Norwegian Institute of International Affairs

POLICY BRIEF – 3 / 2024

The EU's international cyber and digital engagements

Patryk Pawlak

HIGHLIGHTS

• The EU's vision of a human-centric digital future rooted in rules-based order and the rule of law is not universally shared.

• In 2024, the effectiveness of the EU's cyber and digital diplomacy will be tested with three major international events coming up: NETmundial+10, WSIS+20, and the UN Summit of the Future.

• The EU needs to ensure that a broad range of tools at its disposal are used in a more strategic and targeted way that goes beyond traditional binary choices between developed-developing and likeminded-contester countries.

Digital transformation is a key priority for the European Union. It drives economic growth and enables societal development. However, the EU's leadership in digital matters and its capacity to deliver are not universally recognised.

First, there is skepticism about the EU's leadership and its vision for a human-centric digital future — one that places human rights and the rule of law at the center of technological innovation and digital transformation. The United States, India, China, and Brazil have challenged the EU's approach to data governance, digital sovereignty, and internet governance policies.

Second, the EU's global influence is limited by its own ability to deliver certain critical capabilities in the digital and cyber domains. Despite increasing investment in new and emerging technologies such as AI, quantum

computing, and cybersecurity, the EU still underperforms compared to other players, notably the US and China.

Third, while expectations for the EU's role have grown, cyber and digital policies are governed primarily by an intergovernmental method. All these elements impact the EU's international engagements.

How does the EU frame and implement its international cyber and digital engagements (hereafter referred to as CDEs) with third countries? What drives this cooperation, and what are the specific tools and mechanisms deployed by the EU?

Mutualism of digital and cyber policies

Despite clear differences, the distinction between cyber and digital policies is not always clear due to the nature of their symbiotic relation. Their legal basis in the EU Treaties does not offer clear answers. Both the digital and cyber policy domains primarily fall under Article 114 of the Treaty on the Functioning of the European Union (TFEU), which concerns the approximation of national regulations to ensure the establishment and functioning of the internal market. The EU's AI Act and the Network and Information Security Directive (NIS2) are both rooted in this article. Conversely, EU laws on cybercrime are based on Article 83 TFEU. As a general rule, topics related to digital technologies and the broader digital economy – such as Internet governance, digital innovation, digital infrastructure, or emerging technologies like AI and quantum computing – are categorized under the digital umbrella.

Cyber policies, meanwhile, are associated with the safety and security aspects of digital technologies, encompassing cybersecurity, supply chain security, network security standards, and cybercrime. However, these distinctions are more theoretical than practical. For instance, technological standards for the Open Internet encompass both digital and cyber issues: they influence the future of Internet governance and national security. The necessity of incorporating cybersecurity into all digital investments and capabilities, including AI, encryption, and quantum computing, further complicates this distinction. This complexity is also reflected in the EU's external relations.

Digital diplomacy aims to assert the EU's leadership in global digital matters, focusing on enhancing cooperation in and with relevant multilateral and multistakeholder forums to advocate EU policies, such as within the UN's Global Digital Compact. Cyber diplomacy primarily addresses the international security aspects of cyberspace governance. The EU's international engagements in this area strive to promote and strengthen the UN framework for responsible state behaviour in cyberspace, with the primary goal of preventing, discouraging, deterring, and responding to malicious cyber activities. The EU's Cyber Diplomacy Toolbox (CDT) and its implementing guidelines form the cornerstone of the EU's external cyber engagements.

Ecosystem of cooperation patterns

The EU leverages its diplomatic and policy tools to promote convergence with its digital and cyber policies, which are based on a human-centric approach to digital transformation. This approach is grounded in respect for human rights and the rule of law. The choice of specific tools and instruments depends on two main factors: the perceived level of convergence of a partner country's positions with the EU, and specific drivers of cooperation (e.g., national security, economic growth, human rights, or international stability). Considering the convergence of approaches, it is possible to distinguish four main groups of countries: likeminded, contesters, champions, and newcomers.

