Istituto Affari Internazionali

IAI PAPERS 24 | 03 - FEBRUARY 2024

ISSN 2610-9603 | ISBN 978-88-9368-317-3

Challenges to Transatlantic Digital Infrastructure: An EU Perspective

by Anselm Küsters, André Wolf and Eleonora Poli

Fondazione Compagnia di San Paolo

ABSTRACT

Recent disruptions in the Baltic Sea and elsewhere highlight the integral role of digital and physical conduits such as gas pipelines, telecommunications cables and undersea data cables in maintaining European connectivity and security. Overall, the EU's responses to emerging challenges to its digital sovereignty, particularly from China and Russia, aim to enhance the security and resilience of its digital landscape, from the Global Gateway Strategy to the Gaia-X project. However, the complexity of the submarine cable infrastructure requires a broader and more holistic assessment of the opportunities and obstacles to ensuring the uninterrupted flow of information across borders. Ultimately, a concerted transatlantic effort is needed to strengthen the backbone of Europe's digital infrastructure against both man-made and natural adversities, thereby securing a future where sovereignty and resilience are paramount for both the EU and the US.

European Union | USA | Transatlantic relations | Digital policy | Digital infrastructures

keywords

IAI PAPERS 24 | 03 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-317-3 © 2024 IAI

Challenges to Transatlantic Digital Infrastructure: An EU Perspective

by Anselm Küsters, André Wolf and Eleonora Poli*

Introduction

Over the past few years, a series of disruptions, most recently in the Baltic Sea, have underscored the vulnerability of European critical infrastructure to accidents and sabotage. On 8 October 2023, "external activity"[1] resulted in considerable damage to the Balticonnector gas pipeline running from Estonia to Finland, along with harm to adjacent telecommunications cables connecting Estonia to both Finland and Sweden – likely caused by the trailing anchor of a Chinese-flagged, Russia-bound commercial ship. This event followed earlier disruptions, including the severe damage inflicted on the Nord Stream gas pipeline between Russia and Germany in September 2022, and previous suspicions of Russian fishing vessels severing cables linking Norway to the Svalbard archipelago, as well as connections from the UK to various northern islands.[2] To date, there is no established mechanism within the Western security community for responding to such grey zone aggression involving infrastructure sabotage, cyberattacks or disinformation campaigns.[3]

The significance of safeguarding digital infrastructure is not inferior to that of gas pipelines and telecommunication cables. Just as these tangible conduits are

[1] Victor Jack, "Finnish Pipeline Leak Points to 'External Activity,' President Says", in *Politico*, 10 October 2023, https://www.politico.eu/?p=3691224.

[2] Marcus Solarz Hendriks and Harry Halem, *From Space to Seabed. Protecting the UK's Undersea Cables from Hostile Actors*, London, Policy Exchange, 2024, p. 10 and 41f, https://policyexchange.org.uk/publication/from-space-to-seabed.

[3] Elisabeth Braw, "Baltic Sea Sabotage: A Defender's Dilemma", in *Politico*, 15 November 2023, https://www.politico.eu/?p=3859824.

* Anselm Küsters is Head of Digitalisation and New Technologies Department at the Centre for European Policy (CEP) in Berlin. André Wolf is Head of the Department Technological Innovation, Infrastructure and Industrial Development at CEP in Berlin. Eleonora Poli is Head of Analysis at the CEP Rome Office.

. This paper is part of the project "Building a transatlantic technology bridge: challenges and opportunities", managed by the Istituto Affari Internazionali (IAI), in partnership with the German Marshall Fund of the United States and Centrum für Europäische Politik, and supported by Fondazione Compagnia di San Paolo.An US perspective on the topic of digital infrastructures is also available as part of the project (see IAI Papers 24|04).

vital for energy and communication flow, digital infrastructure — encompassing undersea data cables, cloud computing resources and other internet backbone elements — form the lifeline of the European and transatlantic information society.[4] The vulnerability of these systems extends beyond mere interruption of services; it poses a threat to national security, economic stability and citizens' privacy. Therefore, ensuring the resilience and security of digital infrastructure is crucial for the EU, especially regarding submarine communication cables. Carrying over 99 per cent of all internet traffic, submarine cable systems are essential to the EU as it seeks to maintain a vital role in the connectivity ecosystem, to secure its infrastructure and services and to establish its digital sovereignty.[5]

