheet%20%28EN%29.pdf

Harrison, T. et al. (2022). Space Threat Assessment 2022. Center for Strategic and International Studies, https://www.csis.org/analysis/space-threat-assessment-2022.

Kauranen, A. & Solsvik, T. (2023, October 11). Finland says 'outside activity' likely damaged gas pipeline, telecoms cable. Reuters. https://www.reuters.com/markets/commodities/finnish-government-hold-news-conference-suspected-pipeline-leak-media-2023-10-10/

Khurana, M., Frenkel, S., Reinhard, S., Satariano, A., & Metz, C. (2023, July 29). Elon Musk's Unmatched Power in the Stars. The New York Times. https://www.nytimes.com/interactive/2023/07/28/business/starlink.html

Kim, V., Pérez-Peña, R., & Kramer, A. E. (2023, September 8). Elon Musk Refused to Enable Ukraine Drone Attack on Russian Fleet. The New York Times. https://www.nytimes.com/2023/09/08/world/europe/elon-musk-ukraine-starlink-drones.html

Oikonomou, I. (2012). The European Defence Agency and EU military space policy: Whose space odyssey? Space Policy, 28(2), 102–109. https://doi.org/10.1016/J.SPACEPOL.2012.02.008

Regulation 2023/588. (2023). Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0588

Regulation 2019/452. (2019). Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. https://eur-lex.europa.eu/eli/reg/2019/452/oj

References

Reillon, V. (30 January, 2017). European space policy: Historical perspective, specific aspects and key challenges. Think Tank of the European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2017)595917

Srivastave, M., Olearchyk, R., & Schwartz, F. (2022, October 7). Ukrainian forces report Starlink outages during push against Russia. Financial Times. https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397

Starlink. (2023). World's most advanced broadband satellite internet. Starlink. https://www.starlink.com/technology

Withington, T. (30 May, 2023). Ukraine's Favourite Dish. European Security & Defence. https://euro-sd.com/2023/05/articles/30035/ukraines-favourite-dish/