Department of European Public Law
University of Zagreb Faculty of Law

Croatian Yearbook of European Law and Policy

ISSN 1848-9958 (Online) | ISSN 1845-5662 (Print)

Journal webpage: https://www.cyelp.com

Digital Diplomacy: The EU as a Global Digital Actor (Editorial Note)

Ramses A Wessel

Suggested citation: RA Wessel, 'Editorial Note: Digital Diplomacy: The EU as a Global Digital Actor' (2025) 21 CYELP [ONLINE FIRST].

DOI: 10.3935/cyelp.21.2025.640

https://www.cyelp.com/index.php/cyelp/article/view/640

https://orcid.org/0000-0002-5594-3757

Editorial note

Ramses A Wessel*

DIGITAL DIPLOMACY: THE EU AS A GLOBAL DIGITAL ACTOR

In the context of rapid technological change and increasing geopolitical instability, the European Union (EU) has sought to redefine its global role through the lens of what has been termed 'digital diplomacy'. Digital diplomacy, as practised by the EU, integrates regulatory influence, cybersecurity initiatives, and artificial intelligence (AI) policy into broader external relations.

Over the past few years, the European Union has emerged as a significant actor in the global digital policy arena, utilising its regulatory power and external relations mechanisms to project values and norms beyond its borders.[1] Although not a State, the EU wields considerable normative power due to its legal personality (Article 47 TEU) and competences in areas such as trade, data protection, and internal market regulation. Articles 3(5) and 21 TEU set out the Union's external objectives: promoting peace, democracy, human rights, and the rule of law. These form the normative backbone of its digital diplomacy,[2] and the 2025 International Digital Strategy for the European Union expressly presents 'Digital as a core element of the EU's external action'.[3]

This editorial note briefly examines how legal frameworks, strategic objectives, and geopolitical shifts shape the EU's external digital engagements. Drawing from EU treaties, institutional strategies, and academic analysis, the aim is to evaluate the coherence and limitations of the EU's digital foreign policy. We will also assess its development through brief case studies in cybersecurity and AI governance. Given the EU's self-declared lag in

---

* Professor of European Law, University of Groningen. This editorial note is partly based on a presentation given by the author during the 'Jean Monnet Seminar on Advanced Issues of EU Law: Modern Technologies and EU Law', Dubrovnik, April 2025.

[1] Elaine Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity* (Hart 2024). In this book, Fahey concludes that the EU has firmly positioned itself as a proactive rule-maker and global norm exporter. Its approach to digital regulation – particularly in data protection – has influenced legal frameworks in many third countries, often prompting them to align with EU standards to facilitate digital trade and data flows.

[2] Uphold and promoting its values and interests and contributing to the protection of its citizens are even formal legal obligations for the EU on the basis of Art 3(5) TEU. In a broader sense, Art 21(1) TEU refers to the principles which inspired the Union's own creation to guide its global actions.

[3] Joint Communication to the European Parliament and the Council, 'An International Digital Strategy for the European Union' JOIN(2025) 140 final.

technological innovation,[4] a key question is what the EU's ambitions are in this field. It is not the objective of this short note to provide an extensive overview of this complex field. Rather, it aims to draw attention to a development that is becoming increasingly relevant: the 'externalisation' of the EU's internal regulation of the digital world as part of its 'digital diplomacy'.

While the EU's digital diplomacy is framed as a values-driven, normative project, its effectiveness in translating internal regulatory power into global influence remains contested. The EU's reliance on 'regulatory power' – rather than technological or military power – raises questions about its ability to shape global norms in a multipolar digital landscape. Can a model built on human rights, democracy, and the rule of law compete with the market-driven pragmatism of the US or the State-controlled digital authoritarianism of China? This note argues that the EU's normative ambitions, while laudable, face structural and geopolitical limitations that may ultimately constrain its global leadership.