1. EU strategic interests in digital infrastructure and its industrial policy

Transatlantic digital infrastructure is notably interconnected through shared data cables, virtual platforms and cloud services. Europe's recent turn towards a more strategic understanding of this critical infrastructure is epitomised by the new EU defence doctrine, the Strategic Compass for Security and Defence,[6] which defines cyberspace, space and maritime infrastructures as contested areas that must be protected together. In June 2023, the Commission presented a European Economic Security Strategy to counter the increasing willingness of China and Russia to instrumentalise trade and control of critical supply chains for geopolitical gain.[7] Ensuring economic security in this context refers not only to supply chain risks and the risk of exploiting economic dependency, but also to the physical and cyber security of critical infrastructure. Finally, in January 2024, the Commission released a package of five initiatives aiming to strengthen economic security,[8] with a particular focus on risks related to international trade and foreign direct investment flows, considering both the inward and outward perspectives. When it comes to European maritime security, an updated strategy and action plan were approved in October 2023 to uphold the rules-based order at sea and to boost collaboration with NATO to better face environmental challenges and hybrid cyber-attacks.

[4] See Rosanna Fanni et al., "A Digital Connectivity Masterplan for the Global Gateway", in *CEPS Reports*, 19 December 2022, p. 11, https://www.ceps.eu/?p=39251.

[5] PwC EU Services, *Study to Monitor Connectivity. Connecting the EU to Its Partners Though Submarine Cables*, Luxembourg, Publications Office of the European Union, 2022, https://doi.org/10.2759/608766.

[6] Council of the European Union, *A Strategic Compass for Security and Defence*, 21 March 2022, https://www.eeas.europa.eu/node/410976.

[7] European Commission, *European Economic Security Strategy* (JOIN/2023/20), 20 June 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52023JC0020.

[8] European Commission, *Commission Proposes New Initiatives to Strengthen Economic Security*, 24 January 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363.

ISSN 2610-9603 | ISBN 978-88-9368-317-3

ISSN 2610-9603 | ISBN 978-88-9368-317-3

In the wake of Russia's actions against Ukraine, the EU initiated, accelerated or implemented several initiatives that aimed to increase the security and resilience of the European digital infrastructures. To begin with, the EU Global Gateway strategy – approved before Russia's invasion of Ukraine – plans to mobilise 300 billion euros between 2021 and 2027 to "boost smart, clean and secure links in digital, energy and transport […] across the world" through infrastructure development with partner countries.[9] Moreover, when it comes to cybersecurity and requirements for key economic actors, it is worth mentioning the EU's revised Network and Information Security Directive (NIS2), the Cyber Resilience Act and the 5G Cybersecurity Toolbox. European governments are adopting a multi-cloud strategy for public services, spreading various tasks across multiple cloud providers to increase innovation, flexibility and security. Concerns centre on the security risks associated with foreign control of critical digital infrastructure by large American and Chinese companies, and whether cloud computing for critical services should be geographically located within the EU.[10] Finally, the Gaia-X project is focused on establishing a federated cloud data infrastructure across Europe, meaning a network of interconnected data centres and cloud services that are distributed across different Member States but work together in a cohesive manner. However, although initially conceived as a bold counter-initiative to major foreign cloud providers, Gaia-X has not yet achieved widespread adoption by private companies.

2. Challenges and opportunities

Currently, the world is interconnected by 529 cable systems and 1,444 points where these submarine cables reach the shore ("landings") that are either active or under construction globally. In Europe, Marseille is the leading site where these undersea cables make landfall, but new connection points in Barcelona, Genoa, and Crete are emerging as significant, promising to enhance the network's resiliency by providing alternative routes for data transmission (Figure 1). In the first-mile value chain of submarine cable infrastructure, the primary actors include surveyors, system suppliers, installers, owners, maintenance providers, customers and other stakeholders. The market is dominated by four major companies – EU-based Alcatel Submarine Network (ASN), US-based SubCom, Japan's NEC and China's Huawei Marine – with SubCom being the most active in the EU (24 per cent market share in 2020-2025).[11] However, Big Tech content providers such as Google (with 90,000 km of cables) and Facebook (with 50,000 km) are currently disrupting the

[9] European Commission, *Global Gateway: Up to €300 Billion for the European Union's Strategy to Boost Sustainable Links around the World*, 1 December 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433.

[10] Mark Leonard et al., "Redefining Europe's Economic Sovereignty", in *ECFR Policy Briefs*, June 2019, https://ecfr.eu/?p=4420; Ulrike Franke, "Harnessing Artificial Intelligence", in *ECFR Policy Briefs*, June 2019, https://ecfr.eu/?p=4423.

