European Digital Leadership on the Global Stage

by Dimitar Lilkov

Summary

In recent years the EU has tried to solve some of the most complex challenges when it comes to protecting user privacy, fighting disinformation and regulating complex artificial intelligence systems. However, being the first to draft the rule book does not imply international digital leadership by default. If the EU wants to truly safeguard its values and social market economy principles in the online domain, it needs to leverage its cross-continental potential and engage in a proactive agenda with allies and international partners. Importantly, our Union also needs to develop novel policy tools to fortify its own resilience and to be able to respond to external threats from both state and non-state actors. An expanded strategic agenda for international engagement, digital partnerships and tangible European investment in digital infrastructure abroad needs to be a priority concern. This paper sketches the three main avenues for ensuring European leadership on digital matters internationally.

Keywords Digital deterrence – Cybersecurity – Digital infrastructure – Technical standardisation – China – Data – Privacy

Introduction

There is a spectre haunting Europe's digital ambitions—that of complacency. European member states are quite aware that the continent is not the global front-runner in venture capital and breakthrough innovation. As the story goes, our European pastures do not have as many digital unicorns as those in the US, as a risk-averse entrepreneurial culture and a fragmented single market remain persistent handicaps. There have been a series of high-level reports dealing with these and related issues in sufficient detail.[1] These problems are well recognised, even if the policy prescriptions vary.

Complacency comes in a different form. For almost a decade, the EU has positioned itself as the engine of model regulation for the digital realm—a trend-setter in shaping laws fit for the digital age. How do we safeguard personal privacy? Are there legal safeguards for consumer protection and fundamental rights online? Do we have a blatant economic cartel of several California-based technological companies monopolising online search, retail and social media, and how should we to respond to that? These are all valid concerns which have engendered a whole gamut of EU-led initiatives and binding legislation. Acronyms such as GDPR, DSA, DMA and the AI Act[2] have become household names in the policy circles of Brussels, Washington and Beijing. The ambition was there and the product is already here.

However, EU institutions continue to cling to the narrative that they have put in place the gold standard for digital legislation, a product ready for export. Through soft power and the 'Brussels effect',[3] these rules and norms are said to positively influence other markets and peoples globally. The EU's track record and ambition is undeniable. But it would be premature to assume that European leadership on the global stage is guaranteed. In the upcoming legislature Brussels should not rest on its laurels if it actually wants to project influence and ensure mutual gain in the digital economy.

1 European Commission, *The Future of European Competitiveness: Part A – A Competitiveness Strategy for Europe* (Brussels, 2024); E. Letta, *Much More Than a Market, Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens* (Brussels, 2024).

2 Respectively, the General Data Protection Regulation (2016), the Digital Services Act (2022), the Digital Markets Act (2022) and the Artificial Intelligence Act (2024).

3 A. Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

This paper focuses on the new political mandate (2024–9) held by the EU institutions and provides a blueprint for strengthening Europe's global leadership in the digital arena. If the EU wants to truly safeguard its values and social market economy principles in the online domain, it needs to leverage its cross-continental potential and engage in a proactive agenda with its allies and international partners. Importantly, our Union needs to develop novel policy tools to fortify its own resilience and to be able to respond to external threats from both state and non-state actors. The international appeal of Europe's digital profile needs to come from a position of strength and accomplishment, not just from regulatory ambition and bureaucratic wit.

Digital deterrence and economic security

This concept has three pillars. First, the EU must upgrade its blueprint for digital deterrence. The EU has a limited number of supranational tools for responding to external trade or economic coercion, and an under-developed defensive arsenal for dealing with malign digital threats. This situation is explained by the history and dynamics of European integration over the last several decades, during which the EU positioned itself as one of the champions of multilateralism and free trade in times of relative peace, liberalised global trade and shared optimism about the benefits of globalisation. Moreover, unlike the US, the EU has never shaped or enforced its economic and international policies through the prism of safeguarding 'national security'.

