INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

DECEMBER 2022

HYPER-CONNECTIVITY AS A TRIGGER FOR STRATEGIC AUTONOMY IN THE EUROPEAN UNION: THROUGH A TRANSFORMATIVE AND DISRUPTIVE TECHNOLOGICAL TRANSITION

WRITTEN BY
LUCREZIA SALA

EDITED BY
JAMES EDWARD COLOMBO

ABSTRACT

Over the past two decades, the European Union (EU) has intensely recalibrated its strategies to fulfil its mission of promoting peace and security and guaranteeing democracy, rule of law, freedoms, human rights, and equality to its citizens. Given the increase in non-conventional threats in the cyber, hybrid, and "cybrid" domains, the EU has started to strengthen its response to this changing security environment. In this context, technological change has become the main character in a society whose governments, economies, people, and armies are highly dependent on hyper-connectivity and impacted by it. The technological transition has transformed how enemies attack their counterparts, fostering digital rivalries and tighter industry competition. To this end, the Union has recently launched the EU's Secure Connectivity Programme (2023-2027), which encloses the third EU constellation of strategic space infrastructures called IRIS2. The latter, inter alia, has been designed to foster strategic autonomy in the Union, thereby reducing foreign dependencies. It is fundamental for the Union to enhance its ability to respond and counter cyber challenges with a comprehensive and collaborative approach, as individual and protectionist actions from the Member States obstruct the achievement of a higher degree of strategic autonomy in the technological and defence arenas.

INTRODUCTION

Nowadays, satellite communication has become extremely significant not only for governments and the global population but also for the international security and defence industry. Through digital transition and technological advancement, space communication is fundamental to deploying emerging systems that can reinforce the EU's cybersecurity and enhance military connectivity, low latency, and global coverage. The creation of an EU space communication infrastructure would largely decrease congestion in space, resulting from space traffic and space debris that hinders the appropriate execution of operations in that domain. As no EU Governmental Satellite Communications policy existed since a few years ago, in 2021, Regulation (EU) 2021/696 set the basis for the implementation of the first one, called GOVSATCOM, which was enclosed in the 2021-2027 EU Space Programme (Regulation (EU) 2021/696, 2021, April). GOVSATCOM has the objective of procuring satellite communication services under civil and governmental control for both the Union and its Member States' authorities. Through one of its preparatory activities called ENTRUSTED (European Networking for satellite Telecommunication Roadmap for the governmental Users requiring Secure, inTeroperable, innovativE and standardiseD services), research and technology (R&T) and research and development (R&D) of new technologies are advanced under the framework of the EU Horizon 2020 Research and Innovation Programme. Furthermore, given the increasing cyber-attacks and natural disasters that destroy terrestrial communication networks, the EU needs to further secure space-based communication systems and avoid dependency on third countries. For instance, the recent creation of multi-orbital satellite communications internet systems included in the EU's Secure Connectivity Programme (2023-2027) marks a keystone in the achievement of EU strategic autonomy (EU-SA). The Programme will deploy the third constellation of strategic space infrastructures called IRIS2 (Infrastructure for Resilience, Interconnectivity, and Security by Satellite), which T. Breton, the Commissioner of the Internal Market, argues will be a "vector of connectivity and a vector of resilience" and will benefit from the synergies with GOVSATCOM, Copernicus – the EU's Earth observation programme – and Galileo – Europe's satellite navigation system (T. Breton, 2022, November 17). In particular, IRIS2 will allow the EU to become a true space power with a more solid cybersecurity apparatus in the long term, whilst being supported by the European Space Agency (ESA) and the private sector.

WHY CONNECTIVITY MATTERS

IRIS2, which will be fully operational in 2024, aims at creating a new, digital, resilient, and safer Union through technological and scientific progress. As our society is more dependent on security and connectivity, the implementation of such a multi-orbit satellite constellation is of paramount importance for the present and future generations. In particular, the latter will face potentially dangerous challenges stemming from the rise of violent extremism to non-conventional threats in the cyber, hybrid, or "cybrid" domains. These types of danger are mostly produced by the increasing levels of hyper-connectivity in our society, fostered by technological advancement. The latter is not only massively mounting but it is also transforming the current and future battlefield. Consequently, the Union is formulating new strategies with the help of its technological and industrial base to protect its population and enhance its international competitiveness to prevent further foreign dependencies. For this to happen, defence and security capabilities must properly meet spatial needs to address space coercions, paving the way to the concept of "building security through resilience" (NATO, 2017).