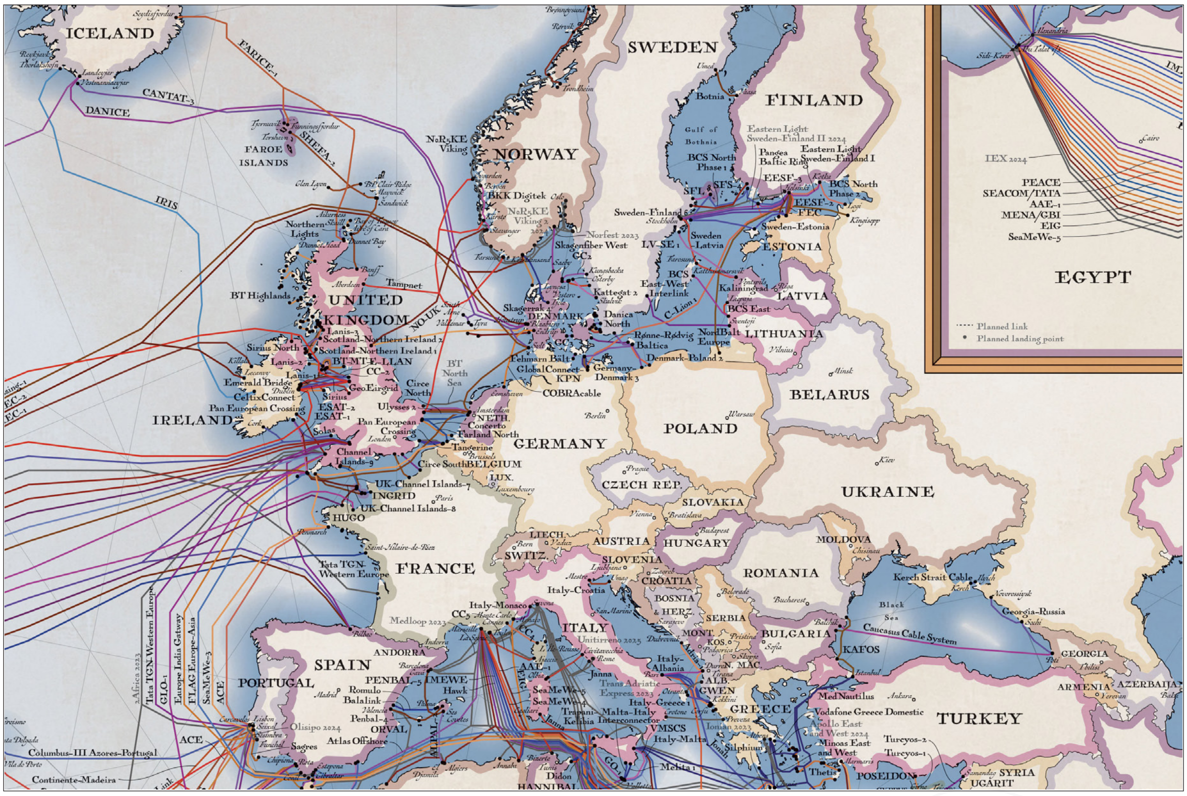
[11] PwC EU Services, *Study to Monitor Connectivity*, cit., p. 14f.

IAI PAPERS 24 | 03 - FEBRUARY 2024

ISSN 2610-9603 | ISBN 978-88-9368-317-3 © 2024 IAI

traditional business model of telecom service providers by increasingly building their own cables in virtually all regions. The influence of these US-based content providers is expected to grow, creating opportunities for EU-US cooperation.

Figure 1 | Cable systems and landings in Europe



Source: TeleGeography, *Sub-Map for Europe*, https://submarine-cable-map-2023.telegeography.com.

As part of the Digital Networks Act, the Commission is planning to increase the resilience of subsea cables, with a new recommendation and funding for the 2024–2027 period. In particular, it aims to define and invest in "Cable Projects of European Interest" that would reduce its reliance on too few undersea internet connections and make it less vulnerable to sabotage.[12] However, the Commission's ambitious plans are hampered by a strained EU budget. In particular, some Member States are concerned about the fairness of the funding process within the Connecting Europe Facility (CEF) committee. This committee decides on funding on the basis of various criteria, including a project's ability to attract private funding. However, there are complaints that funding is not always awarded to the highest quality projects.[13]

[12] See Mathieu Pollet, "EU Looks to Boost Secure Submarine Internet Cables in 2024", in *Politico*, 11 October 2023, https://www.politico.eu/?p=3697125.

[13] See Luca Bertuzzi, "EU Readies Second Round of Submarine Cables Financing, But Resource Allocation Raises Questions", in *Euractiv*, 19 October 2023, https://www.euractiv.com/?p=1995556.