The European Commission needs an improved mandate to implement security standards for critical digital infrastructure and to prohibit high-risk vendors from penetrating sensitive networks. The Commission initiative on secure 5G networks[4] across the EU aimed to lay the foundations for a coordinated European approach based on a common set of measures to mitigate the main cybersecurity risks posed by such networks. Standardisation, certification schemes, network security and scrutiny of untrusted suppliers were considered in detail. In 2023 the Commission went the extra mile and even labelled Chinese companies Huawei and ZTE 'untrusted vendors',[5] recommending their restriction and prohibition across the EU. Problematically, as of late 2024, only 11 EU member states have taken prohibitive measures against untrusted Chinese infrastructure.[6]

Network security and cyber deterrence cannot be determined only by economic justification or political favouritism. Having 'clean' networks, or as limited hostile access to internal communications infrastructure as possible, is of both national and supranational concern. Having an appealing international model for online governance presupposes control over critical infrastructure and communication flows. Neither of these is currently guaranteed. With its new mandate, the European Commission should create an expanded toolkit to limit the threats from compromised information and communications technology infrastructure and products/services which serve the purposes of foreign adversaries. In this case, the enhancement of supranational tools would not be driven by federalist zeal but rather by practical necessity.

The legislative backbone for this is actually in place, but it has not been implemented accordingly. The GDPR offers a case study of good intentions and comprehensive norm-setting, but with restricted options for pan-European implementation. From the limited staffing or administrative resources given to national authorities to the fact that certain data protection authorities are handling a disproportionate number of cases,[7] much is left to be desired on enforcement. Ireland has made a mockery of the rules by disregarding or postponing dozens of pertinent cases against American multinational companies,[8] which have directly benefited from the Irish regulator's negligence.

4 European Commission, 'EU Toolbox for 5G Security', Cybersecurity Toolbox Factsheet (Brussels, 2021).
5 T. Breton, '5G Security: The EU Case for Banning High-Risk Suppliers', European Commission, Press Release, 15 June 2023.
6 C. Kroet, 'Eleven EU Countries Took 5G Security Measures to Ban Huawei, ZTE', *Euronews*, 12 August 2024.
7 J. Ryan and A. Toner, *Europe's Governments Are Failing the GDPR*, Brave (May 2020).
8 V. Manacourt, 'Ireland Frets as Criticism Over Big Tech Links Goes Mainstream', *Politico*, 16 December 2021.

The novel DSA provides an 'upgraded' toolkit but much remains to be seen in terms of its effectiveness in practice. The attempt to expand the Commission's mandate and create true supranational supervision of issues related to online platform governance is an important improvement. However, it is down to the national capitals to allocate the qualified administrative staff and coordination capacity to oversee the extremely complicated technical and legal compliance cases. Legislation such as the DSA needs to have enforcement muscle. For example, online services or digital applications that are deemed to act on behalf of a foreign adversary or secretly condone its malign operations should be subject to supranational review and a potential ban. Overall, the EU needs to provide workable solutions for transforming its legally established values into verifiably testable criteria for technology.[9]

The mass-market penetration of affordable foreign (often Chinese) interconnected Internet-of-Things devices may be beneficial for European users, but carries many risks. The EU needs to finalise progress on the Cyber Resilience Act and expand its efforts on the bolstered cybersecurity requirements for software and hardware products. In 2020 the EU invoked its cyber-diplomacy tools for the first time and imposed sanctions against Russian and Chinese individuals for conducting malicious cyber-attacks. The EU must stand ready to counter such malicious behaviour in cyberspace and have the necessary mechanisms in place to prevent, deter and respond to external threats in the digital domain. Closer transatlantic cooperation is needed to meet these challenges, together with an extension of NATO's capabilities to defend Allies in cyberspace.

Lastly, the EU needs to improve its cross-sectoral coordination and follow up on its own agenda for economic security. In late 2023 the Commission mapped the path forward with a series of new initiatives that aim to reinforce European economic security while also preserving high trade and investment flows.[10]

Improving the screening of foreign direct investment (FDI) and ensuring better alignment between member states on export control policies should be the basis for any serious attempt to introduce (quasi-)federal economic security guardrails. The upcoming review of the current regulation on FDI screening[11] offers the possibility of ensuring that European institutions have the competence to intervene if certain external investments affect joint security interests or concern critical infrastructure. The new political legislature should also explore various avenues for scaling technological research and create opportunities for funding European programmes that could have defence or military applications, not only civil ones. The EU should acknowledge that other global actors such as the US and China are pursuing their own strategies of military–civil fusion, whereby defence companies, universities and research institutions are collaborating on breakthrough innovation.