Hyper-connectivity has increased the demand for services dependent on edge technologies, as both governments and populations need safer satellite communication solutions. For instance, satellite connectivity through Low Earth Orbit1 (LEO) is going to improve and enhance ultra-secured connectivity to armed forces in the Union, thanks to quantum technologies2 and secure encryption. These will be easily implemented through innovative and disruptive technologies, thereby advancing the New Space ecosystem and the European Quantum Communication Infrastructure (EuroQCI), whose Declaration was signed by all the Member States in 2019. This initiative has the objective of integrating quantum-based systems into existing communication infrastructures to protect governmental and military institutions in primis, at the same time as adding an extra layer of security through quantum physics to prevent the revelation of all types of classified information. In this way, the Union will approach a new era of digital sovereignty and industrial competitiveness and will be able to frame a truly European quantum ecosystem through quantum key distribution (QKD) services. Hyper-connectivity will not only be fostered through the EU's Secure Connectivity Programme but also through national quantum communication networks: in fact, the Member States have been creating cross-border links between different networks able to operate both at the ground level and in space.

Furthermore, through innovation and technological research, the EU's Secure Connectivity Programme, with a budget of €2.4 billion, will essentially intensify the competitiveness of the EU industry to ensure a cost-effective, secure, and sovereign space-based satellite communication system. Parallel to the launch of IRIS2,the Programme aims at boosting the preparedness of the Union's infrastructure, crisis management, and surveillance in the fields of security and defence. For this reason, the private sector is a key player in optimizing the costs of the Programme through, for example, the CASSINI Facility3 or InvestEU4 and assisting the EU to develop a global coverage connectivity system that can reach points such as dead zones to foster cohesion across Member States' territories. This is done to boost hyper-connectivity and fulfil the key targets of Europe's Digital Decade, the purpose of which is to empower citizens through a sustainable digital transition and enhance their digital skills whilst securing digital infrastructures (Europe's Digital Decade, 2022).

THE NEXUS WITH STRATEGIC AUTONOMY IN THE EU

The EU's Secure Connectivity Programme will enable the Member States to collaborate and share information more securely, whilst operating in geographical areas and different domains of strategic interest. The relevance of this Programme is based on its supportive nature of EU strategic autonomy, as it will fundamentally reduce European dependency on non-European commercial activities. This matters acutely as EU countries are progressively experiencing an advanced number of sophisticated cyber threats that straddle both national security ownership – as the Russian war in Ukraine has evidenced – and common European areas, meaning that a collaborative approach is crucial to counter these pressures. Additionally, as mentioned in the previous section, the Union will remain connected even in the event of cyber-attacks or damages to terrestrial networks through IRIS2, thereby avoiding the need to depend on third countries. Once again, this is perceived as a substantial step toward the creation of a strategic autonomous Union. However, there exist exogenous and endogenous hurdles that hamper its realisation.

Since NATO declared cyberspace the fifth operational military domain in which to operate, from 2016 onwards Allies are more prone to information-sharing and mutual assistance in the case of cyber-attacks. Similarly, the EU has started to strengthen its Cyber Defence Policy to protect and defend its Member States through mutually enhanced cooperation. An example of this collaboration is the Cyber and Information Domain Coordination Centre (CIDCC), which falls under the Permanent Structured Cooperation (PESCO) framework, and 4 EU countries – France, Germany, Hungary, and the Netherlands – participate to develop such infrastructure. However, it is important to underscore the absence of a project either in the cyberspace domain or in others in which all the 27 countries jointly partake, thereby emphasising a concrete lack of collaboration among the Member States. This shows not only a deficiency in cohesion but also a consequent waste of resources, infrastructures, and military capabilities by the Member States.