On 10 January, the Commission selected 37 projects under the second "Connecting Europe" financing round, allocating a total of 252 million euros for the development of submarine cables (plus additional projects for 5G infrastructure) to enhance the security and resilience of backbone networks between Ireland and the EU mainland, regions in the far reaches of the Atlantic, a direct trans-Arctic link to the Far East, infrastructure for digitally underserved Greek islands and enhanced connectivity with Africa.[14]

However, a key problem is that even if there is sufficient funding and legal possibility to diversify the data cables serving Europe, they still need to be protected from deliberate external damage.[15] The UK example shows how immediate military protection can be organised to ensure that critical submarine cables are not tapped or sabotaged. Since December 2023, the British Navy has deployed warships to protect critical infrastructure such as undersea cables and pipelines in the maritime region extending from the English Channel to the Baltic Sea.[16] This protection mission is part of the commitments under the Joint Expeditionary Force, a northern European military alliance which ensures the security of the infrastructure in this sea region.[17]

In light of these challenges, the EU is currently attempting to create a European satellite constellation, the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS^2), which will provide communication and internet services for both security services and public users.[18] Approved by the European Parliament in February 2023, the constellation's first services should be operational in 2024 and the complete system in 2027. The project has been adopted in record time to ensure quantum-safe communication between European capitals and to protect against cybersecurity attacks in space through jamming (i.e., deliberate prevention of signal reception), spoofing (i.e., deliberate transmission of counterfeit signals) and sabotage. The EU is also planning to outfit the satellites with additional features that would allow them to track other satellites or spy balloons. From the perspective of critical digital infrastructure, IRIS^2 is to be welcomed, but the EU currently lacks sufficient launching capabilities to move its

[14] See European Commission, *Over €250 Million to Support Secure Connectivity Across the EU Under the CEF Digital Programme*, 10 January 2024, https://digital-strategy.ec.europa.eu/en/node/12342.

[15] Anselm Küsters, "Europas verwundbares Rückgrat. Warum die EU digitale kritische Infrastruktur besser schützen muss", in *cepAdhoc*, No. 13 (21 October 2022), https://www.cep.eu/en/eu-topics/details/cep/europas-verwundbares-rueckgrat-cepadhoc.html.

[16] See "Britische Kriegsschiffe sollen Unterwasser-Infrastruktur schützen", in *Der Spiegel*, 30 November 2023, https://www.spiegel.de/ausland/a-8cf3059e-0187-46dc-9a73-8cdaff1ac4f0; "Britain to send seven Royal Navy ships to patrol areas with undersea cables", in *Reuters*, 30 November 2023, http://reut.rs/3N3UquI.

[17] Charlie Duxbury and Claudia Chiappa, "Northern Europe's New Naval Priority: Submarine Sabotage", in *Politico*, 2 January 2024, https://www.politico.eu/?p=4057362.

[18] For these plans see, e.g., Joshua Posaner and Antoaneta Roussi, "EU Hopes New Satellites Can Spot Spy Balloons, Spacecraft", in *Politico*, 14 February 2023, https://www.politico.eu/?p=2633937.

satellites into space.[19] More importantly, while satellite networks can provide an alternative telecommunication pathway and thus increase overall resilience, their likely capacity cannot bear even a tenth of the submarine cable traffic.[20]

3. EU-US cooperation

The so-called Sea-Me-We-6 submarine cable is currently the most important element of transatlantic cooperation in the provision of digital infrastructure. The planned cable, which is being managed by the US company SubCom after two of China's biggest operators, China Telecom and China Mobile, withdrew from the project,[21] will run from Singapore via the Indian Ocean and the Suez Canal directly to the Mediterranean Sea (19,200 kilometres). It will consist of ten fibre optic pairs, each with a transmission rate of 12.6 terabits per second.[22] Sea-Me-We-6 offers a much-needed alternative to the Peace cable, which connects Asia, Africa, and Europe (15,000 kilometres) but is mainly laid by Chinese companies. The cable is thus crucial for Europe and transatlantic cooperation, providing a high-capacity digital link from Singapore to Marseilles, increasing connectivity despite China's reduced involvement, and ensuring diverse international cooperation and robust infrastructure.

Over the past year, the EU-US Trade and Technology Council (TTC) has emerged as a good avenue for supporting such projects and diversifying cable routes. During the first TTC meeting in Pittsburgh on 29 September 2021, a dedicated specific group (WG4) was given the responsibility to investigate the potential for joint efforts in funding secure and stable internet in developing countries. This initiative led to the establishment of a specialised task force dedicated to combined EU-US funding initiatives. At another TTC meeting in December 2022, the EU and the US announced collaborative projects to bolster digital networks in Jamaica and Kenya. In Luleå in May 2023, there were further announcements of support for digital initiatives in Costa Rica and the Philippines. Moreover, the EU and the US have pledged to work together on ensuring that new undersea cable projects are entrusted to reliable suppliers.

[19] For this "launcher crisis", see European Space Policy Institute (ESPI), "The War in Ukraine and the European Space Sector", in *ESPI Briefs*, No. 57 (May 2022), https://www.espi.or.at/?p=438.