Conceptualising EU digital diplomacy

Digital diplomacy has not clearly been defined by the EU. Any conceptualisation therefore needs to be done on the basis of descriptions provided by policy documents and by the relevant literature. It is fair to say that, in general, digital diplomacy refers to the strategic use of digital tools and policies in diplomatic practice. For the EU, this includes the promotion of a rules-based international digital order, the export of normative standards (eg, the GDPR, the AI Act), and partnerships with global actors to counter digital authoritarianism. As articulated by the European External Action Service (EEAS), the EU's digital diplomacy involves engagement with States, international organisations, and private sector stakeholders to shape global digital norms.[5]

On 6 June 2025, the European Commission adopted a Joint Communication on an International Digital Strategy for the European Union, setting out a joint vision for the EU's external action for digital.[6] This Strategy aims to enhance tech competitiveness through cooperation, research, and digital trade agreements. It focuses on strengthening cybersecurity, tackling cybercrime, and securing ICT supply chains. The strategy promotes a values-

[4] See in particular the Draghi Report on EU Competitiveness <https://commission.europa.eu/topics/competitiveness/draghi-report_en> accessed ? One of the responses of the EU was the adoption in 2025 of the EU's 'Competitiveness Compass', Communication on a Competitiveness Compass for the EU, COM(2025) 30 final.
[5] European External Action Service, *Digital Diplomacy for an Inclusive and Sustainable Digital Future* <www.eeas.europa.eu/eeas/digital-diplomacy_en> accessed 14 December 2025.
[6] An International Digital Strategy for the European Union (n 3).

based approach to global digital governance, emphasising human rights and responsible technological advancement.

Reference is made to the 2023 Council Conclusions on Digital Diplomacy.[7] The conclusions mark an evolution towards a holistic, value-driven, and proactive digital foreign policy. While grounded in human rights and democratic values, the strategy balances these with concrete actions on security, technological leadership, and effective international engagement – positioning the EU as both a global standard-setter and a pragmatic international player. The Council conclusions phrase this as follows:

> The Council […] underlines the need for a stronger, more strategic, coherent and effective EU policy and action in global digital affairs to confirm EU engagement and leadership. This is essential to strengthen the EU's strategic autonomy, while preserving an open economy. It requires the EU and its Member States to further develop cooperation with partners around the world, bringing together and leveraging all diplomatic and policy tools, and ensuring complementarity and coherence between internal and external policies.[8]

It is interesting to see that the aims of digital diplomacy combine a need for EU global engagement and leadership, a strengthening of the EU's strategic autonomy,[9] and at the same time an emphasis on multilateralism. The latter element is also strengthened by the EEAS:

> [t]he EU approach to the digital transition is firmly anchored in its commitment to multilateralism and the promotion of universal human rights and fundamental freedoms, the rule of law and democratic principles. The EU, with the full involvement of the Member States, is developing tailored approaches to strengthen cooperation in and with the UN system, the G7, the G20, the OSCE, the OECD, the WTO, NATO, the Council of Europe and other multilateral fora, including multi-stakeholder organisations, and particularly in standardisation bodies, in which coherent and harmonised European standards play an influential role.[10]

Key aspects of digital diplomacy include: *Global Digital Governance* (the EU actively participates in international forums (eg, UN, G7, G20, WTO) to advocate for a rules-based digital order); *Regulatory Influence* (the EU's digital regulations, such as the GDPR and the AI Act, serve as global benchmarks);

---

[7] Council conclusions on EU Digital Diplomacy – Council conclusions approved by the Council at its meeting on 26 June 2023.
[8] Council conclusions on EU Digital Diplomacy (n 7).
[9] See, for instance, for a legal appraisal of strategic autonomy, Eva Kassoti and Ramses A Wessel (eds), 'Strategic Autonomy: The Legal Contours of a Security Policy Construct' (2023) 28 European Foreign Affairs Review, special issue.
[10] EEAS (n 5).