THE FRENCH MODUS OPERANDI

The crucial contributor and supporter of EU strategic autonomy is France. On the one hand, there are Member States, like Germany, that perceive the plans of President E. Macron were fairly ambitious in their willingness to create an autonomous Union whilst failing to consult with them about Europe's plans in the security and defence realm. On the other hand, the Baltic States and Poland in particular, consider Macron have done the bare minimum to militarily support Ukraine. Whether Macron's stance is liked or not, what is certain is that his country is the only alone bringing forward the idea of strategic autonomy in the EU, affirming that the latter can no longer rely on America to defend NATO Allies and that "we are currently experiencing is the brain death of NATO" (The Economist, 2019). Despite these strong affirmations, France's new national strategic review released at the beginning of November 2022 paves the way for strategic autonomous EU defence by 2030 with solid links to the Atlantic Alliance. Most importantly, France will prioritise cyber-defence and cyber-resilience to deliver an autonomous and organised capability in this domain to prevent and reduce the risk of cyber-attacks against France and the Union. For instance, France has pledged to increase long-term private and public investments and consolidate a secure digital base for government departments, as it is deemed too fragile at the moment. The French are aware that their country cannot pursue such a strategy in the cyberspace domain alone, as European and international partners are essential to improve cybersecurity. For this reason, France has committed to operating with EU countries to securitise the European "space borders" and the market for cybersecurity services. Curiously, at the time of writing, the Council has adopted a legislation that enhances the common level of cybersecurity across the Union whilst reassuring resilience and incident response capacities through a new directive, "NIS2"5 (EU Council Press Conference, 2022, November 28). This progress is particularly important for the EU's cybersecurity as it sets the basis for the establishment of the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) that will support collective management of cybersecurity incidents in EU countries. Specifically, NIS2 does not concern entities involved in activities of defence, national or public security, and law enforcement. However, it will allow the Member States to have higher degrees of interoperability when it comes to cyber threats and damages.

France identifies strategic autonomy as dependent on "robust European defence industry capabilities that meet its own needs" (Revue Nationale Stratégique, 2022). The République supports the implementation of a solid technological and industrial base whilst promoting joint acquisitions of European technologies and hardware, fully encouraging the creation of a defence investment programme for joint development and procurement of military equipment and capabilities. However, the need for technological and digital sovereignty is more vital than ever to enhance cybersecurity and ensure secure connectivity. Although technological advancement is pursued in the Union, there are specific defence and military requirements that are not following this transition. To this end, the EU lacks proper investments in R&D and, most importantly, a strong presence of the EU's Defence Technological and Industrial Base (EDTIB) which hinders the effectiveness and preparedness of EU space industries and aggravates the securitisation of cyberspace. Nevertheless, Horizon Europe, the European Defence Fund (EDF), and the Digital Europe Programme are all supplements of cybersecurity research and endorse synergies between civilian and military defence applications as key to generating a robust EDTIB through the EU certification scheme of the EU Agency for Cybersecurity (ENISA), secure cloud, and dual-use technologies – including quantum technologies and encryption. The latter types of technologies, together with Artificial Intelligence (AI), are already considered essential for higher levels of cybersecurity, as the EU's Cybersecurity Strategy for the Digital Decade (2020) has shown. Henceforth, it will be fundamental to give the Member States the appropriate tools to define their digital policies through digital sovereignty and build mutual strategic interdependencies.

Ultimately, it is crucial to stress that EU strategic autonomy can only be pursued through a strong, reliable, and solid technological and industrial base. As already specified in a report written by the author – The EU as a strategic autonomous and defence technological actor: between promises and reality – EU countries persistently jeopardise the achievement of strategic autonomy internally through protectionist actions (L. Sala, 2022, October). Examples of the latter concern intra-states competition in third countries, deficient investments in R&T and R&D, budgetary inefficiencies that create duplication of military capabilities over time, and the lack of a shared culture. To this end, particularly to enhance cybersecurity, R&T and R&D require greater attention from all the Member States without free-riding incentives. Although this comes at an exceptionally perilous moment in which competing countries are vastly investing in research and innovation, the Union should envision a similar approach to apply to the future battlefield. Whilst some may deem it inappropriate to spend money and resources in an area such as cybersecurity that is not fundamentally visible, the future of security is firmly attached to non-conventional threats that must be addressed by a cohesive Union.