[20] Abra Ganz et al., "Submarine Cables and the Risks to Digital Sovereignty", in *SSRN*, 12 January 2024, https://ssrn.com/abstract=4693206.

[21] Since 2020, the US has prevented submarine cable projects involving US and Chinese companies. With their withdrawal, China Telecom and China Mobile may have thus merely pre-empted a US exclusion. For the context, see Achim Sawall, "China steigt bei Seekabel von Asien nach Europa aus", in *Golem.de*, 13 February 2023, https://www.golem.de/news/sea-me-we-6-china-steigt-bei-seekabel-von-asien-nach-europa-aus-2302-171866.html.

[22] Data taken from Submarine Networks: *SEA-ME-WE 6*, https://www.submarinenetworks.com/en/systems/asia-europe-africa/smw6.

ISSN 2610-9603 | ISBN 978-88-9368-317-3

IAI PAPERS 24 | 03 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-317-3 © 2024 IAI

Empirical evidence indicates that such investment initiatives are not only apt to increase the general connectivity of developing countries but can also create a macroeconomic stimulus. A prerequisite is that subsea cable projects be accompanied by a sufficient expansion of local terrestrial broadband infrastructure. For instance, a recent analysis finds evidence for significant positive effects of subsea cable projects on the quantity and quality of jobs in regions with broadband access in several African countries, amongst others Kenya and Nigeria.[23] It also detects a positive impact on financial service exports by these countries. This, in turn, can have important long-term developmental implications, as a growing financial sector can improve access to international capital markets and boost resilience in case of financial shocks.[24] Subsea cables could thus indirectly contribute to reducing credit constraints and boosting economic growth in developing countries in the long run. Hence, it is sensible for the EU and the US not to judge these projects exclusively based on security concerns but also regarding the wider goal of diversifying their international supply chains through supporting the formation of competitive capacities in developing economies.

4. Future prospects for EU-US cooperation

In the near and mid-term future, there are several promising avenues to deepen EU-US cooperation in the realm of digital infrastructure due to mutual gains. Our seven key points are ordered "bottom-up" along the value chain for producing resilient digital infrastructure, starting with a common geographical vision, proceeding to the underlying cables, raw materials and inputs themselves, and ending with protection and safeguard strategies and instruments.

1. *Create a common geographic vision of digital connectivity as a counterpart to China's digital silk road, including joint cable protection zones*. US-EU digital cooperation must develop a shared vision for a digital network in space, analogous to China's digital silk road.[25] Specific protected zones for cables in national waters must be defined to prevent accidental cable cuts through anchoring and fishing activities.[26] While not ruling out "grey zone aggression", this measure would help

[23] Alan C. O'Connor et al., "Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in Kenya", in *RTI Working Papers*, No. 0214363.202.2 (November 2020), https://www.rti.org/node/47074; Alan C. O'Connor et al., "Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in Nigeria", in *RTI Working Papers*, No. 0214363.202.4 (November 2020), https://www.rti.org/node/47077.

[24] Matthew O. Odedokun, "Alternative Econometric Approaches for Analysing the Role of the Financial Sector in Economic Growth: Time-Series Evidence from LDCs", in *Journal of Development Economics*, Vol. 50, No. 1 (June 1996), p. 119-146, DOI 10.1016/0304-3878(96)00006-5.

[25] Bora Ly, "Challenge and Perspective for Digital Silk Road", in *Cogent Business & Management*, Vol. 7, No. 1 (2020), Article 1804180, https://doi.org/10.1080/23311975.2020.1804180.

[26] The European Parliament has considered proposing to maritime authorities to develop such protective measures. Christian Bueger, Tobias Liebetrau and Jonas Franken, "Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU", in *European Parliament In-Depth Analysis*, June 2022, https://www.europarl.europa.eu/thinktank/en/document/

IAI PAPERS 24 | 03 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-317-3 © 2024 IAI

to decide whether a cable was cut accidentally or not. Moreover, the digital level should not be conceived in isolation, but as a building block of an overarching connectivity and development strategy. This should be accompanied by a credible growth prospect for developing countries that is more attractive than China's dirigiste approach to infrastructure cooperation. Above all, this includes more say in network planning, guarantees for local sourcing and a roadmap for future value chain upgrading. Such a more "positive offer" underpinned by EU values would go beyond "naked infrastructure" and include "soft layers", with solutions for self-sovereign digital identity, digital payments, data governance standards and measures that promote local sovereignty on digital connectivity projects.[27]

2. *Speed up the diversification of submarine cables through co-financing new cable projects*. This can be realised best through joint financing of new projects under initiatives like the "Cable Projects of European Interest" envisioned by the Digital Networks Act, the CEF as part of the Global Gateway strategy and the transnational projects planned under the TTC. In light of the strategic importance of certain submarine cables, the EU should increase transatlantic cooperation with US-based firms but also adopt a unified strategy to assist EU-based firms in creating new, secure submarine cable routes.[28] To ensure a shared transatlantic commitment to strategic digital advancements and a joint digital backbone, increasing the number and redundancy of cables should be accompanied by a more careful selection of providers (see point 4 below).