International engagement

As a second pillar, the EU needs to expand its digital outreach internationally. Within this decade, the European institutions need to deepen strategic engagement on technology and multiply the number of agreements in place. In 2021 the EU and the US officially launched a Trade and Technology Council (TTC) with the aim of coordinating approaches to key global trade, economic and technology issues, as well as deepening transatlantic trade ties.[12] The overall setup and technical modus operandi of the TTC has provided a model that could be replicated with other global actors. In 2023 Brussels hosted the first EU–India Trade and Technology Council,

[9] A. Andersdotter, 'Rolling Out Secure Digital Infrastructure and Hardware', in P. Hefele, K. Welle et al. (eds.), *The 7Ds for Sustainability: In Depth,* Wilfried Martens Centre for European Studies (Brussels, June 2024), 122.

[10] European Commission, *Advancing European Economic Security: An Introduction to Five New Initiatives*, Communication, COM (2024) 22 final (24 January 2024).

[11] European Parliament and Council Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, OJ L791 (19 March 2019), 1.

[12] The next section of this paper deals more specifically with the transatlantic partnership and the EU–US TTC in particular.

which focused on deepening strategic engagement on trade and technology with the Asian country.[13] The expanded digital dialogue with New Delhi focuses on strategic technologies, clean tech, trade and resilient value chains. This effort is seen as an attempt to explore topics of mutual concern in digital areas, as well as expanding the strategic autonomy of both countries and reducing dependencies on external actors, such as China and Russia.[14]

Within the next political legislature, the European institutions need to deepen and expand such dialogues and ensure they provide tangible outcomes on an annual basis. Issues related to quantum technology, artificial intelligence (AI) governance or advanced semiconductor supply chains cannot be tackled by individual member states in isolation. The EU has already taken the first steps by holding a Digital Partnership Council with Canada, Japan, South Korea and Singapore. These initiatives need to be maintained and expanded. Such a proactive international agenda will produce positive spillovers, enhancing bilateral trade, reinforcing strategic supply chains and opening up new market opportunities for European companies. The conventional tools of diplomacy will bring fewer and fewer returns unless coupled with digital dialogues and expanded synergies on international tech cooperation. Brussels prides itself on exporting digital legislation, but let us not forget the importance of actually exporting European digital goods and services internationally.

Similar ambitious and transparent initiatives should urgently be developed and implemented in Africa with specific partner countries. Investment in connectivity and European support for the rollout of secure digital infrastructure and societal digital transformation form one of the main pillars of the EU–African Union Joint Vision for 2030.[15] European member states need to keep the momentum going and meet the current pledges in order to fully commit to the renewed partnership with the African continent.

On a parallel (and more niche, technical) front, EU member states need to allocate sufficient time and resources to promoting European technical standards internationally. A proactive agenda for a 'race to the top' on technology entails that the EU's partners have a viable strategy on this level. This is especially pertinent given the People's Republic of China's targeted agenda to influence international standards-setting bodies such as the International Organization for Standardization, the International Electrotechnical Commission and the UN's International Telecommunications Union. For years now, China has pursued a strategy of exporting its own digital standards, ranging from facial-recognition software to 5G, through bi- and multilateral agreements and initiatives.[16] This seemingly technical approach is part of China's wider agenda to promote digital sovereignty and the export of its digital authoritarianism toolkit globally.[17] European partners needs to buttress their representation, financing and strategic interests in the above-mentioned standards-setting bodies. Global democracies need to be working in close cooperation to provide a true liberal, multi-stakeholder approach to online governance and standardisation.

Last but not least, the EU needs to build. Global partnerships should not only be about norms and regulations, but should also leave a tangible mark. In the upcoming political legislature, European policymakers need to deliver on their ambitious pledge to support developing countries with the rollout of secure digital infrastructure, clean energy and improved connectivity. The EU is the biggest global donor of development aid, contributing

[13] European Commission, 'First EU–India Trade and Technology Council Focused on Deepening Strategic Engagement on Trade and Technology', Press Release, 16 May 2023.
[14] P. Moralez and R. Ricart, *The EU–India Trade and Technology Council: Opportunities and Challenges Ahead,* Elcano Royal Institute (Madrid, February 2023).
[15] European Council, '6th European Union—African Union Summit: A Joint Vision for 2030', Joint statement (Brussels, February 2022).
[16] C. Amon and O. Wientzek, *China's Growing Importance in International Standardisation Organisations*, Konrad Adenauer Stiftung (Geneva, April 2022).
[17] D. Lilkov, *Made in China: Tackling Digital Authoritarianism*, Wilfried Martens Centre for European Studies (Brussels, February 2020), 47–52.