Likeminded countries generally present a high level of convergence with EU policies. This group includes countries such as the United States, Australia, Canada, Japan, and South Korea or Norway. The primary focus of engagement with these countries is on coordinating positions to advance a shared vision of future digital policies and cooperating to strengthen their collective capabilities. For instance, the Japan-EU Digital Partnership Council led to the Memorandum of Cooperation on semiconductors.

At the opposite end of the spectrum are the contesters: countries with different worldview that openly challenge the EU's positions and policies. This group includes Russia, China, Iran, and North Korea. Currently, the EU maintains relations only with China and Iran, where digital and cyber issues are part of broader foreign and security policy discussions. The lack of engagement with Russia and North Korea does not mean, however, that the EU has no policies towards these countries.

Between these two extremes are two other groups: champions and newcomers. Champions – including Brazil, India, Kenya, Mexico, Nigeria, and South Africa – actively shape the digital and cyber environment at the regional or international level. They are economic and/or political powerhouses who act as bridge-builders. They do not always share the EU's positions and avoid aligning themselves with contesters. The EU's engagement with these countries usually aims to develop trust, identify common ground for cooperation, and prevent their alignment with contesters. For instance, the EU-India Trade and Technology Council serves as a forum to deepen the strategic partnership linked to geopolitical challenges posed by China's rise.

Newcomers are countries that, for various reasons (e.g., limited capacities, different developmental priorities), have only recently joined the debates about global governance of digital and cyber policies. This category includes a large group of countries in Africa, Latin America,

and the Asia-Pacific. Their growing importance for trade or as political allies places them at the centre of many debates. Consequently, the objective of engagement with these countries is to strengthen their capacities and expertise by sharing lessons and good practices from the EU.

Patchwork of tools and instruments

The EU pursues its relations with partner countries through three different categories of instruments.

The narrowest category comprises cyber- and digital-specific formats like digital partnerships and cyber dialogues. The EU has established Digital Partnership Councils with South Korea, Singapore, and Japan to advance cooperation on specific issues, such as semiconductors, High-Performance Computing (HPC), or platform economy. The EU also conducts cyber dialogues (e.g., with Brazil, China, USA, Ukraine, India) devoted to promoting closer cooperation on standards, supply chain security, combating cybercrime, and responsible state behaviour in cyberspace.

Then come the broader digital cooperation arrangements with partner countries. There is no clear pattern for when the EU opts to use which instrument. Despite clear differences between the United States and India, the EU has opted for the same tool of engagement: a Trade and Technology Council (TTC). TTCs are the EU's instrument of choice for resolving regulatory differences with a partner country. In the cases of Japan and Singapore, the EU opted for Digital Partnerships.

Additionally, the EU has expanded engagements with broader regional blocs. Partnerships like the EU-LAC Digital Alliance, the D4D Hub in Africa, or projects like ESIWA in the Asia-Pacific represent different modalities to engage on digital and cyber globally. More strategic and interest-based engagements with these regions are also a tactical response to geopolitical competition.

The final category comprises mechanisms for mainstreaming digital and cyber issues into broader relations with partner countries, including in areas such as education, justice, law enforcement, agriculture, or climate cooperation. The EU's development and cooperation assistance supports partner countries in achieving their developmental goals. EU funding – including through the Global Gateway initiatives – is used for improving digital infrastructure, strengthening cyber resilience, or enhancing regulatory and institutional frameworks. The EU also funds capacity-building initiatives focused on strengthening partner countries' cyber resilience (Cyber4Dev), combatting cybercrime (GLACY+), and supporting cyber diplomacy capabilities (EU Cyber Diplomacy Initiative).

The increasing economic competition and national security concerns have also highlighted the need to integrate cyber-specific components as a cross-cutting issue in other policy areas (e.g., energy, transportation, or agriculture) and include de-risking elements in digital projects that incorporate cybersecurity technical safeguards to mitigate digital risks.

Conclusions

The EU engages with international partners through various means: negotiations (for agreements, laws, regulation), transgovernmental forums (dialogues, councils), market interactions (standards, market access), and normative discourses (positions in international negotiations).

In this context, third countries can influence the EU at all stages of the policy cycle, from agenda setting to formulation, adoption, implementation, and enforcement. A more in-depth cooperation occurs with the EEA/EFTA countries, which shape the EU's law-making process through comments and notes.

The EU candidate countries, on the other hand, are expected to align their institutional and legal frameworks with the EU. Countries particularly exposed to cyber operations and interference from Russia - Ukraine, Moldova, Georgia, Albania, Montenegro, and North Macedonia – receive particular attention, which gives them informal opportunities to influence the EU.

While the EU's engagement with the like-minded group, the EEA/EFTA countries, and candidate countries is extensive and deep, owing to the EU's history of cooperation, engagement with champions and newcomers presents a challenge. This requires a paradigm shift within the EU.

What concrete steps could the EU take in short- and medium-term?

1. Present a more comprehensive offer for regional champions and newcomers: The EU's current approach is characterised by binary choices between developed-developing and likeminded-contester countries. Despite digital cooperation with African and Latin American regions being a political priority, the EU has yet to sign a digital partnership with any country from these regions. The EU must embrace a diverse geography of interests, translate it into concrete regional engagements and utilise the full spectrum of mechanisms to structure its relations with newcomers and champions from other regions. These engagements should extend beyond capacity building and technical assistance, to include digital partnerships and digital trade agreements. Such agreements are vital to promote specific digital principles and support the developmental objectives of these countries. A series of Regional Digital Action Plans could establish priorities for such cooperation, building on initiatives such as the EU-LAC Digital Alliance or the Policy and Regulation Initiative for Digital Africa (PRIDA).

2. Develop a Global Digital Cooperation Strategy: To promote its vision of a digital future, the EU cannot rely solely on its market power; it needs to invest in alternative ways of engaging with external partners. Individual programmes and policies should not be a substitute for a cohesive strategy. The EU's approach to cyber, digital, technology, and hybrid threats remains largely uncoordinated. The emerging patchwork of instruments and toolboxes gives the impression that the EU lacks a strategy. Such a document could be easily drafted building on the EU's contributions to the UN Global Digital Compact and the existing cyber and hybrid toolboxes. At the same time, the EU should not take the like-minded EEA/EFTA countries for granted and should tap into their respective strengths by expanding cooperation on the implementation of the Cyber Diplomacy Toolbox (CDT). This is particularly pertinent given the anticipated cooperation in the implementation of the CDT. Concurrently, countries like Norway and Switzerland should utilise their formal and informal channels of engagement with EU decision-making. Both Switzerland and Norway have issued national positions on the application of international law in cyberspace, which could contribute to the ongoing work on the EU's own position.

3. Strengthen the EU's capacities in cyber and digital diplomacy: Effective implementation of the EU's cyber and digital policies necessitates adequate resources, including funding and staff. However, several commitments, such as the establishment of a global EU Cyber Diplomacy Network and a well-trained network of digital diplomats, have yet to be fulfilled. For the EU cyber and digital diplomacy to bring results and become competitive towards other big players, it cannot depend solely on the guidance of Brussels-based experts or an extensive use of external consultants. While there have been modest efforts to enhance understanding of cyber and digital issues, adopting a more structured approach to pre- and post-deployment training could significantly address this gap.

Further reading

Barmpaliou, Nayia and Pawlak, Patryk (2023) Operational Guidance. The EU's International Cooperation on Cyber Capacity Building, EU CyberNet, October 2023.

Hofmann, Stephanie and Pawlak, Patryk (2023) "Governing cyberspace: policy boundary politics across organizations", Review of International Political Economy, 30:6, pp. 2122-2149.

This policy brief is based on research conducted in the project "Norway and the EU towards 2030", funded by the Norwegian Ministry of Foreign Affairs.

Patryk Pawlak is a Part-time Professor at the Robert Schuman Centre for Advanced Studies in Florence and a visiting scholar at Carnegie Europe. His fields of expertise are global governance of cyberspace, the impact of technology on foreign and security policy, and the EU's cyber and digital diplomacy.

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

Cover photo: NUPI/Midjourney Bot

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no