3. *Invest and collaborate in research for developing more resilient data-transmitting cables*. This initiative would look at how, over time, existing pipelines and cables could be best reinforced with physical protection (e.g., certain types of concrete) and surveillance measures (e.g., fibre optic cables that could sense objects being dropped nearby). Sensors and detection systems on crucial segments of submarine cables could pre-emptively identify physical threats and, supported by EU guidelines, might become a mandatory aspect of licensing for submarine cable landings.[29] In addition, this research pillar would address often-overlooked natural disaster risks like underground volcanic activity, which might intensify due to rapid climate change.[30]

EXPO_IDA(2022)702557.

[27] Rosanna Fanni et al., "A Digital Connectivity Masterplan for the Global Gateway", cit., p. 4, 22f.

[28] PwC EU Services, *Study to Monitor Connectivity*, cit.

[29] Christian Bueger et al., "Protecting Subsea Data Cables in Europe and the Atlantic: Challenges of a New Era", in *Atlantic Centre Policy Briefs*, No. 13 (July 2022), p. 9, https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_13.pdf. For an overview of existing sensor technologies (acoustic, optic, magnetic and oceanographic) that could be used for autonomous monitoring of underwater cables, see Dimitrios Eleftherakis and Raul Vicen-Bueno, "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", in *Sensors*, Vol. 20, No. 3 (2020), p. 737, https://doi.org/10.3390/s20030737.

[30] For evidence, see: Bill McGuire, *Waking the Giant. How a Changing Climate Triggers Earthquakes, Tsunamis, and Volcanoes*, Oxford, Oxford University Press, 2012.

4. *Diversify the suppliers for digital infrastructure components through a joint European regime for regulatory approval, antitrust investigations and a European "Clean Cable Initiative"*. The technical underpinnings of digital infrastructure involve several entities, which may be private or semi-public in nature, tasked with manufacturing, deploying, maintaining, and owning the network cables. In planning procurement, policymakers must consider the entire cybersecurity ecosystem in the transatlantic sphere. In particular, the EU should reduce reliance on Chinese companies, including Huawei, ZTE and China Telecom, and instead coordinate with the US to support common technical standards. Here, we emphasise three measures: First, creating a joint European regime for regulatory approval for cable-laying, as the EU currently leaves the authority to approve the laying of cables to individual member states.[31] Secondly, the EU should conduct more antitrust investigations in this sector, like it did in 2021, when it detected that Chinese companies used predatory pricing to dump fibre-optic cables (which might include critical backdoors) into the European market.[32] Third, inspired by the US government's Clean Cable campaign, a European Clean Cable investment programme would ensure that critical cables connecting the continent to the internet cannot be tapped or used for blackmailing.[33] Here there is clear potential for transatlantic cooperation. Even though 26 EU countries have agreed to abide by "The Clean Network" principles, the US announcement was met with caution in Europe. This caution stemmed from fears that the initiative could lead to a divided internet and a general scepticism about US claims that Huawei posed insurmountable security threats.[34] Given the speed with which the geopolitical situation in Europe has changed since 2020, it is worth reviving this initiative, as it would be better received by Europeans. Overall, this strong regulatory approach is justified by the fact that it is prohibitively expensive and difficult to revise digital supply chains and technical dependencies once certain components have been integrated, which is increasingly problematic in a world of fast-paced geopolitics.

5. *Extend plans for future cooperation on raw materials (raw materials club) to digital inputs*. The plans on digital cooperation should be institutionally linked to the ongoing EU-US negotiations on establishing a long-term partnership in accessing physical raw materials critical for the green and digital transformation. The large overlap of economic objectives of both initiatives makes a joint institution under the umbrella of strengthening supply chain security sensible. A good example of this is the role of the semiconductor industry in both economic areas, representing an important critical raw material consumer as well as a key to digital sovereignty.

[31] Abra Ganz et al., "Submarine Cables and the Risks to Digital Sovereignty", cit., p. 13.

[32] Ryan Daws, "EU to Slap Large Tariffs on Chinese Optical Fibre Cables", in *Telecoms Tech News*, 19 November 2021, https://www.telecomstechnews.com/?p=96360.

[33] For this proposal, see Anselm Küsters, "Europas verwundbares Rückgrat", cit.

[34] Xuewu Gu, "The Illusion of 'The Clean Network'", in *Structural Power in the Global Age. Why Modernity is Ending and Globality Prevails*, Cham, Springer, 2022, p. 123-131.