approximately 50% of the world's total, but it needs to be more focused and strategic in its allocations.[18] The much anticipated Global Gateway initiative has pledged up to €300 billion to 2027 for connectivity projects on various continents. This is an opportunity not only to improve infrastructure projects but also to respond to the growing investment gap in climate action and clean energy in Africa, Latin America and Asia. There is also an opening for the EU to reform its own approach to development policy and to explore novel approaches to transparent and efficient project funding.[19]

This is particularly pertinent as China's own global development initiative, the Digital Silk Road, part of its larger Belt and Road Initiative, has gained traction (and notoriety) in the last half decade.[20] The Belt and Road Initiative and its spillover projects span Asia and even reach Europe, aiming to provide fresh funding for digital, energy, maritime and railway infrastructure. Recent studies have shown that this approach aims to provide fast-track (i.e. easy) funding to low-income countries in return for political concessions, debt dependencies, or outright Chinese ownership of assets or strategic infrastructure.[21]

A healthy dose of realism and focus on strategic interests are desperately needed to outweigh policy inertia. The sincere expectation that European soft power and good intentions alone will suffice in the international digital arena is nothing but a false promise.

Escalating risks and challenges require transatlantic solutions

When it comes to the international dimension, the transatlantic alliance remains a key pillar for Europe's digital agenda. Some of the most pressing international issues, such as developing international technological standards, securing supply chains for advanced technology, curbing devastating cyber-attacks and implementing export controls on dual-use technological items with military applications, can only be tackled if Brussels and Washington maintain and enhance their ambitious partnership. In this regard the expanded EU–US TTC could be a vital tool for pursuing an ambitious joint agenda while also expanding bilateral trade. The current trade patterns surpass €100 billion annually in digital goods and services. The TTC has already made progress on items such as trustworthy AI, supply-chain monitoring and joint standards for electric vehicles (EVs). An additional effort is needed to grow this joint agenda and turn the TTC into an expanded supranational mechanism for transatlantic deliberation and decision-making.

In its three years of existence, the TTC's concrete outputs remain minimal, consisting mostly of a plethora of dialogues, principles and roadmaps. It has published a Joint AI Roadmap, a set of Principles for Child and Youth Protection Online, a Declaration on the Future of the Internet and a stakeholder dialogue on green tech. An agreement on a common standard for EV charging ports represents one of the few concrete deals. The EU should attempt to deepen and streamline the EU–US TTC and increase its institutional leverage. Improved working groups and increased stakeholder engagement are needed to boost the overall format. This also entails the expansion of joint work on early warnings with regard to the security of semiconductor supply chains.

Cooperation on export controls on dual-use items with advanced military applications is a long-term joint priority. This is urgent, especially in the wake of the unilateral, extraterritorial export controls regime imposed on exports of advanced computing components and semiconductors to China in October 2022 by the US

[18] S. Tagliapietra, 'The European Union's Global Gateway: An Institutional and Economic Overview', *The World Economy* 47/4 (April 2024).
[19] P. Hefele and S. Crooks, *The Future of European Development Cooperation: A Centre–Right Perspective*, Wilfried Martens Centre for European Studies (Brussels, 2024).
[20] J. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021).
[21] N. Clark, *The Rise and Fall of the BRI*, Council on Foreign Relations (April 2023).

Bureau of Industry and Security. This unilateral act by the US had direct implications for EU member states as the Netherlands was under heavy political pressure to join the control regime and limit Dutch exports of specific lithographic equipment.

Transatlantic efforts on intelligence cooperation and preventing the grave misuse of technology which threatens joint security should be streamlined, regardless of who is running the future US presidential administration. Within the next legislature, Brussels and Washington need to upgrade EU–US coordination on handling the potential risks of the proliferation of AI and biotechnologies. Both economic blocs need to align better on terminology and risk mitigation, even if they pursue their own domestic regulatory agendas on digital governance. Both need to continue their efforts and expand the current G7 Hiroshima Process on AI in order to work towards a multilateral framework which provides sufficient guardrails against the misuse of foundational models and the weaponisation of advanced technology.