Cybersecurity & Resilience (strengthening global cybersecurity cooperation, combating cybercrime, and promoting digital rights); *Technology & Trade Agreements* (engaging in digital trade policies and partnerships with key allies like the US, Japan, and India);[11] *Countering Digital Authoritarianism* (promoting an open, secure, and free internet while countering disinformation and digital repression);[12] and *Capacity Building* (supporting digital development in emerging economies through initiatives like Global Gateway).[13]

All of this is to be done on the basis of what Anu Bradford has famously described as a 'Rights-Driven Regulatory Model', which focuses on safeguarding individual rights, data privacy, and claims a human-centric, and a fair digital marketplace through strong regulatory frameworks (like the GDPR and the Digital Markets Act).[14] Guided by its own values (compare Article 21 TEU), the EU thus attempts to set global standards for tech regulation, emphasising democratic values and protection against both corporations and the State. Bradford contrasted this model with both the American and the Chinese models. The American 'Market-Driven Model' prioritises economic growth, innovation, and free speech. Regulation is minimal, allowing tech companies significant freedom and influence. The Chinese 'State-Driven Model' positions the State at the centre of digital governance, using technology for political and social control. The government heavily monitors and guides the tech sector, prioritising State interests and surveillance, often at the expense of individual freedoms and data privacy.

It has to be kept in mind, however, that while the EU's 'Rights-Driven Regulatory Model' is often celebrated for its emphasis on human rights, data privacy, and democratic oversight, this model also has evident flaws. First, the EU's regulatory approach risks overburdening innovation with compliance costs, potentially stifling the very technological leadership it seeks to foster. Second, the model's effectiveness depends on the willingness of third countries to adopt EU standards – a process that is far from automatic and often contingent on economic or political leverage. Finally, the EU's normative framework may struggle to address the asymmetrical power dynamics of the digital economy, where a handful of non-European tech giants dominate the

---

[11] See also on the sensitive link between trade and technology Charlotte Beaucillon and Sara Poli (eds), 'Special Focus on EU Strategic Autonomy and Technological Sovereignty' (2023) 8(2) European Papers.

[12] As part of its digital diplomacy efforts, the EU itself has also become much more active with regard to the use of social media. As argued by Zaiotti, 'The EU has recognized that digital platforms are an essential tool in contemporary world affairs for the purpose of communicating and engaging with the outside world, particularly foreign audiences'. See Ruben Zaiotti, 'The European Union and Digital Diplomacy: Projecting Global Europe in the Social Media Era' in Corneliu Bjola and Ilan Manor (eds), *The Oxford Handbook of Digital Diplomacy* (OUP 2024) 457.

[13] See '2025 International Digital Strategy for the European Union' (n 3).

[14] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).

market. The EU's ability to 'export' its values is thus not just a question of legal design, but of geopolitical clout.

All these elements together allow us to loosely define EU digital diplomacy as: *The strategic use of digital technologies – including the internet and social media – to strengthen the EU's global role, protect its strategic interests, advance its regulatory values (such as human rights, rule of law, and democracy), and shape international digital policy and governance, both by conducting diplomatic activities online and by addressing digital issues (like cybersecurity, internet governance, and AI) as key topics in foreign policy.*[15]

Cybersecurity as a diplomatic priority

One key element of digital diplomacy concerns cybersecurity. The EU lacks an explicit treaty basis for cybersecurity, necessitating a piecemeal legal approach.[16] At the same time, the EU has recognised cybersecurity as a strategic priority since the 2013 Cybersecurity Strategy.[17] Subsequent documents, including the 2016 Global Strategy and the 2020 EU Security Union Strategy, emphasise resilience, cooperation, and the integration of cyber elements into the Common Security and Defence Policy (CSDP). Other recent instruments also reveal the ongoing attention the EU pays to this topic: the *2016 NIS Directive*, updated in 2020 as NIS2 (concerning measures for a high common level of security of network and information systems across the Union);[18] the *2019/2025 Cybersecurity Act* (strengthening the role of the European Union Agency for Cybersecurity – ENISA, and providing for a European Cybersecurity Certification Framework – ECCF); the *2024 Cyber Resilience Act* (establishing common standards for products with digital elements, including hardware and software); and the *2024 Cyber Solidarity Act* (improving the preparedness, detection, and response to cybersecurity incidents across the EU).[19] Furthermore, the EU Cyber Diplomacy Toolbox,

---

[15] In their *Oxford Handbook of Digital Diplomacy* (n 12) 3, Bjola and Manor define digital diplomacy in a general, non-EU related, context as: 'the use of digital technologies, such as social media and other online platforms, including virtual communication channels and the metaverse, by ministries of foreign affairs (MFAs) and international organizations (IOs) to communicate with each other and the general public, conduct diplomacy, and advance their foreign policy goals'. Here, much more than in the case of the EU, the emphasis is on communication.

[16] cf Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2018) 56 Journal of Common Market Studies 1259; as well as Ramses A Wessel, 'European Law and Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021) 490.

[17] European Commission Joint Communication, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' JOIN(2013) 01 final.

[18] See in general on the NIS and its implementation: Theodoros Karathanasis, *Cybersecurity and EU Law: Adopting the Network and Information Security Directive* (Routledge 2024).

[19] See respectively Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15; Regulation (EU) 2024/2847 of the

adopted in 2017, aims for the 'further development and implementation of a common and comprehensive EU approach for cyber diplomacy at global level'.[20] This toolbox enables joint diplomatic responses to cyber threats, including the use of targeted sanctions. This latter aspect led, *inter alia*, to the adoption of a Council Decision on restrictive measures against cyber-attacks threatening the Union or its Member States.[21] In 2025, further steps were taken to clarify what a cyber crisis is, what triggers a cyber crisis mechanism at Union level, and how relevant actors should interact and make the best use of available mechanisms in terms of crisis management.[22]

Other publications deal with these instruments in much more detail.[23] For this editorial note, it is particularly important to highlight that, based on various instruments, the growing ambition of the EU as a global cyber actor necessitates a shift from an inward-looking approach to cyber incidents towards a more outward-looking perspective. This signifies a transition from the traditional focus on network defence and resilience-building within the EU to one that promotes and enforces norms beyond its borders. Consequently, it can be noted that, with regard to cybersecurity, the EU's internal rule-making has proven to be inseparable from its external rule-making. While the EU and its Member States[24] are active at the global level to influence the creation of new norms and to set global standards by aiming at a certain harmonisation of the diverging rules,[25] the activities are more visible in regulating the EU's own market, with a keen eye on the protection of fundamental values.

European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L2024/2847; Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) [2025] OJ L2025/38.

[20] Council Conclusions on Cyber Diplomacy (2015) 6122/1511.

[21] Council Decision 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States; and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[22] Commission, 'Proposal for a Council Recommendation for an EU Blueprint on cybersecurity crisis management' COM (2025) 66 final.

[23] See, more extensively, Yuliya Miadzvetskaya and Ramses A Wessel, 'The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox' (2021) 7 European Papers 413; Wessel (n 16).

[24] In the UN framework in particular, it is above all some Member States that participate in discussions of the UN Group of Governmental Experts (UNGGE) on non-binding normative agreements for cyberspace, or in the Open-Ended Working Group (OEWG) open to all UN members. In addition, discussions continue to take place in the Council of Europe in the framework of the Budapest Convention on Cybercrime, <www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 14 December 2025.

[25] As famously analysed by Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2019). See also on the divergence, Tatiana Nascimento Heim and Ramses A Wessel, 'The Various Dimensions of Cyberthreats: (In)consistencies in the Global Regulation of Cybersecurity' (2023) 40 Anales de Derecho 39.

While the EU's cybersecurity strategy thus reflects a commendable shift from reactive resilience to proactive norm-setting, the fragmented legal bases for cybersecurity – spanning internal market regulations, CSDP, and external relations – raise questions about institutional coherence and accountability. Moreover, the EU's emphasis on cyber solidarity and sanctions as tools of digital diplomacy may not be sufficient to deter State-sponsored cyber threats, particularly from actors like Russia or China. The EU's normative power in cybersecurity is further tested by its dependence on US-led intelligence sharing and the limited enforcement mechanisms for its cyber diplomacy toolbox. Without stronger operational capabilities and a unified strategic vision, the EU risks being perceived as a normative actor with limited practical influence.

Artificial intelligence and normative projection

A more novel aspect of digital diplomacy is related to the EU's global role in the regulation of AI.[26] Here also, the story starts with the adoption of internal instruments. The 2024 AI Act is the world's first horizontal AI regulation, adopting a risk-based framework.[27] It prohibits high-risk uses of AI and aims to secure the EU's digital sovereignty. At the same time, the Act is not just an internal instrument, but represents an effort to set global standards by leveraging the EU's internal market power. Indeed, the AI Act has strong extraterritorial ambitions, seeking to influence AI development globally.[28] This is emphasised again in the above-mentioned 2025 International Digital Strategy, as well as in the AI Continent Action Plan, adopted in the same year:[29] 'the EU will continue to engage bilaterally, regionally and multilaterally with trusted partners to attract investments in the EU, support the establishment of a global level playing field for trustworthy AI, and to promote the good governance of AI globally'.

Yet, as argued by Fidato and Lonardo, 'The EU has a problem: it is lagging behind in technological developments on Artificial Intelligence (AI). To solve it, the EU does what it does best: it regulates'. At the same time, 'AI

[26] See, in general, Nathalie A Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (CUP 2025).
[27] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689. Among the many publications on the AI Act, see for a general overview, for instance, Federico Casolari, 'A Constitutionally Oriented Reading of the EU Artificial Intelligence Act' in Luca Mezzetti (ed), *Science, Technology and Law: Mutual Impact and Current Challenges* (Bologna Press 2024) 215.
[28] See. for an extensive analysis, Riccardo Fidato and Luigi Lonardo, 'The Foreign Affairs Aspects of the Artificial Intelligence Policy of the European Union' (2025) 30 European Foreign Affairs Review 11.
[29] Commission, 'AI Continent Action Plan' (Communication) COM(2025) 165 final.

touches virtually any policy, so Brussels' strategy can hardly work internally without a corresponding diplomacy to support it: the AI Act expressly aims at providing the EU with a strong *regulatory* basis to set a new *global* standard, with a view to achieve digital sovereignty'.[30]

The European Union has indeed progressively developed a regulatory stance on AI through various strategic initiatives. In April 2018, the European Commission published a comprehensive strategy on AI, focusing on boosting technological capacity, preparing for socio-economic disruptions, and defining an ethical framework based on EU values. This strategy already highlighted the importance of international cooperation based – as often – on the EU's idea that it 'can lead the way', in this case 'in developing and using AI for good and for all, building on its values and its strength'.[31] The 2020 White Paper on AI systematised previous efforts and introduced the EU's dual-track approach: aiming for 'excellence and trust'.[32] The AI Act, which entered into force on 1 August 2024, aims to deliver on the trust element and was adopted under the internal market provision Article 114 TFEU, emphasising the harmonisation of rules for AI technologies to ensure the proper functioning of the internal market.

Since the start of the current European Commission in December 2024, the EU has shifted its focus towards positioning itself as a global leader in AI capabilities and uses, as outlined in the above-mentioned Competitiveness Compass. This document emphasises AI industrial uptake, research and innovation, and boosting supercomputing capacity as key enablers of global AI leadership. In April 2025 the Commission launched the *AI Continent Action Plan*, a plan that set the path for Europe to become a global leader in AI.[33] This was followed in the autumn of 2025 by the *Apply AI* and the *AI in Science* strategies as the next steps in delivering this ambition and in positioning the EU to accelerate the use of AI in key sectors and science.[34] Indeed, these are not just internal instruments, but together with the AI Act are meant to allow the EU to become more of an assertive and influential global rule-maker in this area.

At the same time, the AI Act's success hinges on two critical, and uncertain, factors: compliance and competitiveness. First, the EU's ability to enforce its standards beyond its borders is untested, particularly in jurisdictions where local regulations conflict with EU norms. Second, the Act's stringent requirements may disincentivise innovation within the EU, further

---

[30] Fidato and Lonardo (n 28) 11–12.
[31] Commission, 'Artificial Intelligence for Europe' (Communication) COM(2018) 237 final.
[32] Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' [2020] COM(2020) 65 final. See also Fidato and Lonardo (n 28) at 17.
[33] Commission, 'AI Continent Action Plan' (Communication) COM(2025) 165 final.
[34] Commission, 'Apply AI Strategy' (Communication) COM(2025) 723 final; and Commission, 'A European Strategy for Artificial Intelligence in Science: Paving the way for the Resource for AI Science in Europe (RAISE) (Communication) COM(2025) 724 final.

widening the technological gap with the US and China. The EU's normative leadership in AI governance is thus a double-edged sword: it may set global benchmarks for ethical AI, but it could also marginalise European players in the global AI race. The EU must therefore strike a delicate balance between regulatory rigour and technological pragmatism if it is to achieve its dual goals of ethical leadership and digital sovereignty.

Conclusion: challenges and limitations

Digital diplomacy has become a core component of the EU's external actions, reflecting its broader ambition to be a normative power in global digital governance. The governance and regulation of digital issues are developing strongly, partly due to their close relation to global cooperation in other areas, such as trade. Irrespective of the patchwork of soft- and hard-law instruments and cross-sectoral strategies, rather than a coherent, unified legal framework, digital diplomacy has emerged as a central component of the EU's external action. The governance and regulation of the digital sphere is evolving rapidly, driven in part by its close interconnection with other domains of global cooperation, such as trade.

Furthermore, the evolution of the EU's regulatory digital framework is increasingly characterised by what may be termed the 'externalisation' of its internal digital regime. The growing number of threats originating from actors in third countries and the risks connected to the misuse of AI have compelled the integration of digital elements into the Union's external policies, including its foreign and security policy.

While the EU has registered important successes – particularly in establishing global regulatory standards – it must address institutional and legal fragmentation if it is to fulfil its full potential. As digital threats continue to evolve and strategic competition intensifies, the Union may find it necessary to recalibrate some of its foundational principles to ensure greater agility and coherence in its external digital policies. Yet, as Ursula Von der Leyen stated in her State of the Union speech in September 2025: 'Whether on environmental or digital regulation. We set our own standards. We set our own regulations. Europe will always decide for itself'.[35] That starting point seems important for the Union to continue playing the normative role that it has chosen for itself.

It is clear that digital diplomacy has now become an integral part of the EU's external relations machinery. The Union aspires to play a leading role in shaping technology governance, including through global standard-setting. Cybersecurity and artificial intelligence serve as notable examples of its

[35] 2025 State of the Union Address by President von der Leyen, 9 September 2025.

activity in this domain. While the EU's traditional reliance on regulation is not the only factor causing its inability to lead in technological innovation and to act swiftly and effectively,[36] the developments seen in 2025 do reveal a certain change of policy and perception. The coming years will show whether the EU is capable of achieving its digital ambitions, and its future success seems to depend on addressing three key challenges. First, the EU must bridge the gap between regulatory power and technological leadership. Without a robust industrial base in digital technologies, the EU's normative influence risks being perceived as hollow. Second, the EU needs to reconcile its multilateral aspirations with geopolitical realities. In a world where digital governance is increasingly shaped by US-China rivalry, the EU's commitment to multilateralism may be tested by the need for strategic alliances and pragmatic compromises. Finally, the EU must demonstrate agility in adapting its digital policies to rapidly evolving threats, from AI-driven disinformation to cyber warfare. The EU's normative model is not inherently flawed, but its effectiveness will ultimately depend on the Union's ability to translate its values into action – and to do so with the speed and flexibility that the digital age demands.

Suggested citation: RA Wessel, 'Editorial Note: Digital Diplomacy: The EU as a Global Digital Actor' (2025) 21 CYELP VIII.

[36] Bradford argued that the relation between digital regulation and technological progress is considerably more complex than what is usually seen in public debates. The entire legal and technological ecosystem in Europe is simply different from the one in, for instance, the US. See Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024), 118(2) Northwestern University Law Review.