ISSN 2610-9603 | ISBN 978-88-9368-317-3

6. *Provide increased protection of key maritime and cable routes, particularly in the Baltic Sea*. While it would be cost-prohibitive to provide patrols or greater physical protection for the whole 1.4 million kilometres of submarine cables worldwide,[35] regular missions surrounding European shores that focus on the most vulnerable parts of the cables could have an important deterrence effect. Besides investing heavily in own security capabilities, such as specialised boats and drones, increased EU protection should be pushed in the short term through collaboration within the Northern Joint Expeditionary Force and within NATO.

7. *Establish a separate EU Commissioner for security and defence*, with competences in the areas of space, cyber and defence. This could be done when forming the next European Commission after the 2024 elections and is necessary in light of the need to boost military spending and strengthen digital infrastructure within the EU. Having such a Commissioner would help advocate for a larger EU role within NATO, given the recommended 24/7 control of key maritime and cable routes for which NATO support is indispensable.

In sum, the proposed avenues for EU-US cooperation in digital infrastructure are not just about enhancing connectivity; they represent a strategic alignment of values, objectives and visions. This cooperation is pivotal for ensuring the EU's digital resilience against both geopolitical and natural threats. By diversifying cables and suppliers through "Cable Projects of European Interest", CEF investments as part of the Global Gateway strategy, as well as TTC projects; by formulating a common geographic vision of digital connectivity and plans for a raw materials club; and by setting up an EU Commissioner for security and defence that pushes for increased protection of key maritime and cable routes, the EU will significantly enhance its autonomy and security.

Updated 22 February 2024

[35] Abra Ganz et al., "Submarine Cables and the Risks to Digital Sovereignty", cit., p. 10.

IAI PAPERS 24 | 03 - FEBRUARY 2024   ISSN 2610-9603 | ISBN 978-88-9368-317-3   © 2024 IAI

References

Luca Bertuzzi, "EU Readies Second Round of Submarine Cables Financing, But Resource Allocation Raises Questions", in *Euractiv*, 19 October 2023, https://www.euractiv.com/?p=1995556

Elisabeth Braw, "Baltic Sea Sabotage: A Defender's Dilemma", in *Politico*, 15 November 2023, https://www.politico.eu/?p=3859824

Christian Bueger et al., "Protecting Subsea Data Cables in Europe and the Atlantic: Challenges of a New Era", in *Atlantic Centre Policy Briefs*, No. 13 (July 2022), https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_13.pdf

Christian Bueger, Tobias Liebetrau and Jonas Franken, "Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU", in *European Parliament In-Depth Analysis*, June 2022, https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557

Council of the European Union, *A Strategic Compass for Security and Defence*, 21 March 2022, https://www.eeas.europa.eu/node/410976

Ryan Daws, "EU to Slap Large Tariffs on Chinese Optical Fibre Cables", in *Telecoms Tech News*, 19 November 2021, https://www.telecomstechnews.com/?p=96360

Charlie Duxbury and Claudia Chiappa, "Northern Europe's New Naval Priority: Submarine Sabotage", in *Politico*, 2 January 2024, https://www.politico.eu/?p=4057362

Dimitrios Eleftherakis and Raul Vicen-Bueno, "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", in *Sensors*, Vol. 20, No. 3 (2020), p. 737, https://doi.org/10.3390/s20030737

European Commission, *Commission Proposes New Initiatives to Strengthen Economic Security*, 24 January 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363

European Commission, *European Economic Security Strategy* (JOIN/2023/20), 20 June 2023, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52023JC0020

European Commission, *Global Gateway: Up to €300 Billion for the European Union's Strategy to Boost Sustainable Links around the World*, 1 December 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433

European Commission, *Over €250 Million to Support Secure Connectivity Across the EU Under the CEF Digital Programme*, 10 January 2024, https://digital-strategy.ec.europa.eu/en/node/12342

European Space Policy Institute (ESPI), "The War in Ukraine and the European Space Sector", in *ESPI Briefs*, No. 57 (May 2022), https://www.espi.or.at/?p=438

Rosanna Fanni et al., "A Digital Connectivity Masterplan for the Global Gateway", in *CEPS Reports*, 19 December 2022, https://www.ceps.eu/?p=39251

Abra Ganz et al., "Submarine Cables and the Risks to Digital Sovereignty", in *SSRN*, 12 January 2024, https://ssrn.com/abstract=4693206

Xuewu Gu, "The Illusion of 'The Clean Network'", in *Structural Power in the Global Age. Why Modernity is Ending and Globality Prevails*, Cham, Springer, 2022, p. 123-131

Victor Jack, "Finnish Pipeline Leak Points to 'External Activity,' President Says", in *Politico*, 10 October 2023, https://www.politico.eu/?p=3691224

Anselm Küsters, "Europas verwundbares Rückgrat. Warum die EU digitale kritische Infrastruktur besser schützen muss", in *cepAdhoc*, No. 13 (21 October 2022), https://www.cep.eu/en/eu-topics/details/cep/europas-verwundbares-rueckgrat-cepadhoc.html

Mark Leonard et al., "Redefining Europe's Economic Sovereignty", in *ECFR Policy Briefs*, June 2019, https://ecfr.eu/?p=4420; Ulrike Franke, "Harnessing Artificial Intelligence", in ECFR Policy Briefs, June 2019, https://ecfr.eu/?p=4423

Bora Ly, "Challenge and Perspective for Digital Silk Road", in *Cogent Business & Management*, Vol. 7, No. 1 (2020), Article 1804180, https://doi.org/10.1080/23311975.2020.1804180

Bill McGuire, *Waking the Giant. How a Changing Climate Triggers Earthquakes, Tsunamis, and Volcanoes*, Oxford, Oxford University Press, 2012

Alan C. O'Connor et al., "Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in Kenya", in *RTI Working Papers*, No. 0214363.202.2 (November 2020), https://www.rti.org/node/47074

Alan C. O'Connor et al., "Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in Nigeria", in *RTI Working Papers*, No. 0214363.202.4 (November 2020), https://www.rti.org/node/47077

Matthew O. Odedokun, "Alternative Econometric Approaches for Analysing the Role of the Financial Sector in Economic Growth: Time-Series Evidence from LDCs", in *Journal of Development Economics*, Vol. 50, No. 1 (June 1996), p. 119-146,

IAI PAPERS 24 | 03 - FEBRUARY 2024 ISSN 2610-9603 | ISBN 978-88-9368-317-3 © 2024 IAI

DOI 10.1016/0304-3878(96)00006-5

Mathieu Pollet, "EU Looks to Boost Secure Submarine Internet Cables in 2024", in *Politico*, 11 October 2023, https://www.politico.eu/?p=3697125

Joshua Posaner and Antoaneta Roussi, "EU Hopes New Satellites Can Spot Spy Balloons, Spacecraft", in *Politico*, 14 February 2023, https://www.politico.eu/?p=2633937

PwC EU Services, *Study to Monitor Connectivity. Connecting the EU to Its Partners Though Submarine Cables*, Luxembourg, Publications Office of the European Union, 2022, https://doi.org/10.2759/608766

Achim Sawall, "China steigt bei Seekabel von Asien nach Europa aus", in *Golem.de*, 13 February 2023, https://www.golem.de/news/sea-me-we-6-china-steigt-bei-seekabel-von-asien-nach-europa-aus-2302-171866.html

Marcus Solarz Hendriks and Harry Halem, *From Space to Seabed. Protecting the UK's Undersea Cables from Hostile Actors*, London, Policy Exchange, 2024, https://policyexchange.org.uk/publication/from-space-to-seabed

ISSN 2610-9603 | ISBN 978-88-9368-317-3

ISSN 2610-9603 | ISBN 978-88-9368-317-3

Istituto Affari Internazionali (IAI)
The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17 - I-00186 Rome, Italy
T +39 06 6976831
iai@iai.it
www.iai.it

Latest IAI PAPERS

Director: Riccardo Alcaro (r.alcaro@iai.it)

24 | 03	Anselm Küsters, André Wolf and Eleonora Poli, *Challenges to Transatlantic Digital Infrastructure: An EU Perspective*
24 | 02	Nicola Casarini, *The Future of the Belt and Road in Europe: How China's Connectivity Project is Being Reconfigured across the Old Continent – and What It Means for the Euro-Atlantic Alliance*
24 | 01	Federica Marconi, Max Münchmeyer and Irene Paviotti, *The State of EU-US Digital and Energy Cooperation*
23 | 23	Leila Alieva, *De-colonising the Azerbaijan-Armenian Conflict: Breaking the Knot of Security and Dependence*
23 | 22	Jing Men, *The Chinese Perspectives on the EU's Policy towards China*
23 | 21	Rend Al-Rahim, *Transitional Justice in Iraq: The Challenges of National Healing and Recovery*
23 | 20	Marina Rudyak, *China and the Global South: Many Initiatives, One Narrative*
23 | 19	Tanina Zappone, *Reinventing Soft Power: The Strong Impact of China's Soft Power "Shortcomings" on the Global South*
23 | 18	Pier Paolo Raimondi, *Italy and Norway: Perspectives for a Further Energy Cooperation*
23 | 17	James A. Millward, *Sinicisation, the Tribute System and Dynasties: Three Concepts to Justify Colonialism and Attack non-Sinitic Diversity in the People's Republic of China*