The transatlantic relationship remains key to maintaining robust international alliances on securing strategic supply chains and streamlining the exchange of critical raw materials and rare earth elements, which are of great importance for the clean energy transition. In this regard, Brussels and Washington need to make progress on finalising a joint agreement on critical raw materials, similar to the one concluded between the US and Japan in 2023. In pursuit of the joint commitment to free trade, the transatlantic alliance also needs to set up a green marketplace[22] by eliminating tariffs and non-tariff barriers to the expanded free trade of clean-energy technologies, batteries, EVs and related hardware.

It is important to note that even though there are huge overlaps in EU–US interests in the digital sector, Europe pursues a different philosophy when it comes to privacy protection and digital market setup. None of these above-mentioned positive initiatives should be used as a pressure point to water down European tech regulation and data governance. EU–US tech relations have been hampered by a lack of trust when it comes to data sharing since the European Court of Justice stated in 2020 that the US does not provide sufficient guarantees for the protection of personal data coming from the EU.[23] Thus the US needs to provide a viable and trusted mechanism that ensures that Europe's provisions are being met, and not just vague reassurances that this is the case.

Unfortunately, for a long time now, many European capitals have been resigned to the idea that a few American digital companies will continue to dominate search, direct messaging, social media and retail across the EU. The European member states should commit to a stricter approach to curbing the monopolistic practices of many of these platforms, which have been confirmed as such by several cases brought before the European Court of Justice and the US Department of Justice.

[22] A. Mettler, 'Europe Lost to China on Solar—Now It's About to Do the Same With Wind', *Politico*, 11 August 2023.
[23] A. Lee, 'The European Court of Justice Has Ruled That Privacy Shield Is Invalid, *WIRED,* July 2020.

	Programme 1	Programme 2	Programme 3
	Ensuring the digital deterrence of external threats	**Engaging internationally**	**Enhancing the transatlantic tech partnership**
Project 1	Exclude high-risk vendors from building and servicing Europe's critical digital infrastructure (e.g. 5G). Expand the Commission's mandate to implement a common strategy on network security and mitigation measures.	Expand cross-border data agreements and technology dialogues with allies and international partners. Deepen strategic engagement on safeguarding technological supply chains, joint research and development in advanced technologies, and boosting trade.	Finalise the EU–US agreement on critical raw materials. This will limit supply-chain risks and open up the US market to EU clean-energy components and EVs. Establish a transatlantic green marketplace by eliminating tariffs and non-tariff barriers to the expanded free trade of clean-energy technologies, batteries, EVs and related hardware.
Project 2	Coordinate action between member states and the Commission on strictly enforcing the DSA and its provisions on fighting disinformation and the dissemination of illegal content. Expand the DSA to include harmonised standards for software/app security. Include the option for the Commission to flag certain applications or software services as 'malign' or as going against predefined European standards.	Engage with international standards-setting bodies (i.e. the International Organization for Standardization, the International Electrotechnical Commission) and the UN (i.e. the International Telecommunications Union) to promote European digital standards. Oppose China's agenda to influence these standards-setting bodies. Through partnership and international influence, the EU needs to actively oppose the spread of digital authoritarianism, unlawful online surveillance and digital profiling. European legislative frameworks such as the GDPR, DSA and AI Act need to serve as global templates.	Deepen and streamline the EU–US TTC. Improved working groups and increased stakeholder engagement are needed to boost the overall format. Expand work on early warnings with regard to the security of semiconductor supply chains. Adopt joint standards on EVs and clean technologies.
Project 3	Strengthen FDI screening with improved, harmonised national rules. Expand the Commission's competence to intervene if certain external investments affect joint security interests or concern critical infrastructure.	Leverage the EU Global Gateway Initiative through enhanced investment packages for Africa, Latin America and the Caribbean which include strategic projects on advanced and secure digital infrastructure. Open up new market opportunities for European businesses to build, support and maintain secure infrastructure and provide digital services abroad.	Cooperate on export controls on dual-use items with advanced military applications. Improve transatlantic efforts on intelligence cooperation and preventing the grave misuse of technology which threatens joint security. Improve EU–US coordination on handling the potential risks of the proliferation of AI and biotechnologies. Both economic blocs need to align better on terminology and risk mitigation, even if pursuing their own domestic regulatory agendas.

Bibliography

Amon, C. and Wientzek, O., *China's Growing Importance in International Standardisation Organisations*, Konrad Adenauer Stiftung (Geneva, April 2022), accessed at https://www.kas.de/documents/6419516/12332519/Chinas+growing+importance+in+international+SDOs.pdf/b94b7af6-7afc-84bc-b360-7491b4642728?version=1.0&t=1655823730794 on 7 November 2024.

Andersdotter, A., 'Rolling Out Secure Digital Infrastructure and Hardware', in Hefele, P., Welle, K. et al. (eds.), *The 7Ds for Sustainability: In Depth*, Wilfried Martens Centre for European Studies (Brussels, June 2024), 122–3, accessed at https://www.martenscentre.eu/publication/the-7ds-in-depth/ on 7 November 2024.

Bradford, A., *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

Breton, T., '5G Security: The EU Case for Banning High-Risk Suppliers', European Commission, Press Release, 15 June 2023, accessed at https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3312 on 4 November 2024.

Clark, N., *The Rise and Fall of the BRI*, Council on Foreign Relations (April 2023), accessed at https://www.cfr.org/blog/rise-and-fall-bri on 7 November 2024.

European Commission, *Advancing European Economic Security: An Introduction to Five New Initiatives*, Communication, COM (2024) 22 final (24 January 2024), accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0022 on 7 November 2024.

European Commission, 'EU Toolbox for 5G Security', Cybersecurity Toolbox Factsheet (Brussels, 2021).

European Commission, 'First EU–India Trade and Technology Council Focused on Deepening Strategic Engagement on Trade and Technology', Press Release, 16 May 2023, accessed at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2728 on 7 November 2024.

European Commission, *The Future of European Competitiveness: Part A – A Competitiveness Strategy for Europe* (Brussels, 2024), accessed at https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en on 7 November 2024.

European Council, '6th European Union—African Union Summit: A Joint Vision for 2030', Joint statement (Brussels, February 2022), accessed at https://www.consilium.europa.eu/media/54412/final_declaration-en.pdf on 7 November 2024.

European Parliament and Council Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, OJ L791 (19 March 2019), 1.

Hefele P. and Crooks, S., *The Future of European Development Cooperation: A Centre–Right Perspective*, Wilfried Martens Centre for European Studies (Brussels, 2024), accessed at https://www.martenscentre.eu/publication/the-future-of-european-development-cooperation-a-centre-right-perspective/ on 7 November 2024.

Hillman, J., *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021).

Kroet, C., 'Eleven EU Countries Took 5G Security Measures to Ban Huawei, ZTE', *Euronews*, 12 August 2024, accessed at https://www.euronews.com/next/2024/08/12/eleven-eu-countries-took-5g-security-measures-to-ban-huawei-zte on 7 November 2024.

Lee, A., 'The European Court of Justice Has Ruled that Privacy Shield Is Invalid', *WIRED*, 16 July 2020, accessed at https://www.wired.com/story/privacy-shield-ruling/ on 7 November 2024.

Letta, E., *Much More Than a Market, Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens* (Brussels, April 2024), accessed at https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf on 7 November 2024.

Lilkov, D., *Made in China: Tackling Digital Authoritarianism*, Wilfried Martens Centre for European Studies (Brussels, February 2020), accessed at https://www.martenscentre.eu/publication/made-in-china-tackling-digital-authoritarianism/ on 7 November 2024.

Manacourt, V., 'Ireland Frets as Criticism Over Big Tech Links Goes Mainstream', *Politico*, 16 December 2021, accessed at https://www.politico.eu/article/ireland-frets-criticism-over-big-tech-links-goes-mainstream/ on 7 November.

Mettler, A., 'Europe Lost to China on Solar—Now It's About to Do the Same With Wind', *Politico*, 11 August 2023, accessed at https://www.politico.eu/article/solar-power-china-europ-now-its-about-to-do-the-same-with-wind/ on 7 November 2024.

Moralez, P. and Ricart, R., *The EU–India Trade and Technology Council: Opportunities and Challenges Ahead*, Elcano Royal Institute (Madrid, February 2023), accessed at https://www.realinstitutoelcano.org/en/commentaries/the-eu-india-trade-and-technology-council-opportunities-and-challenges-ahead/ on 7 November 2024.

Ryan, J. and Toner, A., *Europe's Governments Are Failing the GDPR*, Brave (May 2020), accessed at https://brave.com/blog/dpa-report-2020/ on 4 November 2024.

Tagliapietra, S., 'The European Union's Global Gateway: An Institutional and Economic Overview', *The World Economy* 47/4 (April 2024), 1326–35, accessed at https://onlinelibrary.wiley.com/doi/10.1111/twec.13551 on 7 November 2024.