CONCLUSION

Through this analysis, it is clear that the EU's Secure Connectivity Programme (2023-2027) is a keystone for the achievement of EU strategic autonomy through the launch of IRIS2, the third satellite constellation promoting secure connectivity "Made in the EU" (T. Breton, 2022, November 17). The significance of this stems from the increasing digital hyper-connectivity and reliance on innovative technologies that our societies depend on. Through the integration of quantum-based systems in existing communication infrastructures, IRIS2 aims to enable secure, reliable, and cost-effective satellite communications that can reach dead zones and thereby provide global coverage. Unfortunately, technological change has not only opened new opportunities but also has a transformative and disruptive connotation. These entail a higher degree of hyper-connectivity which brings within itself more considerable cyberattacks that thwart the appropriate functioning of terrestrial networks and may damage governmental and military authorities, thus provoking breaches of security. For instance, IRIS2 is designed to preserve information and connection in the EU in case of damages post-cyberattacks, without depending on third countries.

Hereafter, one can affirm that the Union has become progressively more mindful of the advantages and disadvantages that hyper-connectivity implies, and to this end, it has committed to long-term investments, research, and innovation to reach a higher degree of cybersecurity. In particular, France is the pioneer of future autonomous capabilities in this realm and aims at facilitating cyberspace resilience through a collective approach. Undoubtedly, this will encourage more substantial efforts toward EU strategic autonomy by the Member States, as France alone cannot achieve this critical goal. Ultimately, as competition has become much tighter, the EU must bear in mind that the creation of a collaborative approach to heighten cybersecurity is a prerequisite for the future of security and that many countries are way ahead in technological sovereignty and transition. Nonetheless, the EU can still extend its technological superiority through a more concrete technological and industrial base, which aims at reducing all the ineptitudes and gaps in the EU security and defence industry.

FOOTNOTES

1. LEO is an orbit close to the Earth's surface that allows the Union to have images in higher resolution given its position.
2. Quantum technologies concern quantum communication, computing, simulation, and metrology and sensing.
3. The CASSINI Facility was launched by T. Breton on January 25, 2022. Deploying €1 billion, the Facility aims at boosting investments in EU companies developing space technology or marketing digital applications.
4. InvestEU is the programme that succeeds the Juncker Plan (2015-20) and aims at boosting long-term investment and innovation in the EU over the period 2021-27.
5. NIS2 is the successor of the directive on security of network and information systems (NIS).

BIBLIOGRAPHY

Breton, T. (2022, November 17). Welcome to IRIS², Europe's new Infrastructure for Resilience, Interconnection & Security by Satellites. Retrieved from: https://www.linkedin.com/pulse/welcome-iris-europes-new-infrastructure-resilience-security-breton/

Dempsey, J. (2022). France's Military Pivot to Europe. Carnegie Europe. Retrieved from: https://carnegieeurope.eu/strategiceurope/88403

Gilli, A. NATO, technological superiority, and emerging and disruptive technologies. Nato Defense College 17(2021), pp 5-18. Retrieved from: https://www.jstor.org/stable/pdf/resrep29562.7.pdf

GOVSATCOM (2020, October 7). Europa.eu. Retrieved from: https://www.euspa.europa.eu/european-space/govsatcom

European Commission (2022). Commission welcomes political agreement to launch IRIS², the Union's Secure Connectivity Programme. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6952

European Commission (2022, November 24). The European Quantum Communication Infrastructure (EuroQCI) Initiative. Shaping Europe's Digital Future. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

European Commision (2022). IRIS2: The new EU secure satellite constellation. Defence Industry and Space. Retrieved from: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en

EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. (2022). Europa.eu; European Council. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/
Evroux, C. (2022, October). EU secure connectivity programme Building a multi-orbital satellite constellation. EPRS | European Parliamentary Research Service. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729442/EPRS_BRI(2022)729442_EN.pdf
Revue nationale stratégique 2022 | Secrétariat général de la défense et de la sécurité nationale. (2022). Gouv.fr. Retrieved from: http://www.sgdsn.gouv.fr/communiques_presse/revue-nationale-strategique-2022/

Sala, L. (2022, October 19). The European Union as a Strategic Autonomous and Defence Technological Actor: Between Promises and Reality. Finabel. Retrieved from: https://finabel.org/the-european-union-as-a-strategic-autonomous-and-defence-technological-actor-between-promises-and-reality/

Space Entrepreneurship Initiative - CASSINI. (2022). Defence Industry and Space. Retrieved from: https://defence-industry-space.ec.europa.eu/eu-space-policy/space-entrepreneurship-initiative-cassini_en

The Economist. (2019, November 7). Emmanuel Macron warns Europe: NATO is becoming brain-dead. The Economist. https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead