Digitalisation

Table of abbreviations

5 G	Fifth generation technology standard for cellular networks
AI	Artificial Intelligence
APIs	Application programming interfaces
ARCEP	Autorité de régulation des communications électroniques
CEE	Central and Eastern Europe
CMU	Capital Markets Union
DSA	Digital Services Act
DSM	Digital Single Market
EV	Electric Vehicle
Fintech	Financial technology
FDI	foreign direct investment
GDPR	General Data Protection Regulation
GPAI	general purpose AI
ICT	Information and Communication Technologies
O-RAN	Open Radio Access Network
R&D	Research and Development
SME	Small and Medium Sized Enterprise
STEM	Science, Mathematics, Engineering and Mathematics
TTC	Trade and Technology Council

Introduction

by Peter Hefele

Alongside the Green Deal and the first steps towards a Defence Union, creating a single European digital space was a key project of the outgoing European Commission (2019–24). This involved establishing an interconnected set of rules and regulations aimed at creating a level playing field for competition among European and international companies, enhancing the rights of Europe's 'digital citizens', protecting the integrity of democratic institutions and processes, and promoting global cooperation in the digital sphere.

Digitalisation is now seen as a key enabler that will lay the foundation for Europe's future value creation. The success of this project will also determine the geopolitical weight of the Union vis-à-vis major competing powers such as the US and China. From a novel approach to artificial intelligence governance to a revamped understanding of competition law in the digital domain, the EU's ambitions are high. Yet, piecemeal legislation and the lack of a fully integrated digital single market have led to inconsistent regulation, infrastructure gaps, a lack of investment and security-related issues in its digital sphere.

Many European tech companies are struggling to offer their services outside national borders and to expand their reach to a genuinely European (and global) customer base. To survive in a world where the US and China and their digital giants dominate international competition, the EU needs not only up-to-date regulations that create a fair and level playing field and protect the interests of European citizens but also a strong industrial base. The EU must ensure the production and importation of next-generation semiconductors, joint European funding for breakthrough research and development, and access to secure global supply chains. These goals cannot remain aspirations but must be realised. The resilience of hardware infrastructure and software services throughout the EU is more than a mere technical concern: it impacts the security of sensitive user data, intellectual property rights and national security. At the same time, Europe needs a new culture of risk-taking and entrepreneurship to unleash the innovation potential of digitalisation in the fields of the green transformation and healthcare. Digitalisation is also helping to overcome regional disparities within Europe and is enabling new growth, particularly in the Central and Eastern European countries.

The EU needs to boost its internal connectivity and digital excellence, and prepare for the ever-expanding global threats from hostile actors, malicious digital applications and state-led malign influence on online campaigns. When it comes to international partnerships, 'coopetition' will be the modus operandi of those countries that are part of the global democratic alliance. At the same time, efforts continue to be made to find a global consensus on the general principles for the use of artificial intelligence.

Rolling out Secure, Resilient Digital Infrastructures for Europe

by Amelia Andersdotter

Summary

The EU has a number of opportunities in the field of cybersecurity. By investing in competitive research and leveraging capital from the west and talent from the east, the EU could establish itself as a global stronghold of innovation in cybersecurity and privacy technologies. Consistent and coherent governance, combined with competitively organised markets and standardisation, could ensure that European values are imbued not just in local technological projects, but in the global economy as well.

Keywords 5G – Standardisation – Cybersecurity – Securities – Privacy – Innovation

Introduction

The EU is an end-destination market for information and communication technology (ICT). From hardware design and manufacture to software service conceptualisation and implementation, Europe, its companies and its public institutions are dependent on other regions. To manage this complex cyber-environment with its fragile logistical chains, the EU needs to agree on a proactive cyber strategy. Cloud infrastructures, the Internet of Things and 5G/6G networks are all expected to enable industrial and administrative efficiency. Meanwhile, establishing and protecting EU sovereignty and leadership will require a combination of *ex ante* measures (certifications, standards and capacity), *ex post* measures (procurement, research and enforcement) and governance (consistency, law and regulation, and strategic development).

Building a complete European digital market must involve synergising access to capital and manufacturing in the west with the product- and service-development skills of the east. The reasons for this are not only related to equitable and fair growth in the Union, but are also practical. EU member states must increasingly coordinate their actions across policy fields such as climate change, security policy and strategic manufacturing, and will run up against the challenge that a certain level of institutional stability and experience, as well as domestic capital, is necessary to make these adjustments. When such stability and experience are absent in a country, its peoples and institutions may legitimately fear that committing to another country's technologies might reduce their autonomy. Cross-commitment makes sure everyone has a stake in the successful adjustment of the entire European economy.

At the same time, the EU is having to answer crucial questions about how to transform its legally established values into verifiably testable criteria for technology, while also safeguarding competition and innovation. At both the European and the national levels, institutions need to develop a less risk-averse culture, where bold investments can lead the way to both competitive markets and future technologies, but also provide important opportunities to learn from failures.

High-level governance tools such as harmonised standards and self-conformity assessments, the realisation from classical European competition law that robust and competitive markets require a minimum number of competitors to remain viable, and transparency as a core value for success are already in place.

Catching up or falling behind? Roadblocks for Europe

In the cybersphere, the EU is either trying to catch up or falling behind. In jest, observers remark that in our multipolar world, the US is responsible for innovation, China for manufacture and the EU for regulation.[1] The concern should be that neither service development nor material production occurs on European soil.

In fact, while the European single market has been under construction for more than 30 years, the market is anything but digital. European startups such as Workable (human resources management), Gorilla (electricity pricing), Revolut (fintech), ESET (security) and Spotify (streaming) have launched their services by first establishing themselves in their home member state, before advancing to either the Netherlands or the UK, and then conquering the US market, ahead of returning 'home' to Europe to capture other larger markets beyond their home market. This is a costly and time-consuming endeavour, in which EU-founded companies have to compete against US companies on the US market before even standing a chance in the EU market.

Western European markets remain closed not just to Eastern European service and product developers, but to all non-domestic companies. For example, in France, all spectrum licences for commercial mobile network operations are held by French entities.[2] Only Belgium has ever awarded a spectrum licence to an Eastern European player (a 5G licence to DIGI Communications).[3] A large part of this challenge is surely rooted in the linguistic diversity of the EU, but the spectres of mistrust and security policy still present effective barriers to both market integration and industrial prominence.

Ambitious projects to ensure cross-border service availability, such as Gaia-X for cloud services, end up doing little more than developing structured text files (JSON tags).[4] Even where frameworks for competitive procurement are being developed to help guide public-sector investments, they are rarely implemented and poorly enforced.[5]

These shortfalls of the European integration project can only be remedied by the member states; however, the EU needs to develop more robust mechanisms to call them out. Rather than retreating into autocracy and a 'not made here' mentality, the member states need to work out why European entities do not invest in each other.

One example of the lack of cross-border cooperation is that of European participation and representation in industry-driven standards development. There are industry-wide platforms for the development of the common technical practices that underpin the entire global communications infrastructure, for example, the standardisation work of IEEE 802.11, the Internet Engineering Task Force, the UTF-8 Consortium or the USB Implementers Forum. In these fora, European companies are present and contribute, but do not lead the work. In fact, the only consortium of notable import founded and governed from European soil is the Open Radio Access Network (O-RAN) Alliance. This is not to denigrate the contributions of European companies to global technology standards, but rather to point out that they are neither interested in, nor capable of leading the way for others in the way we have come to expect from the Linux Foundation, the Kubernetes Foundation,[6] the Ceph and OpenStack foundations,[7] or the Connectivity Standards Alliance.[8]

---

1 C. Hobbs, 'Project Note: In Search of Europe's Digital Sovereignty', in European Council on Foreign Relations, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US–China Rivalry* (30 July 2020).

2 ARCEP, 'Mon Réseaux Mobile'.

3 *Tweakers.net*, 'Nieuwe provider Digi Belgium start voor het einde van het jaar', 16 May 2024.

4 See Gaia-X Technical Committee, 'Gaia-X Architecture Document – 23.10 Release, Chapter 3: Conceptual Model', chapter 3.3.1 'Gaia-X Credentials'. These credentials implement a JSON-LD syntax from W3C, 'Verifiable Credentials Data Model v2.0', 19 October 2024, chapter 6.1.

5 Germany, Commissioner of the Federal Government for Information Technology, *Architekturrichtlinie für die IT des Bundes*, version 6.1 (Berlin, January 2024).

6 Founded by Google through a donation of source code developed in-house for assisting in the management of virtual server configurations.

7 Founded by IBM to enable industry-wide collaboration around cloud application programming interface developments.

8 Currently stewarding ZigBee and Matter, the latter being a connected-home-over-Internet-protocol framework originally developed by Amazon, Apple and Google.

Meanwhile, the European regulatory standards framework has its roots in the beginnings of the single market, but primarily functions well in the context of synergising and finding compromise on national standards. Harmonised standards are developed to counter technical barriers to trade in market areas ranging from radio to cement.

In the majority of cases, functional safety standards and requirements frameworks already existed in the member states before the initiation of the single market, and the European-level institutions simply serve to ensure that European integration does not degrade the quality and safety of food, construction materials or electrical safety. The European Committee for Standardisation, the European Committee for Electrotechnical Standardization and the European Technical Standards Institute provide the intergovernmental frameworks within which the harmonisation of standard requirements can occur. For markets where product cycles are much longer than the typical certification cycle, for instance, sewer-pipe linings, fire alarms or food preservatives, these harmonised standards function well. The long lead times for the development and application of the standard matter little when product lifetimes are longer than 10 years.

However, for ICT, the European standardisation system does not perform so well. It lacks the flexibility afforded by industry-led groups and is encumbered by political formalism. The same mechanisms that are a strength in terms of safeguarding the application of the precautionary principle in food and building safety become a hindrance on the ICT market, where product cycles are shorter than certification cycles. Added to this is the fact that most ICT standards are already in production (for instance, in the shape of finalised code) and ready for deployment by the time they are standardised. This contrasts, for instance, with steel-pipe manufacturing, where a standard is established before production begins. The EU would do well to invest in its capacity to benefit directly from sensible industry standards in these circumstances, namely, by absorbing the outcomes from industry-driven standards bodies directly into procurement guidelines, rather than forcing them through its already established intergovernmental frameworks.[9]

Finally, the EU needs consistent and coherent political leadership. Instead of sending the European Commission services scrambling to invent a way in which ‘European values’ make their particular unit especially important to the European economy, political leaders need to have a sufficiently shared understanding of what they are doing to help the services work in tandem with each other and the cabinets on what a good enforcement policy might look like. Terms such as ‘data protection’ or ‘trustworthy’ need to be imbued with practical meaning, both to assist with the understanding of current laws and to drive new legislation.

A path towards the future: reiterating what has already worked

As dire as the situation may appear, the EU has succeeded in establishing a portfolio of policy options with which to gather knowledge, fund projects and create regulation. In the last 10 years alone, the second Payment Services Directive[10] has paved the way for open application programming interfaces (APIs) in the banking sector, which has enabled lots of innovative products to be launched on the European markets that otherwise would not have been commercially feasible. The Digital Operational Resiliency Act[11] is expected to create a market space for multiple cloud-service providers, thereby ensuring that no single cloud-service vendor becomes

[9] A. Andersdotter and L. Olejnik, ‘Policy Strategies for Value-Based Technology Standards’, *Internet Policy Review* 10/3 (2021).

[10] European Parliament and Council Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L337 (25 November 2015), 35.

[11] European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 (Text with EEA relevance), OJ L333 (14 December 2022), 1.

too big to fail. With this evaluation of the financial sector, it should be considered whether similar regulation could be useful in other areas. Home automation, vehicle sharing and digital-content platforms could be areas where functional requirements for interoperable APIs could help consumers to switch between providers.

Regulations such as the General Data Protection Regulation are only now beginning to take effect on the markets as enforcement authorities become more competent and confident. Despite this, privacy engineering and privacy-enhancing technologies mostly remain the public concern of large American tech companies,[12] while European companies have either failed completely or at least failed to advertise any enthusiasm for or engagement with the topic. Here, a cultural shift is needed in the leadership of the largest European companies, which can only be brought about by consistent and steadfast political leadership.

The US Defence Advanced Research Projects Agency has a strategy of funding multiple consortia to perform the same task, thereby ensuring that all pressing technical problems are addressed in a multiplicity of ways by different entities. Each challenge thereby gives rise to a competitive market for solutions already in the initial stage of development. The ongoing development of open-source electronic design automation libraries for chipsets is a prime example.[13] The EU would do well to replicate this strategy.

On the research front, the EU should further explore social science perspectives. Instead of looking only at technology development, the EU needs economic and social models into which technical innovations can be sensibly incorporated. This may include exploring European conceptualisations of leadership and industrial leadership, innovation management practices, and both business- and socially oriented interactions between European technology companies and the public sector. Consider, for instance, the application of cryptographic tokens to property sales in European jurisdictions where notaries mediate property transactions: instead of creating efficiency, cryptographic protocols introduced the necessity of having two notaries where previously only one was needed.[14]

To identify current gaps in enforcement and standardisation, the EU should not hesitate to use its full arsenal of institutional tools. The General Data Protection Regulation calls for data-protection-friendly technical standardisation:[15] a European Parliament special inquiry should be requested to investigate which industry-driven initiatives exist in this space and how they relate to the enforcement challenges currently faced by data protection authorities. The ePrivacy Directive calls for technical tools to enable stronger protection from tracking:[16] a European Parliament special inquiry should be requested to map the challenges and opportunities arising from this obligation. The Radio Equipment Directive formulates built-in data-protection and privacy features as an essential requirement of all radio equipment,[17] an obligation that has been present in European law since 1999, but which has still not been realised fully for all radios:[18] a European Parliament special inquiry should be requested to investigate industry-driven initiatives and regulator efforts to advance this essential requirement.

---

12 Google Cloud, 'Use Differential Privacy' (last updated on 15 October 2024); Amazon, 'AWS Clean Rooms Differential Privacy'; Github.com, 'Mozilla Prio Project' (archived on 13 February 2024).

13 See Defence Advanced Research Projects Agency initiatives Posh Open Source Hardware and Intelligent Design of Electronic Assets, and the initiatives sponsored under these programmes.

14 J.-F. Blanchette, *Burdens of Proof* (MIT University Press, 2012).

15 European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L119 (27 April 2016), 1, arts. 12(7)–12(8), 25 and 43(9).

16 European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201 (12 July 2002), 37, art. 5(3).

17 European Parliament and Council Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L153 (16 April 2014), 62, art. 3(e).

18 Although note, exceptionally, European Technical Standards Institute standard EN 303 645.

No other European body is as well placed as the European Parliament to maintain good relationships with all stakeholders, allowing it to survey the breadth and depth of industrial and social challenges in these already well-established priority fields of the Union.

The European Commission, in its turn, is well-placed to enforce existing legislation and agreements between member states. The politically appointed functionaries need to focus on the challenges faced by apolitical civil servants and determine where there are gaps or difficulties in enforcement, not only where member state governments feel that this enforcement is opportune, but across the board. A well-functioning executive is at the heart of any enterprise, whether it be a small or medium-sized company or a grand international experiment in cooperation across borders.

The European institutions could have a key role to play in identifying current capital flows in the EU. Whose money is being invested where, and in which services? The French telecommunications regulator Autorité de régulation des communications électroniques (ARCEP) has already done a lot of heavy lifting in terms of showcasing energy flows in the network operator industry.[19] Similarly pedagogic presentations are required about investments in innovation and development to enable and inspire a more integrated and equitable European digital single market. With more and more EU countries in Central and Eastern Europe (CEE) fearing that they are being left behind, careful analysis and consideration of the actual conditions on the ground could help to bring a sense of cohesion and clarity to the development of the EU market.

This might include understanding how research and development or customer support activities are being outsourced to CEE countries by Western European companies, but it may also shed light on the extent to which Western European capital is flowing into home-grown CEE activities such as e-commerce (the Allegro group), airlines (WizzAir) or cybersecurity (ESET). More recently, Europe has been the destination for large investments in privacy technologies in fintech and encrypted ledgers, which has primarily benefited developer bases in CEE.[20] However, it remains unclear whether the EU will be able to capitalise on its contributions to these emerging markets.[21]

Conclusion

Europe needs consistent, coherent leadership and governance to fully benefit from its contributions to the digital economy. As a large consumer market, and an internally under-appreciated centre for technological development and innovation, with strong social and fundamental rights ideals, the EU should be able to shape global privacy and security standards in line with its foundational values. However, the Union must strive for greater maturity in its policy application.

Following up on already established policy directions, such as the commitment to data protection, privacy and procedure, will rationalise the European project for both citizens and businesses. The positive effects will reverberate throughout the technological stacks. But this needs to be coupled with paying greater attention to the capital flows to and within Europe, from east to west, and to the shared European funding of competitive and innovative research.

The EU should also develop procedures to benefit from existing mechanisms in standardisation. Translating European values into deterministic and predictable test criteria remains a challenge for policymakers and technology developers alike.

19 ARCEP and ADEME, *Assessment of the Environmental Impacts of the ICT Sector: Methodological Gap Analysis* (2023).
20 Electric Capital, *2023 Crypto Developer Report* (January 2024).
21 European Securities and Markets Agency, *Crypto Assets: Market Structures and EU Relevance* (Paris, 10 April 2024).

	Programme 1	Programme 2	Programme 3
	Creating digital resilience	**Ensuring digital sovereignty**	**Building future infrastructures**
Project 1	Establish (self-)certification schemes for products and services destined for the European market based on exact and replicable requirements. Continue to invest in European hardware infrastructure, including basic infrastructure such as long-distance cables and electricity grids.	Build capacity in project management for open-source code-as-infrastructure, especially in terms of industry-oriented fora (e.g. O-RAN Alliance). Trust, but verify: European open-source code libraries that address shared challenges should act as both public infrastructure and a trustworthy technology base.	Produce a standardisation strategy for 5G, O-RAN, cloud technologies and the Internet of Things that emphasises European values. Ensure fast deployment of the latest compliant technologies by allowing the flexibility of self-certification against approved standards with product recall penalties in the event of demonstrated infringements. Ensure that spectrum licences include requirements on the security of network equipment.
Project 2	Ensure technical resilience in investments across Europe. Use at least two vendors of network equipment from two different countries in any national network. Make the operation of a commercial system independent from features available from only one single upstream supplier (e.g. lock-in mechanisms, vendor-specific APIs or de facto standards).	Support technology development in Europe through strategic procurement, including where there is a risk of failure. Map capital flows into European technology industries and startups. Ensure that public money goes to public, open infrastructures, even code, that instil trust by being verifiable.	Hold a series of European Parliamentary inquiries into topic-specific enforcement activities in the area of cyber-excellence (e.g. activities regarding the essential requirement of radio equipment to respect data protection, as contained in Directive 2014/53/EU, art. 3(e)). Continue to focus on cyber-exercises and scenarios, especially in the cross-border context—consider the possibility of holding competitions that test sectoral, randomly selected teams, or similar, rather than national ones.
Project 3	Leverage the framework of harmonised standards. Develop shared open-source libraries for common goals and norms in public infrastructure, such as billing systems, personnel systems and so on. Support red-team research, responsible vulnerability disclosure and remedy/patching schemes.	Consistently recognise both the technical aspects of security (objective, deterministic criteria) and the organisational and legal aspects (venues of conflict resolution, jurisdiction and decision-making) when addressing cyber-governance. Bring together existing forces for capitalisation and market access to achieve pan-European service-launch opportunities.	Realise opportunities for innovators by opening up new regulatory spaces through replication of the changes in the fintech sector (with open APIs for specific bank payment systems in the 2010s) and the wireless local area network sector (when microwave bands were opened up to licence-exempt use in the 1990s).

Bibliography

Amazon, 'AWS Clean Rooms Differential Privacy' (2024), accessed at https://aws.amazon.com/clean-rooms/differential-privacy/ on 26 October 2024.

Andersdotter, A. and Olejnik, L., 'Policy Strategies for Value-Based Technology Standards', *Internet Policy Review* 10/3 (2021), doi:10.14763/2021.3.1573.

ARCEP, 'Mon Réseaux Mobile', accessed at https://monreseaumobile.arcep.fr/ on 26 October 2024.

ARCEP and ADEME, *Assessment of the Environmental Impacts of the ICT Sector: Methodological Gap Analysis* (2023), accessed at https://en.arcep.fr/uploads/tx_gspublication/environment-impact-ICT-sector-methdological-gap-analysis_april2023.pdf on 26 October 2024.

Blanchette, J.-F., *Burdens of Proof* (MIT University Press, 2012).

Electric Capital, *2023 Crypto Developer Report* (January 2024), accessed at https://www.developerreport.com/developer-report-geography on 26 October 2024.

European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201 (12 July 2002), 37.

European Parliament and Council Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance), OJ L153 (16 April 2014), 62.

European Parliament and Council Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L337 (25 November 2015), 35.

European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L119 (27 April 2016), 1.

European Parliament and Council Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 (Text with EEA relevance), OJ L333 (14 December 2022), 1.

European Securities and Markets Agency, *Crypto Assets: Market Structures and EU Relevance* (Paris, 10 April 2024), accessed at https://www.esma.europa.eu/sites/default/files/2024-04/ESMA50-524821-3153_risk_article_crypto_assets_market_structures_and_eu_relevance.pdf on 26 October 2024.

Gaia-X Technical Committee, 'Gaia-X Architecture Document – 23.10 Release, Chapter 3: Conceptual Model', accessed at https://docs.gaia-x.eu/technical-committee/architecture-document/23.10/gx_conceptual_model/ on 26 October 2024.

Germany, Commissioner of the Federal Government for Information Technology, *Architekturrichtlinie für die IT des Bundes*, version 6.1 (Berlin, January 2024), accessed at https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/ArchRL.html on 26 October 2024.

Github.com, 'Mozilla Prio Project' (archived on 13 February 2024), accessed at https://github.com/mozilla/prio-processor on 26 October 2024.

Google Cloud, 'Use Differential Privacy' (last updated on 15 October 2024), accessed at https://cloud.google.com/bigquery/docs/differential-privacy on 26 October 2024.

Hobbs, C., 'Project Note: In Search of Europe's Digital Sovereignty', in European Council on Foreign Relations, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US–China Rivalry* (30 July 2020), 91–4, accessed at https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/#project-note-in-search-of-europes-digital-sovereignty on 26 October 2024.

Tweakers.net, 'Nieuwe provider Digi Belgium start voor het einde van het jaar', 16 May 2024, accessed at https://tweakers.net/nieuws/222022/nieuwe-provider-digi-belgium-start-voor-het-einde-van-het-jaar.html on 26 October 2024.

W3C, 'Verifiable Credentials Data Model v2.0, 19 October 2024, accessed at https://www.w3.org/TR/vc-data-model-2.0/ on 26 October 2024.

Completing the European Digital Single Market

by Milda Kaklauskaitė

Summary

With the aim of strengthening the EU's digital single market, this paper sets forth key policy recommendations which focus on unifying digital regulations and infrastructure. Simplifying bureaucracy by introducing an 'EU Company' status would ease cross-border operations for tech startups and small and medium-sized enterprises, fostering rapid market entry. Promoting innovation through incentives for large businesses to adopt European solutions and encouraging data sharing would level the playing field and boost the competitiveness of smaller companies. To support startup growth, completing the Capital Markets Union and aligning pension funds with startup needs are crucial, as these actions would unlock substantial investment and drive economic progress.

Enhancing cybersecurity is essential for digital sovereignty; investing in training and establishing a pan-European cybersecurity fund would ensure protection against cyber threats. Harmonising public procurement rules would encourage the adoption of European solutions, reducing reliance on external suppliers. Implementing these measures would enhance Europe's tech ecosystem, attract investment and ensure resilience in the digital economy.

Keywords DSM – Harmonisation – Startups – SMEs – Pension funds – Venture capital – Insolvency – Cybersecurity – CMU – Training – Procurement

Introduction

The digital single market (DSM) was introduced in 2015 for the purpose of bringing the EU's single market into the digital age.[1] While the single market, established in 1993, facilitated the free movement of goods, services, capital and people, the DSM aimed to enhance business competitiveness and protect online data. Key achievements include eliminating roaming charges and introducing digital copyright and e-commerce regulations, with the Digital Services Act focusing on user protection.

Despite these significant advancements, challenges remain. Excessive legislative and administrative burdens hinder tech innovators from scaling across borders. Larger companies are slow to adopt innovations from small European providers, and access to non-sensitive data is limited. The EU is also criticised for its lack of private investment, which stifles tech innovation, and for its fragmented financial sector, which restricts cross-border funding, particularly from pension funds. Cybersecurity is another area of concern. While there are calls for greater strategic autonomy and technological independence, the EU's cybersecurity sector is often overshadowed by non-EU providers, with much of Europe's innovative technology being bought by foreign companies.

This policy paper examines the bottlenecks preventing the completion of the DSM and outlines the concrete and practical recommendations that must be implemented to address these challenges. Special attention is given to the needs of the European tech startups and small and medium-sized enterprises (SMEs) to expand their businesses; the ways to boost private investments, which are essential to drive tech innovation; and the changes needed to boost the EU's cybersecurity posture.

[1] European Commission, *A Digital Single Market Strategy for Europe*, Communication, COM (2015) 192 final (6 May 2015).

Key barriers to the EU's ambition for the DSM

The EU faces critical challenges to achieving a fully realised DSM, which is essential for global competitiveness. Three key issues require urgent policy action. First, market fragmentation and slow innovation hinder tech startups and SMEs. Second, a lack of private capital stifles growth in fintech and other sectors, driving high-potential firms to seek investment abroad and limiting domestic growth. Third, Europe struggles with cybersecurity due to expertise shortages, underinvestment and reliance on non-European providers. The following discussion elaborates on these challenges, highlighting how each presents distinct barriers to Europe's long-term competitiveness and digital leadership.

Europe's tech startups and SMEs in headwinds

European tech startups and SMEs face substantial barriers due to European market fragmentation, which severely limits their ability to scale and grow at the same pace as their counterparts in larger, more homogenous markets like the US. The European markets' regulatory fragmentation has been identified as a key impediment to cross-border scaling.[2] Unlike the unified US market, Europe is divided into multiple national ecosystems with distinct regulations, administrative frameworks and languages. This fragmentation hinders startups from scaling in a stable regulatory environment, slowing their growth.

Another significant challenge is the slow adoption of innovative technologies due to a conservative, risk-averse mindset among European buyers. Unlike in the US, where early adoption is encouraged, European businesses tend to favour established providers for comprehensive solutions. This preference makes it difficult for startups and SMEs to gain credibility and secure the essential market references needed for customer acquisition and growth.[3] Conversations with startups reveal that this risk aversion is further fuelled by a reliance on known brands, which are perceived as more reliable, with this putting European tech startups and SMEs at a substantial disadvantage when competing against large multinationals and foreign tech giants.

Small businesses face significant disadvantages compared to large international corporations due to limited access to essential data and data-gathering tools crucial for growth and operational success. In Europe, where small businesses account for over 99% of all companies, this issue is particularly pressing.[4] While SMEs dominate the European business landscape, over half of the net turnover in the EU comes from large enterprises, further emphasising the competitive disadvantage SMEs face.[5] Unlike large corporations with abundant resources, SMEs struggle to leverage data for decision-making, which is vital for scaling operations and expanding their customer base.

Europe's unwelcoming investment climate

A critical challenge facing the European innovation landscape is the lack of private financial capital, stemming from the fragmentation of the financial markets.[6] The absence of a fully integrated Capital Markets Union (CMU) hampers the free flow of venture capital and stifles fintech innovation. Varying regulations and procedures

[2] World Economic Forum, 'Uniting Europe's Markets', Davos Annual Meeting (19 January 2024); M. Gordiano, 'Accelerating Europe: Competitiveness for a New Era', *McKinsey Global Institute*, 16 January 2024).

[3] L. Guk, 'Go to Market — Or Die', *Sifted*, 29 July 2020.

[4] L. Di Bella et al., *Annual Report on European SMEs 2022/2023* (Luxembourg, 2023), 6.

[5] Eurostat, 'Large Businesses Generated Half of EU's Net Turnover' (12 December 2023).

[6] While the EU, alongside its member states, has made strides in establishing robust financing mechanisms for research, such as Horizon 2020, Horizon Europe and the Digital Europe programmes, the region remains reliant primarily on public funds, including grants and loans, to support innovation. These initiatives effectively foster early-stage research collaboration between startups, research centres and other stakeholders. However, once this initial funding phase concludes, many projects face the notorious 'valley of death', where startups, particularly in deep tech, fail to secure follow-on investment despite offering groundbreaking innovations and being seen as having high potential. Companies also need funding for initial commercialisation and market expansion phases, not just research.

across member states burden investors and deter cross-border investments. This lack of harmonisation is a major reason investors avoid reinvesting in Europe.[7] This limits startups' ability to access investment beyond their home markets and hinders their international exposure and advisory support for growth.

Another issue is the ineffective deployment of financial capital from European pension funds. European pension funds hold vast amounts of capital but remain largely inactive in investments. In 2022, just 0.024% of pension fund assets under management were invested in European venture capital firms.[8] Regulations limit diversification into higher-risk assets, pushing pension funds towards safer government bonds. Meanwhile, more agile non-European pension funds are stepping in to fill Europe's venture financing gap.[9] As a result, European venture capital firms primarily focus on early-stage investments, neglecting later stages like Series C[10] or pre–initial public offering[11] rounds.[12] The EU seeks to address this issue with governmental investment funds, but the strict conditions placed on the use of public money misalign with optimal investment opportunities.[13] Unlocking dormant European pension capital is key to building larger European venture capital funds.

Divergent insolvency regimes across the EU create uncertainty and complexity for cross-border investments, raising risks and costs for investors. These disparities limit investment recovery in case of failure, discouraging risk-taking. As a result, European startups struggle to secure funding and compete with US rivals, who work in a more mature, risk-tolerant ecosystem.[14] The EU Restructuring Directive of 2019 (Second Chance Directive) was a step towards harmonising restructuring laws.[15] However, insolvency proceedings still vary significantly, particularly in asset management, distribution and timely restructuring, highlighting the need for further harmonisation.

Europe's crippling cybersecurity stance

The cybersecurity skills gap is a global issue, and Europe is no exception as the sector rapidly expands. Recent reports from the OECD reveal that Europe currently faces a shortage of almost 350,000 cybersecurity professionals and forecast a significant increase in the need for cybersecurity skills in the coming years.[16] This gap underscores the urgent need for strategic efforts to develop and attract talent to secure EU digital systems. While European and international businesses are aware of this growing issue, there is still a lack of coordination between the public and private sectors to build a sustainable pipeline of cybersecurity experts.

Furthermore, the EU's cybersecurity posture is weakened by insufficient investment in cybersecurity innovation. A European Investment Bank study estimates an investment gap of around €1.75 billion per year in the EU cybersecurity market.[17] This funding gap has contributed to the frequent acquisition of European cybersecurity

7 Some very interesting first-hand insights and opinions by international investors who invest across Europe can be found on the European Accelerationism website, launched as a community movement by Andreas Klinger, an angel investor and serial entrepreneur, with a group of other founders. See European Accelerationism (website).

8 Atomico, *State of European Tech 2023* (London, 2023), 212.

9 F. Perticarari, 'Europe, America Is Coming for Your Startups', *Sifted,* 27 September 2023.

10 Series C funding is aimed at preparing a company for significant growth initiatives, such as being acquired, going public or expanding through acquisitions. The aim is to raise substantial capital to scale operations and enhance market presence.

11 Pre–initial public offering describes the period leading up to a company's first public offering of shares. This stage is vital for laying the groundwork for a successful transition to being a publicly traded entity.

12 A. Schwarzenbrunner, 'Report: Inside the Minds of European VCs', *SpeedInvest*, 6 June 2023.

13 J. Lerner, *Boulevard of Broken Dreams: Why Public Efforts to Boost Entrepreneurship and Venture Capital Have Failed and What to Do About It* (Princeton: Princeton University Press, 2012), 111–61.

14 *McKinsey & Company*, 'Europe's Start-up Ecosystem: Heating up, but Still Facing Challenges', 11 October 2020.

15 European Parliament and Council Directive (EU) 2019/1023 on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132 (Directive on restructuring and insolvency), OJ L172 (20 June 2019), 18.

16 OECD, *Building a Skilled Cyber Security Workforce in Europe: Insights From France, Germany and Poland* (Paris, 2024), 24.

17 European Investment Bank, *Report on European Cybersecurity Investment Platform* (Luxembourg, 22 October 2022), 36.

startups by non-European entities, leading to the relocation of these companies abroad. BforeAI and Enigmedia, now known as Opscura, are among the latest examples.[18] As a result, Europe loses both intellectual property and talent, increasing its reliance on non-European suppliers and raising risks in securing sensitive assets and critical infrastructure.

The EU's reliance on non-European cybersecurity suppliers is further aggravated by public procurement frameworks that disadvantage small providers. Existing rules often unintentionally exclude small cybersecurity providers from tenders, disproportionately favouring large multinationals, many based outside Europe. This widens cyber supply-chain risks, limits smaller European firms' access to clients and market references, and reduces the public sector's potential role as a strategic customer.[19] Fragmented procurement regulations across the EU further hinder small providers from participating in cross-border procurement processes.

Cracking the code: recommendations for the EU's digital future

Although these issues vary in nature, they are all central to Europe's ability to innovate and compete on the global stage. The EU must address these areas strategically. The following are concrete policy recommendations for the European Commission (2024–9) and the EU member states to effectively address the identified challenges in completing the digital single market.

On startups and SMEs

1. Establishing an 'EU Company' status as a standardised European entity should be a top priority for the next European Commission. The idea of an EU-wide legal status to reduce the administrative burden for startups and SMEs has been discussed since around 2011 but has remained unimplemented. Adopting a European entity standard would streamline market entry for startups and SMEs aiming to expand internationally, helping them to navigate and comply with the legal requirements of 27 different EU member states. Such alleviation of the administrative burden would greatly simplify cross-border operations and reduce market fragmentation in Europe. The success of this initiative will depend on ensuring the procedures and standards that have to be met to achieve EU Company status are business friendly. The EU needs to make sure that companies can acquire this status without facing unreasonable legal costs and onerous administrative requirements.

2. To boost market traction and credibility for small businesses, the EU could incentivise large companies to adopt innovative solutions from European startups and SMEs, countering the region's conservative innovation culture and preference for established firms. Some key measures to implement are the following:

    - Offer large firms a competitive advantage in public tenders for including SMEs in their supply chains or innovation.
    - Provide tax incentives for partnerships between large companies and European startups, especially in priority sectors such as the green transition and digitalisation.
    - Establish a fund to reduce risks for large firms adopting innovative, untested solutions from startups.
    - Update procurement rules to ensure a portion of contracts go to SMEs.

[18] Opscura, 'ICS Cybersecurity Firm Opscura Launches With $9.4 Million in Series A Funding', 7 February 2023; BforeAI, 'BforeAI Announces $15 Million in Series A Funding Led by SYN Ventures', 24 April 2024.

[19] U. Horstmann, 'If Governments Want to Help Startups, They Should Stop Being Such Terrible Customers', *Sifted,* 7 November 2023.

- Develop standardised partnership templates to simplify legal and administrative barriers, encouraging collaboration and acceptance of the above-mentioned measures.

3. Promoting digital transformation and increasing digital intensity among European SMEs is critical for their competitiveness and the EU's digital economy. While the Open Data Directive[20] provides a framework for reusing public-sector information, its enforcement needs strengthening, and private-sector data sharing must be incentivised. As a first step, cross-border data flows should be ensured by harmonising data protection and sharing regulations across member states. The EU should support the development of shared data platforms in key industries, creating sector-specific data spaces that allow SMEs to access relevant information. Larger corporations should be incentivised to share anonymised data with smaller businesses in their value chains through tax breaks and a voluntary EU-wide data-sharing code of conduct, which would encourage businesses to participate in responsible data sharing.

On private investments

1. The CMU, proposed in 2014, has seen only incremental progress despite several action plans from the European Commission since 2015.[21] While many measures have been adopted, they have largely reinforced existing market fragmentation. A truly ambitious CMU reform must prioritise the implementation of standardised rules, tax laws and supervision for investors and financial firms across the EU. The current preferential tax treatment of debt over equity should be abolished to establish a more risk-friendly culture. A European safe asset should eventually be created as well, offering investors a liquid, risk-free reserve and a benchmark for financial products, separate from national bonds. Only then will the EU be able to attract investments in critical tech sectors and advance fintech innovation.

2. The 1974 US pension fund reform showed how directing pension funds into venture capital spurs innovation.[22] Enabling European pension funds to invest in venture capital could be transformative, empowering European venture capital firms to establish larger funds and offer more substantial investments, particularly for growth-stage companies. The UK has already started reforming pension funds to channel more private capital into startups[23] The EU must review regulatory barriers to encourage pension funds to diversify beyond traditional low-risk equities and bonds, allowing them to invest more freely in venture capital.

3. To create a more favourable investment environment, Europe must address the fragmentation of national insolvency laws. The 2022 Insolvency Law Proposal aims to harmonise key aspects of insolvency law which might not have been covered by the Second Chance Directive.[24] However, it still faces hurdles. First, the proposal has not yet been agreed upon due to criticism that it conflicts with national insolvency laws in some member states. Second, it requires updates to address missing elements. To eliminate discrepancies across countries, the EU should establish a unified definition of insolvency and specify the main parties involved in the insolvency proceedings. The conditions for triggering insolvency proceedings and harmonising avoidance rules must be standardised across member states. Regulations on financial collateral and securities settlement should be aligned. These changes would facilitate faster implementation of the 'second chance' policy, which is crucial for reducing the social stigma surrounding business failure—a

[20] European Parliament and Council Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ L172 (20 June 2019), 56.
[21] European Council, 'What the EU Is Doing to Deepen Its Capital Markets' (last reviewed on 9 October 2024).
[22] W. Gornall and I. A. Strebulaev, 'The Economic Impact of Venture Capital: Evidence From Public Companies', *S&P Market Intelligence* (June 2021), 2–4.
[23] UK Government, '£320 Million Plan to Usher Innovation and Deliver Mansion House Reforms', 21 November 2023.
[24] European Commission, 'Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law', COM (2022) 702 final (7 December 2022).

stigma much more pronounced in Europe than in the US. The Directive itself needs certain revisions, as its introduced preventative restructuring framework is overly complex for smaller businesses to navigate effectively and should be simplified.

On cybersecurity posture

1. The launch of the Cybersecurity Skills Academy in 2023 represents a step towards bridging the cybersecurity skills gap by aiming to unite private and public initiatives. However, more coordinated action at the EU level is needed to address this gap in Europe. First, the EU should integrate cybersecurity education into primary and secondary school curricula to build foundational skills and raise early awareness, which should be followed by awareness campaigns promoting cybersecurity as a rewarding career path.[25] EU-wide vocational training and apprenticeship programmes for those without formal cybersecurity education should be put in place. Continuous upskilling for professionals should also be prioritised, given the rapid evolution of cyber threats. Effective implementation will require cooperation with the private sector, with the EU offering tax incentives for businesses participating in cybersecurity training and certification for their employees.

2. Building on models like the NATO Innovation Fund and the European Tech Champions initiative, the EU should establish a cybersecurity investment platform, with initial funding of €1 billion from the EU and member states. This would signal high-level political commitment and attract private investors. The need for such a platform has been echoed by cybersecurity stakeholders across Europe.[26] For success, the platform should be structured as a 'fund of funds' to enable rapid investment into cybersecurity venture capital funds. It must avoid market restrictions on investee companies and lengthy approval procedures, as these would hinder competitiveness with overseas investments that come with fewer conditions.

3. To boost SME participation in procurement, the EU and member states should align requirements to avoid excluding smaller cybersecurity providers. More procurement of homegrown solutions would help to reduce potential dependencies on non-European suppliers and security backdoors. While procurement is largely national, the European single procurement document has made bidding easier.[27] However, further reforms are needed to help European cybersecurity providers compete and reduce bias favouring well-known providers. These include:

    - limiting turnover thresholds to no more than twice the contract value, and prioritising team qualifications over market experience;
    - facilitating joint bidding, allowing small businesses to collaborate on larger contracts;
    - ensuring procurement criteria are proportionate to the size of the business; and
    - simplifying processes by reducing documentation, financial guarantees and compliance costs.

[25] Private initiatives carried out by the Women4Cyber Foundation (website) and by the European Cyber Security Organisation, such as *Youth4Cyber* (see European Cyber Security Organisation, 'Youth4Cyber' serve as exemplary models in tackling the cybersecurity skills gap. These existing programmes offer a solid foundation upon which the EU can build further.

[26] European Cyber Security Organisation, *The Letter of Intent to the European Commission on Creating a European Cybersecurity Investment Platform*, 20 September 2020 and 20 November 2020.

[27] European Commission, 'European Single Procurement Document and eCertis'.

Conclusion

The challenges outlined in this policy analysis hinder of the digital economy in Europe reaching its full potential. The various legal complexities that startups and investors must navigate stifle innovation and weaken the continent's competitiveness with the US and China. Addressing these barriers—particularly through regulatory harmonisation and capital market integration—is essential for completing the DSM. A truly integrated and functioning DSM cannot be achieved without a robust cybersecurity framework capable of tackling ever-evolving threats.

Implementing the identified recommendations would provide European startups and SMEs with a more conducive environment for scaling, would increase market access opportunities, and would provide better access to data sharing and pooling. A unified capital market would deepen integration, allowing European businesses to compete more effectively with global players. A fully developed CMU, the deployment of untapped capital from pension funds and harmonised insolvency would facilitate cross-border investments, providing clarity and revising the risk-averse culture that hinders innovation in the EU. Cultivating a steady pipeline of cybersecurity professionals, securing adequate funding for cybersecurity innovation and promoting the widespread adoption of homegrown technologies would strengthen Europe's cybersecurity posture.

Ultimately, these measures would foster a competitive landscape for European businesses, allowing them to scale and compete on an equal footing with international giants. To ensure the effectiveness and market relevance of these recommendations, close collaboration with industry representatives, startup and SME associations, investors and cybersecurity stakeholders will be essential.

	Programme 1	Programme 2	Programme 3
	Fostering Europe's tech startup and SME ecosystem	**Attracting private investment**	**Strengthening the European cybersecurity posture**
Project 1	Reduce fragmentation and administrative burdens for companies operating or aiming to expand in multiple countries. Establish an 'EU Company' status to simplify cross-border operations for businesses and streamline market entry by alleviating the administrative burden of setting up entities and complying with local regulations.	Complete the CMU to remove the fragmentation across national borders and allow the free flow of venture capital investments into the tech sector across the EU. Finalising the CMU is the precursor to an improved fintech innovation outlook. Only through improved market integration can the EU rise to the challenge of long-term competitiveness vis-à-vis China and the US.	Increase funding for cybersecurity training programmes (upskilling and reskilling) to address the skills gap and build a robust pipeline of cybersecurity professionals.
Project 2	Provide incentives for large businesses to adopt innovative European solutions. This would support homegrown companies in gaining market traction and establishing credibility among potential customers. A matchmaking platform could be established to co-create solutions tailored to specific needs. Incentives, such as tax breaks, could be introduced to help offset the perceived risks.	Create incentives for European pension funds to back European venture capital firms and growth companies. Aligning the interests of pension funds with the growth of European startups would unlock immense potential both for investors and for the broader European economy.	Establish a pan-European public–private fund of funds dedicated to cybersecurity to foster innovation and safeguard the EU's digital landscape. Given the pervasive and cross-sectoral nature of cybersecurity, collaborative investments must be promoted among both public and private entities across the EU, which would ensure robust protection against evolving cyber threats and advance Europe's digital agenda
Project 3	Strengthen European players' access to data and create opportunities for data pooling and sharing. Facilitating access to non-sensitive data is essential to empower smaller companies, thereby bolstering their competitiveness in the market. Promote the digital transformation and improve digital intensity among European SMEs.	Promote the harmonisation of insolvency proceedings across the EU to help promote cross-border investment. This would provide legal certainty across borders, ensuring investors can navigate insolvency proceedings with confidence. Adopt the 'second chance' rule across borders to provide more assurance among investors in early-stage companies, which are associated with higher risks.	Promote amendments to and harmonisation of public procurement rules across member states to support the growth of European cybersecurity solutions and enhance Europe's cybersecurity posture. Current regulations often disadvantage European cybersecurity providers, hindering innovation and creating potential dependencies on non-European suppliers.

Bibliography

Atomico, *State of European Tech 2023* (London, 2023), accessed at https://stateofeuropeantech.com/ on 20 August 2024.

BforeAI, 'BforeAI Announces $15 Million in Series A Funding Led by SYN Ventures', 24 April 2024, accessed at https://bfore.ai/bforeai-announces-15-million-in-series-a-funding-led-by-syn-ventures/ on 13 September 2024.

Di Bella, L. et al., *Annual Report on European SMEs 2022/2023* (Luxembourg, 2023).

European Accelerationism (website), accessed at https://eu-acc.com/ on 20 August 2024.

European Commission, *A Digital Single Market Strategy For Europe*, Communication, COM (2015) 192 final (6 May 2015), accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 on 10 August 2024.

European Commission, 'European Single Procurement Document and eCertis', accessed at https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/european-single-procurement-document-and-ecertis_en on 12 September 2024.

European Commission, 'Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law', COM (2022) 702 final (7 December 2022), accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0702 on 13 September 2024.

European Council, 'What the EU Is Doing to Deepen Its Capital Markets' (last reviewed on 9 October 2024), accessed at https://www.consilium.europa.eu/en/policies/what-the-eu-is-doing-to-deepen-its-capital-markets/ on 13 September 2024.

European Cyber Security Organisation, *The Letter of Intent to the European Commission on Creating a European Cybersecurity Investment Platform*, 20 September 2020 and 20 November 2020, accessed at https://ecs-org.eu/activities/european-cybersecurity-investment-platform/ on 10 September 2024.

European Cyber Security Organisation, 'Youth4Cyber', accessed at https://ecs-org.eu/activities/youth4cyber/ on 12 September 2024.

European Investment Bank, *Report on European Cybersecurity Investment Platform* (Luxembourg, 22 October 2022), accessed at https://www.eib.org/en/publications/20220206-european-cybersecurity-investment-platform on 23 August 2024.

European Parliament and Council Directive (EU) 2019/1023 on preventive restructuring frameworks, on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132 (Directive on restructuring and insolvency), OJ L172 (20 June 2019), 18, accessed at https://eur-lex.europa.eu/eli/dir/2019/1023/oj on 23 August 2024.

European Parliament and Council Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ L172 (20 June 2019), 56, accessed at https://eur-lex.europa.eu/eli/dir/2019/1024/oj on 10 September 2024.

European Parliament and Council Regulation (EU) 2022/612 on roaming on public mobile communications networks within the Union, OJ L115 (6 April 2022), 1, accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0612 on 10 August 2024.

Eurostat, 'Large Businesses Generated Half of EU's Net Turnover', 12 December 2023, accessed at https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20231212-1 on 20 August 2024.

Gordiano, M. et al., 'Accelerating Europe: Competitiveness for a New Era', *McKinsey Global Institute*, 16 January 2024, accessed at https://www.mckinsey.com/mgi/our-research/accelerating-europe-competitiveness-for-a-new-era on 12 August 2024.

Gornall, W. and Strebulaev, I. A., 'The Economic Impact of Venture Capital: Evidence from Public Companies', *S&P Market Intelligence* (June 2021), accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2681841 on 10 September 2024.

Guk, L., 'Go to Market — or Die', *Sifted*, 29 July 2020, accessed at https://sifted.eu/articles/go-to-market-strategy-startups on 20 August 2024.

Horstmann, U., 'If Governments Want to Help Startups, They Should Stop Being Such Terrible Customers', *Sifted*, 7 November 2023, accessed at https://sifted.eu/articles/if-governments-want-to-help-startups on 23 August 2024.

Lerner, J., *Boulevard of Broken Dreams: Why Public Efforts to Boost Entrepreneurship and Venture Capital Have Failed and What to Do About It* (Princeton: Princeton University Press, 2012).

McKinsey & Company, 'Europe's Start-up Ecosystem: Heating up, but Still Facing Challenges', 11 October 2020, accessed at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/europes-start-up-ecosystem-heating-up-but-still-facing-challenges on 23 August 2024.

OECD, *Building a Skilled Cyber Security Workforce in Europe: Insights From France, Germany and Poland* (Paris, 2024).

Opscura, 'ICS Cybersecurity Firm Opscura Launches With $9.4 Million in Series A Funding', 7 February 2023, accessed at https://www.opscura.io/ics-cybersecurity-firm-opscura-launches-with-9-4-million-in-series-a-funding/ on 13 September 2024.

Perticarari, F., 'Europe, America Is Coming for Your Startups', *Sifted*, 27 September 2023, accessed at https://sifted.eu/articles/europe-america-is-coming-for-your-startups on 22 August 2024.

Schwarzenbrunner, A., 'Report: Inside the Minds of European VCs', *SpeedInvest*, 6 June 2023, accessed at https://www.speedinvest.com/blog/europe-startup-ecosystem-overview on 22 August 2024.

UK Government, '£320 Million Plan to Usher Innovation and Deliver Mansion House Reforms', 21 November 2023, accessed at https://www.gov.uk/government/news/320-million-plan-to-usher-innovation-and-deliver-mansion-house-reforms on 10 September 2024.

Women4Cyber Foundation (website), accessed at https://women4cyber.eu/ on 13 September 2024.

World Economic Forum, 'Uniting Europe's Markets', Davos Annual Meeting (19 January 2024), accessed at https://www.weforum.org/events/world-economic-forum-annual-meeting-2024/sessions/uniting-europes-markets/ on 12 August 2024.

Enhancing European Technological Excellence

by Žiga Turk

Summary

This paper outlines the urgent need for Europe to enhance its technological prowess amidst increasing global competition from the US and China. It emphasises three key technological topics: information and communications technology, cleantech and defence. The first is critical as a productivity multiplier, cleantech is essential for the EU to achieve a net-zero economy while maintaining a competitive edge, and defence technology is crucial for the Union's strategic autonomy amid rising geopolitical tensions. Three horizontal methods are proposed: investing in talent and skills, fostering innovation and entrepreneurship, and creating a dependable playing field through regulatory reform and market integration. The urgency stems from Europe's current lag in digital and artificial intelligence investment, fragmented markets and slow adoption of transversal technologies. To secure its economic future and strategic autonomy, Europe must undertake sweeping reforms, prioritise technological resilience and build a robust ecosystem that supports technological advancement across all sectors.

Keywords Technology – Information technology – Green transition – Cleantech – Military technology – Regulatory simplification – Entrepreneurship – Skills

Introduction

The EU stands at a critical cross-roads and urgently needs a wake-up call regarding its technological policies as global competitors such as the US and China are surging ahead in key domains.

Without bold action, Europe's economic future is at stake, risking not only its competitive position but also its strategic autonomy in an increasingly interconnected and technologically driven world. The time for incremental changes has passed; Europe needs decisive, sweeping reforms to secure its place in the global technological landscape. Its social model depends on this.

There is no shortage of regulation, policy documents or strategies in this arena in the EU. These include the Digital Services Act and the Digital Markets Act, which aim to create a safer and more open digital space.[1] The EU has also advanced legislation including the Artificial Intelligence Act and the Cyber Resilience Act to govern the development and deployment of artificial intelligence (AI) technologies and to enhance the cybersecurity of digital products and services.[2] The European Chips Act is focused on bolstering the EU's semiconductor supply chain, while the European Data Act seeks to unlock industrial data and foster a competitive cloud market.[3] The EU's strategic approach is further supported by the Digital Decade initiative, the Europe Fit for the Digital Age initiative and research priorities in the Horizon Europe programme (2021–7).[4] Other relevant EU policies and initiatives that align with the ideas in this paper include the New European Innovation Agenda, the Research and Innovation Strategy 2020–2024, and Shaping Europe's Digital Future.[5]

1 European Commission, 'The Digital Services Act Package' (updated 4 October 2024); European Commission, 'The Digital Markets Act' (2024).
2 European Commission, 'AI Act' (updated 14 October 2024); European Commission, 'EU Cyber Resilience Act' (updated 8 July 2024).
3 European Commission, 'European Chips Act'; European Commission, 'Data Act' (updated 10 October 2024).
4 European Commission, 'Europe's Digital Decade: Digital Targets for 2030'; European Commission, 'A Europe Fit for the Digital Age' (2024); European Commission, 'Horizon Europe' (2024).
5 European Commission, 'The New European Innovation Agenda' (2024); European Commission, 'Research and Innovation Strategy 2020–2024'; European Commission, 'Shaping Europe's Digital Future (2024)'.

However, critical analyses paint a rather discomforting picture of the current state of affairs. As succinctly put in a *Financial Times* op-ed:[6]

> The US, at the turn of the millennium, did not 'plan' to outgrow Europe. It did not have a version of Mario Draghi's new competitiveness report. It did not produce an equivalent of the Lisbon Agenda, which in 2000 committed the EU to building the most 'dynamic knowledge-based economy in the world'. The US has been deplorably negligent on the report front. Yet here we are. The transatlantic divergence in material outcomes has been going on for two decades. And Europe was poorer to begin with.

The programmes suggested herein aim to build upon these efforts, focusing on ensuring the EU's technological resilience by empowering research and innovation across the EU, while also ensuring that European businesses are equipped to leverage these advancements for competitive advantage. Namely, the commercial exploitation of what is generally quite good European research has, to date, been lacking. This was identified decades ago in the Bangemann report:[7]

> Actions must be taken . . . to strike down entrenched positions which put Europe at a competitive disadvantage: it means fostering an entrepreneurial mentality to enable the emergence of new dynamic sectors of the economy; it means developing a common regulatory approach to bring forth a competitive, Europe- wide, market for information services; it does NOT mean more public money, financial assistance, subsidies, dirigisme, or protectionism.

State of play

European competitiveness, particularly in technology, has been a focal concern for policymakers and business leaders, as underscored in a report by the McKinsey Global Institute.[8] Over the past decade, there has been a growing divergence between Europe and leading global economies, particularly those of the US and China, in key technological and corporate performance metrics. Europe's ability to sustain growth, achieve strategic autonomy and maintain social welfare depends on bridging this gap. The report estimates that corporate value added of €2–€4 trillion a year could be at stake by 2040, which represents about one percentage point of growth annually or nearly 90% of current European social expenditure.[9]

The McKinsey report states that between 2014 and 2019, large European companies lagged behind their US counterparts by three percentage points in return on invested capital, grew 40% more slowly, and invested 40% less in research and development (R&D). This underperformance is particularly pronounced in technology-centric sectors but the weaknesses are not entirely sector-specific. Rather, there are issues with both the transversal technologies that permeate every industry and the ecosystem for doing business and innovating.

The report highlights 10 key transversal technologies: next-level automation, future of connectivity, distributed infrastructure, next-generation computing, applied AI, future of programming, trust architecture, bio-revolution, next-generation materials and future of cleantech. Of these, European performance is competitive only in cleantech and next-generation materials, and is particularly weak in information technology–related fields.

6 J. Ganesh, 'Why Europe Will Not Catch up With the US', *Financial Times*, 18 September 2024.
7 *Bulletin of the European Union*, 'Report on Europe and the Global Information Society', Supplement 2/94 (Brussels, 1994), 5–41.
8 McKinsey Global Institute, *Securing Europe's Competitiveness: Addressing its Technology Gap* (September 2022).
9 Ibid.

The evaluation of European technological excellence is summarised in the following table.

Table 1 Analysis of European technological excellence

Strengths	Weaknesses
• *Leadership in sustainability and cleantech*, including political commitment. • *High-quality education systems*, particularly in life sciences and engineering. • *Regulatory leadership* influencing international norms and promoting consumer trust. • *Strong social and economic inclusion*.	• *Lag in digital and AI investment*. • *Fragmented market and regulation* hinder the scaling of technologies. • *Slow adoption of transversal technologies*. • *Lower R&D investment in general* and particularly in high-impact sectors such as information and communications technology (ICT) and pharmaceuticals.
Opportunities	**Threats**
• *Scaling successful initiatives*, firms and technologies through greater integration of markets and regulatory environments. • *Increased collaboration*, leveraging public–private partnerships, particularly in defence, healthcare and digital infrastructure. • *Focus on strategic autonomy* in critical sectors such as semiconductors, defence, cybersecurity and digital infrastructure to reduce external dependencies. • *Capitalise on cleantech political leadership*.	• *Competition from the US and China*, particularly in digital and AI, where these countries dominate investment and market share. • *Disruption of transversal technologies* threatens Europe's traditional industrial strongholds, such as automotive and aerospace, if adaptation lags. • *Regulatory and bureaucratic hurdles* stifle innovation, slow market entry for new technologies and discourage investment. • *Risk of falling behind in critical technologies* such as AI, quantum computing and cybersecurity.

Priorities

As stated above, Europe risks being left behind, particularly in terms of transversal technologies such as AI, next-generation computing and advanced connectivity. These technologies are not confined to single industries; they shape entire sectors and economies, making Europe's lag all the more perilous. This thinking guides the selection of priority topics.

However, the greatest potential for transformative change lies in structural reforms to Europe's innovation and business ecosystem. The EU must dismantle regulatory barriers, foster cross-border collaboration and scale up successful initiatives to turn its fragmented market into a powerhouse of technological advancement. This focus guides the general horizontal mechanisms outlined in this paper.

Technological areas

Three technological topics have been selected:

1. *Digital*. ICT has been selected as it is a multiplier for productivity growth across the economy. Europe is currently behind in terms of R&D spending on ICT compared to the US, which invests about four times more. Bridging this gap is essential for fostering a dynamic and competitive technology ecosystem within the EU.

2. *Green*. Cleantech includes a range of technologies such as solar, wind, hydropower, nuclear fusion and hydrogen, all of which are crucial for the transition to a net-zero economy. It has been selected due to

the high political urgency of this transition and the support for it within the EU. The EU has the potential to lead in cleantech innovation, although it currently lags in production.

3. *Defence*. While one could select many other transversal technologies, the EU today does not have this luxury. Advanced defence technology is crucial for the EU amidst, on the one hand, the digitalisation of the battlefield and, on the other, the current global uncertainties. The use of such technology directly impacts the Union's ability to safeguard its strategic interests, ensure the security of its citizens, maintain stability within its borders and project strength beyond them. A robust and advanced defence technological base is essential for the EU to respond effectively and autonomously.

Structural horizontal mechanisms

Addressing the structural issues hindering Europe's technological competitiveness requires a comprehensive approach that focuses on three critical pillars: skills, innovation and entrepreneurial environment, and an integrated and dependable playing field.

The horizontal mechanisms and policies for the three pillars include the following:

- *Investing in talent and skills*. Everything starts with a focus on human capital, advocating for the enhanced development and attraction of talent, particularly in the science, technology, engineering and mathematics (STEM) fields and digital skills. This includes not only improving educational outcomes but also making Europe more attractive to top global talent, alongside policies that encourage innovation, creativity and entrepreneurship within the EU workforce.
- *Facilitating innovation and entrepreneurship*. This highlights the importance of fostering a more supportive regulatory environment that encourages disruption and innovation. This could involve streamlining regulatory processes, promoting risk-taking and entrepreneurship, and providing more substantial support for startups and scale-ups, including better access to finance and markets.
- *A dependable playing field*. Europe should achieve scale, increase efficiency and establish a dependable playing field to foster competitiveness and growth. This includes increasing and pooling resources within the EU and with other democracies to support cross-border scale-up and consolidation, balancing the precautionary principle with accelerated cost–benefit decision-making and ensuring fair competition for all market players, especially in the digital and tech sectors.

Policy recommendations

ICT in depth

The primary challenges stem from fragmented markets, lagging investment in key technologies, skills shortages, cybersecurity vulnerabilities and regulatory complexities. Addressing these challenges collaboratively offers the EU a path to enhancing its technological sovereignty, bolstering economic growth and ensuring its security in an increasingly interconnected world.

To catch up with global advancements in the digital domain, the EU must focus on several key areas. Deepening the digital market is essential, and requires the harmonisation of regulations across member states and support for initiatives such as the digital single market, which facilitates cross-border digital services. Alongside this, boosting investment in critical technologies such as AI, quantum computing and digital infrastructure should be prioritised, leveraging frameworks such as the European Innovation Council and the Digital Europe Programme to mobilise resources and foster public–private partnerships. Addressing the growing digital

skills gap is equally important, necessitating substantial investment in education and training, particularly in emerging technologies. Programmes such as the European Year of Skills and the Talent for Growth Task Force, which promote collaboration among governments, businesses and educational institutions, should play a pivotal role. Furthermore, in response to increasing cybersecurity threats, especially from the east, the EU must strengthen its cyber-defence by standardising regulations and investing in advanced cybersecurity technologies. Finally, simplifying regulatory frameworks is crucial, particularly in fast-evolving fields such as AI, where a more flexible, risk-based approach could balance the need for oversight with the fostering of innovation.

Cleantech in depth

Europe's transition towards a green economy requires a balanced approach that supports industries while advancing sustainability goals. A pragmatic, market-driven strategy is essential to avoid the pitfalls of greenwashing and economic degrowth, instead focusing on innovation, competitiveness and preserving the industrial base that underpins Europe's prosperity.

A successful market-driven green transition should be centred on innovation and technological neutrality, empowering industries to adopt the most efficient solutions, from advanced nuclear options such as small modular reactors to carbon capture and utilisation technologies, alongside renewable sources such as wind and solar.

This approach would prevent an over-reliance on specific technologies and would foster a variety of emissions-reduction strategies tailored to different sectors. To ensure genuine impact, cleantech developments must meet rigorous standards, with transparent reporting key to directing financial and policy support towards innovations that truly contribute to sustainability, thereby avoiding greenwashing or superficial solutions. It is also essential to protect industrial competitiveness by implementing green policies that are designed to avoid imposing disproportionate costs on businesses, thus ensuring they remain competitive globally and are not driven to relocate outside of Europe.

Market-based mechanisms, such as uniform carbon pricing, should play a key role in creating incentives for companies to innovate and reduce emissions efficiently, aligning with a preference for fewer regulations and a reliance on market forces to drive real change. Additionally, energy security and supply-chain resilience are critical to a sustainable transition, and require the diversification of energy sources and a reduced reliance on non-EU countries for essential materials and technologies.

Fostering a fair transition is equally important, ensuring that all regions, industries and communities benefit, particularly through the reskilling of workers from traditional sectors and providing targeted support for small and medium-sized enterprises (SMEs). Finally, the focus should be on promoting sustainable growth rather than degrowth, emphasising the idea that economic expansion and environmental protection can coexist. By leveraging innovation and market dynamics, Europe can pursue a green future that supports both environmental goals and economic prosperity.

Military technology in depth

Investment in military technology is crucial for the EU as it will strengthen the bloc's strategic autonomy, enhance its defence capabilities and ensure the security of its member states in an increasingly complex global security environment. Such investment not only supports the development of cutting-edge defence systems and innovations but also fosters collaboration among member states, driving forward a more integrated and

resilient European defence industry.[10] By bolstering its military technological edge, the EU aims to protect its interests, contribute to global stability and reduce its dependency on external powers for critical defence needs, aligning with its broader goals of strategic sovereignty and security self-reliance.

Collaborative actions to enhance the EU's defence capabilities require a unified approach across several dimensions. The EU must work towards a more coordinated defence procurement strategy by consolidating resources and reducing the duplication of efforts through the use of frameworks such as the European Defence Fund and the European Defence Industrial Development Programme. These initiatives facilitate joint investments in critical technologies, ensuring more impactful results.

Additionally, cybersecurity is a key focus, necessitating the development of a comprehensive EU strategy that enhances both offensive and defensive digital resilience. This involves greater investment in cyber-defence technologies, improved collaboration between member states and the integration of private-sector innovations into military operations.

Standardisation and interoperability efforts, such as expanding the High-Level Forum on European Standardisation to include dual-use technologies, are vital for enabling seamless joint operations and the rapid deployment of new technologies across borders. Moreover, prioritising investment in emerging technologies such as AI, quantum computing and autonomous systems is essential to maintaining the EU's competitiveness in future warfare landscapes.

Finally, achieving strategic autonomy through technological development requires reducing reliance on external suppliers by strengthening the European defence technological and industrial base through targeted funding and policy support, thus ensuring the EU's long-term security and sovereignty in critical areas such as advanced semiconductors and AI.

Conclusion

Europe stands at a pivotal moment where its technological future will determine not only its economic competitiveness but also its strategic autonomy and societal welfare. The technological landscape is rapidly evolving, with critical areas such as AI, next-generation computing and advanced connectivity defining the contours of global power and influence. Europe must act decisively, leveraging its strengths in sustainability and education, while addressing weaknesses in digital investment and market fragmentation. Structural reforms that foster a unified market, enhance cross-border collaboration and scale up successful initiatives are not optional but essential. Without a bold, integrated approach, Europe risks falling behind in key technological domains, imperilling its economic resilience and strategic influence in an increasingly interconnected world.

The EU's success in closing the competitiveness gap depends on its ability to create a conducive environment for innovation and entrepreneurship. Prioritising strategic autonomy in critical sectors, investing in talent and skills, and fostering a supportive regulatory landscape will be crucial. Europe's leadership in cleantech and sustainability offers a strong foundation, but it must expand this success to other critical technologies. The time for incremental change has passed; what is required now is a transformative vision that galvanises Europe's technological potential, securing its place as a leader in the global economy.

[10] S. Lorenzo Perez, L. Lazaro Cabrera and A. Duprat-Macabies, 'EU Tech Policy Brief: July 2024', *Center for Democracy and Technology*, 5 July 2024.

	Programme 1	Programme 2	Programme 3
	Growing ICT	**Making cleantech competitive**	**Bolstering defence**
Project 1	Enhance STEM education with a focus on integrating ICT competences. This could involve updating curricula, providing teacher training and investing in ICT resources within educational institutions to foster a tech-savvy generation. Create centres of excellence for higher education in STEM across Europe to attract talent from abroad.	Establish programmes that will approach sustainable development from a rational viewpoint—focusing on development and growth that can sustain itself and approach the climate-change problem from the perspective of mitigating the effects and reducing greenhouse gases where it is least expensive. In particular, focus on knowledge related to the circular economy and the regenerative economy.	Collaboration should be established between the defence sector and educational institutions. This includes promoting STEM education, as well as specialist training in emerging technologies relevant to defence. Moreover, providing continuous education and upskilling opportunities is critical as the defence sector evolves with new technologies such as quantum computing and digital twins.
Project 2	Establish low-red-tape incubation programmes that provide resources, mentorship and funding to ICT startups. These programmes should catalyse innovation by supporting entrepreneurs in developing and scaling viable technology solutions. Create a platform for best-practice sharing among member states.	Support the establishment of cleantech innovation hubs that bring together researchers, startups and investors to accelerate development. These hubs can provide essential resources, mentorship and networking opportunities to foster innovation and commercialise sustainable technologies, as seen in the Cleantech for UK initiative.	Create a robust ecosystem that integrates advanced technologies and entrepreneurial ventures into the defence sector. Promote dual-use technologies that have both civilian and military applications. Strengthen public–private partnerships including the European Defence Fund. Encourage startups and SMEs. Expand funding opportunities through initiatives such as the NATO Innovation Fund and the European Defence Industrial Development Programme, which supports early-stage innovators in developing new technologies relevant to defence.
Project 3	Carry out a review with the aim of reducing the regulatory burden on the EU's digital industry and making it comparable to those of competitors. Ensure fair market access for emerging ICT companies, prevent monopolistic practices and encourage competition.	Revise and institute new trade policies to deter EU businesses from offshoring their energy-intensive operations—a practice that, while diminishing the EU's apparent environmental footprint, undermines its industrial foundation without yielding global benefits. Existing initiatives such as the European Sovereignty Fund and the Green Deal Industrial Plan should evolve in this direction.	The EU defence industry should be bolstered through a combination of government procurement, regulatory modernisation and market-driven approaches. A common defence market, common procurement practices and common standards should be established. Interoperability standards should be set up. Targeted incentives, such as tax breaks and funding for R&D, could attract private-sector investment and encourage the participation of SMEs in the defence sector.

Bibliography

Capgemini, *Aerospace and Defence Technovision 2024 AD Sector Playbook* (2024), accessed at https://www.capgemini.com/wp-content/uploads/2024/07/TECHNOVISION-2024-AD-Sector-Playbook-web.pdf on 1 November 2024.

Česnakas, G., 'The Implications of the Technological Trends in Military on the Defence of Small States', *Lithuanian Annual Strategic Review* 17 (2019), 273–95, doi:10.2478/lasr-2019-0012.

Cisco, *Ten Point Tech Policy Plan 2024 Europe* (2024), accessed at https://www.cisco.com/c/dam/en_us/about/government-affairs/ten-tech-policies-to-power-the-future/documents/Cisco_Ten_Point_Tech_Policy_Plan_2024_Europe.pdf on 1 November 2024.

Bulletin of the European Union, 'Report on Europe and the Global Information Society', Supplement 2/94 (Brussels, 1994), accessed at https://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf on 13 November 2024.

Deloitte, 'Tech Trends 2024' (2024), accessed at https://www.deloitte.com/be/en/Industries/technology/about/tech-trends.html on 1 November 2024.

Digital Europe, *Europe, a Secure and Digital Powerhouse: Recommendations for the Digitalisation of Defence* (Brussels, 2024), accessed at https://cdn.digitaleurope.org/uploads/2024/06/DIGITAL-EUROPE-DEFENSE-REPORT-FINAL-WEB.pdf on 1 November 2024.

Eckert, D., *Forgotten Lessons: The European Digital Policy Journey – 1980–2020* (Cham: Springer, 2024).

European Commission, 'A Europe Fit for the Digital Age' (2024), accessed at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit- digital-age_en on 1 November 2024.

European Commission, 'AI Act' (updated 14 October 2024), accessed at https://digital- strategy.ec.europa.eu/en/policies/regulatory-framework-ai on 1 November 2024.

European Commission, 'Data Act' (updated 10 October 2024), accessed at https://digital- strategy.ec.europa.eu/en/policies/data-act on 1 November 2024.

European Commission, 'EU Cyber Resilience Act' (updated 8 July 2024), accessed at https://digital- strategy.ec.europa.eu/en/policies/cyber-resilience-act on 1 November 2024.

European Commission, 'European Chips Act', accessed at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit- digital-age/european-chips-act_en on 1 November 2024.

European Commission, 'Europe's Digital Decade: Digital Targets for 2030', accessed at https://commission.europa.eu/strategy-and-policy/priorities-2019- 2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en on 1 November 2024.

European Commission, 'Horizon Europe' (2024), accessed at https://research-and- innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and- open-calls/horizon-europe_en on 3 July 2024.

European Commission, 'Research and Innovation Strategy 2020–2024', accessed at https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024_en on 1 November 2024.

European Commission, 'Shaping Europe's Digital Future' (2024), accessed at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit- digital-age/shaping-europes-digital-future_en on 1 November 2024.

European Commission, 'The Digital Markets Act' (2024), accessed at https://digital- markets-act.ec.europa.eu/index_en on 1 November 2024

European Commission, 'The Digital Services Act Package' (updated 4 October 2024), accessed at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package on 1 November 2024

European Commission, 'The New European Innovation Agenda' (2024), accessed at https://research-and-innovation.ec.europa.eu/strategy/support-policy-making/shaping-eu-research-and-innovation-policy/new-european-innovation-agenda_en on 1 November 2024

European Conservatives and Reformists Group, *ECR Priorities 2024–2029* (2024), accessed at https://ecrgroup.eu/files/EN_ECR-Priorities_2024-2029.pdf on 1 November 2024

Ganesh, J., 'Why Europe Will Not Catch up With the US', *Financial Times*, 18 September 2024.

Hartzell, C. L., 'Future Weapons Technology of 2040', *NCO Journal*, accessed at https://www.armyupress.army.mil/Journals/NCO-Journal/ on 1 November 2024.

Hexagon AB, *The Future of Defence Technologies: 10 Trends and Predictions to Watch* (2023), accessed at https://bynder.hexagon.com/m/5903c1bc22b9a297/original/Hexagon_GSP_The_future_of_defense_technologies_10_trends_white_paper.pdf on 1 November 2024.

ITI, *ITI Policy Recommendations for a European Tech Agenda* (2024), accessed at https://www.itic.org/policy/ITIPolicyRecommendationsforaEuropeanTechAgenda.pdf on 1 November 2024.

Lorenzo Perez, S., Lazaro Cabrera, L. and Duprat-Macabies, A., 'EU Tech Policy Brief: July 2024', *Center for Democracy and Technology*, 5 July 2024, accessed at https://cdt.org/insights/eu-tech-policy-brief-july-2024/ on 1 November 2024.

McKinsey Global Institute, *Securing Europe's Competitiveness: Addressing Its Technology Gap* (September 2022), accessed at https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf on 1 November 2024.

NATO Science & Technology Organization, *Science & Technology Trends: 2023– 2043, Volume 1: Overview* (2023), accessed at https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf on 1 November 2024.

NATO Science & Technology Organization, *Science & Technology Trends: 2023- 2043, Volume 2: Analysis* (2023), accessed at https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf on 1 November 2024.

Implementing the EU AI Act: How Soon Is Now?

by Anastas Punev

Summary

This paper reflects on the future implementation of the EU Artificial Intelligence (AI) Act and mainly focuses on its possible drawbacks, which could undermine the visionary idea of instituting the first comprehensive regulation on AI. Drawing on comparisons between the AI Act and similar legislative attempts at regulating global phenomena, recommendations are made as to how to adapt the AI Act to foster EU leadership.

Keywords AI Act – AI liability – GPAI

The future of the AI Act: GDPR déjà vu?

The Artificial Intelligence (AI) Act was a result of 3 years of discussion and exactly 3,312 proposed amendments. In the proud words of Thierry Breton, the former European Commissioner for Internal Market, the political deal that produced the Act made the EU 'the first continent to set clear rules for the use of AI'.[1] Some of the key messages used to portray the novelty of the AI Act, however, are instantly reminiscent of a similar 'global first' model legislation—the General Data Protection Regulation (GDPR). Among the main features of the AI Act are the 'robust enforcement framework', the tough penalties for non-compliant businesses and the establishment of a new institution: the EU AI Office at the European Commission. All these measures are instantly comparable to the GDPR, which was also aimed at balancing fundamental rights and innovation, thus fostering the EU's global role. Unfortunately, the GDPR's goals have been undermined to a large extent by poor enforcement. Therefore, comparing the two seems appropriate, as the enactment of the AI Act, in its definitional, substantive and institutional aspects, has already been labelled as 'GDPR mimesis'.[2]

Extensive research shows that millions of European small and medium-sized enterprises (SMEs) have not complied with the excessive burdens provided by the GDPR, and this has thrown into question the purpose and future impact of the regulation.[3] Additionally, there was a considerable lack of consistency among the member states in implementing the GDPR, which only exacerbated the bureaucracy and created the impression that the regulation was forcing numerous extraneous duties on companies. Such risks are, unfortunately, also attributable to the AI Act. Not only does it lack a preliminary analysis of its future implementation, but the whole design of the Act appears comparable to the GDPR. That is, it treats technology as something that merely needs better organisation: AI systems must be labelled and then monitored to reduce their negative effects.[4] This is confirmed by the lack of calculation of the financial burden companies face to comply with the legislation. This issue has already been raised by trade associations such as Digital Europe, which referred to the AI Act as 'uncharted territory'.[5]

1 T. Breton, 'The European AI Act Is Here!', *LinkedIn*, 9 December 2023.
2 V. Papakonstantinou and P. de Hert, 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI', *European Law Blog*, 1 April 2024.
3 GDPR.EU, *2019 GDPR Small Business Survey* (May 2019).
4 V. Papakonstantinou, 'The AI Act and a (Sorely Missing!) Right to AI Individualization; Why Are We Building Skynet?', *European Law Blog*, 16 July 2024.
5 G. Kaur, 'Concerns Remain Even as the EU Reaches a Landmark Deal to Govern AI', *CIO*, 11 December 2023.

The future simultaneous application of the AI Act and the GDPR has also caused controversy even before the entry into force of the new regulation. The requirements of both acts can be interpreted in a mutually contradictory manner because their goals cannot be entirely reconciled. While the AI Act presupposes that AI systems need large amounts of data, it also allows limitless data processing, which can contravene the explicit consent required under Article 9 of the GDPR. And the Act does not contain any clear instructions on how personal data from publicly available sources will be collected for the mandatory self-training, validation and testing of AI systems, which are the main ways in which these systems can be improved.[6]

Furthermore, Article 6 of the AI Act expressly grants the Commission the power to classify AI systems as high-risk by providing a 'comprehensive list of practical examples'. Such an extensive power, without any further narrowing of its scope, could hinder the enforcement of the Act, considering the Commission's lack of sufficient technical expertise. Here the GDPR is once again a useful reference as its implementation has already shown that safeguarding the rationale of the law without straying into over-regulation is better achieved by activists with sector expertise. Yet, the voice of individual users is not heard in the Act. The legislation could provide, among other things, an ombudsperson or a similar body entrusted with directly representing users in situations involving enforcement.[7] No less important is that the AI office's powers could lead to a duplication of roles and, as a result, to inefficiency and a lack of clarity regarding responsibilities. The recent controversy related to the investigation into how X handled the Israel–Hamas conflict revealed how significant misapprehension arose out of the confusion over which body had authority for what: the Commission team overseeing the Digital Services Act or the separate unit in charge of a voluntary EU code to guard against disinformation.[8]

Balance of responsibilities, foundation models and fundamental rights

Another widely disputed issue surrounding the entry into force of the AI Act is that of responsibility, since the Act is intended as product safety legislation whose main aim is to reduce the risk of the potentially dangerous use of AI. In this regard the AI Act focuses mainly on the prohibitions and limitations to be applied to AI. It proceeds by adopting a detailed risk-based approach, placing AI systems into four risk categories depending on their use: unacceptable-risk, high-risk, limited-risk, and minimal- or no-risk. Conversely, there are specific requirements for foundation AI models[9] capable of performing a wide range of distinct tasks, irrespective of their risk categorisation.

According to the European Council's official statement, mirrored in the AI Act, the rules on high-risk systems apply to general purpose AI (GPAI) models that can be used in contexts involving significant risk unless such uses are explicitly excluded. This is further reflected in the vague language of the law, according to which a GPAI model can be classified as containing 'systemic risk' on the basis of criteria such as 'high-impact capabilities'. Therein lies the main challenge in implementing the AI Act without hindering innovation. One and the same AI model can simultaneously enable care robots and lethal weapons. Thus, many models can be placed in the high-risk category even if only one of their general uses turns out to involve a high degree of risk.[10] This seems even more dangerous for open-source foundation models as the description of their requirements is very generic compared to the intricate descriptions of the (various) risks set out in the AI Act. This could easily lead to ambiguous interpretations. For this reason, it has rightly been proposed that mitigation measures should focus solely on the potential future uses of the technologies so that continuous adaptation is allowed.[11]

---

6 S. Wadhwani, 'Last Mile Trouble: What Needs to Be Sorted in EU AI Act Before Next Week's Trilogue Talks', *Spiceworks*, 29 November 2023.
7 L. Edwards, *Regulating AI in Europe: Four Problems and Four Solutions*, Ada Lovelace Institute (March 2022), 11.
8 M. Scott, 'The EU's Online Content Rulebook Isn't Ready for Primetime', *Politico*, 14 February 2024.
9 A foundation model (also known as general-purpose AI or GPAI) is an AI model designed to produce a wide and general variety of outputs. As such, it differs from narrow AI systems which focus on a specific task.
10 C. Djeffal, 'The EU AI Act at a Crossroads: Generative AI as a Challenge for Regulation', *European Law Blog*, 24 July 2023.
11 Ibid.

Concerning innovation and liability, the one-size-fits-all approach of the AI Act is particularly impractical for providers of mostly decentralised open-source AI systems. This is especially true given the excessive regulatory burden, which could be difficult to comply with. For example, the requirement to maintain 10 years of documentation is practically impossible to implement as open-source systems by definition allow other agents to modify the software and thus break the chain of liability. A more reasonable approach would be to regulate specific high-risk AI applications and not the underlying GPAI models. This could balance the AI Act's goals with the threats and would not discourage new possible fields for the application of AI, especially for SMEs, which should not be faced with excessive costs and obstacles.[12] Furthermore, while the levels of risk are defined in the Act, the allocation of responsibility among the different providers throughout the various stages involved in the use of AI remains vague and thus unpredictable for businesses from the outset. In fact, 'AI' is even disputed as a meaningful term because it is neither a product in the traditional sense of the word (as expressly recognised by the AI Act) nor a one-off service but a dynamic system that moves through a series of stages which make up the AI life cycle.[13]

Even more importantly, there are large groups of people that are not sufficiently addressed in the Act, such as those mostly impacted by the AI models: consumers, data subjects and end users. They have been left in the dark as their role as rights-holders is not expressly guaranteed and protected. For example, users buying a system off the shelf will most certainly not regard themselves as responsible for the 'substantial modification' necessary for them to become regarded legally as providers, and so they could fall under the scope of the Act even without realising it.[14] Precisely for this reason, the product safety framework of the Act is not suitable for the possible violations of fundamental rights in an AI context. In product safety legislation any adverse risk can supposedly be calculated by measuring the likelihood of an event and its effects, but this is largely impossible when it comes to AI. A braver step in guaranteeing fundamental rights would have been, for example, to declare that every human being has property rights to their genetic data and personal identifiable information.[15]

Even if such ideas are not implemented in the future, some of the carve-outs and the broad definitions of the AI Act should at least be clarified as they constitute a clear threat to individual rights. For example, emotional recognition or biometric categorisation could still be used in law enforcement under somewhat murky circumstances.[16] Similarly, the EU AI Office will be empowered to explain fundamental categories such as transparency obligations 'when deemed necessary'—a dangerous and possibly far-reaching notion that only expands the regulatory space at the expense of individual rights.[17] Even organisations such as the Office of the United Nations High Commissioner for Human Rights have already underlined that the risk-dependent formula of the AI Act must be related to adverse impacts on human rights and not to mere technical specifications.[18]

12 A. Prabhakar, 'The EU AI Act Is a Cautionary Tale in Open-Source AI Regulation', *Center for Data Innovation*, 20 November 2023.
13 Edwards, *Regulating AI in Europe*, 6.
14 Ibid., 7.
15 Kaur, 'Concerns Remain'.
16 M. V. Bravo, 'What U.S. Regulators Can Learn From the EU AI Act', *Electronic Privacy Information Center*, 22 March 2024.
17 B. Martens, 'The European Union AI Act: Premature or Precocious Regulation?', *Bruegel*, 7 March 2024.
18 V. Türk, 'Open Letter From the United Nations High Commissioner for Human Rights to European Union Institutions on the European Union Artificial Intelligence Act', Office of the United Nations High Commissioner for Human Rights, 8 November 2023.

The political impact of the AI Act

As is evident from the above considerations, AI is another battlefield where the clash between market forces will have very clear implications for the overall exercise of power, especially in a geopolitical sense. From this perspective, the AI Act has a key role in establishing the EU's position as a pioneer in AI legislation. The Act is being adopted at a very critical point in time because China has already introduced its AI legislation, and the US is still considering its own approach. If two models have already been established, it is hard to imagine that US companies will opt for a third one that would differ considerably and increase the risk of non-compliance.[19] Thus, the EU AI Act represents one of the few opportunities for the Union to demonstrate the 'Brussels effect' and achieve a global first. Moreover, the nature of AI is decentralised and universal, so the area of impact of the AI Act is wider than the EU single market, thus leading to a possible first-mover advantage.[20] In this regard, the EU has a unique role, as the Sino-US tech rivalry is igniting, and the Union act as a bridge between the two superpowers since AI is a matter of global governance. An already established principle is that AI governance is only as good as the worst-governed country.[21]

However, the EU seems to rely on this 'universal' character of the EU AI Act too much, as if that renders the Act unavoidable for its global competitors, while stakeholders have already expressed their doubts about the Act, even before its entry into force. For instance, Sam Altman, OpenAI's CEO, admitted that if compliance proves unfeasible, OpenAI might cease its operations in the EU.[22] In light of this, the Brussels effect bears the parallel risk of a 'Brussels side effect': the shortcomings related to the EU regulatory approach might be accepted outside the EU but at the cost of their negative spread across the globe.[23] Thus, the AI Act model might be successful in imposing widely accepted standards, but the result would be a non-stringent regulation ill-suited to defend fundamental rights.

The Chinese model, on the other hand, does not aim for global supremacy but is mostly pragmatic in its aims, adhering to a 'vertical strategy' in which regulations are tailored to certain AI applications. Its main short-term advantage would be the more relaxed regulatory environment.[24] This is the opposite of the AI Act's horizontal model whereby a wide range of technological applications is encompassed under a single legislative framework. OpenAI's product ChatGPT offers a good illustration of the possible advantages of a vertical model of legislation—it has already demonstrated the promise of large language models and made many of the EU's earlier legislative efforts obsolete.[25] It would be a missed opportunity if the EU were to decide not to include more agility in its quest for future-proof regulation. This is even more concerning from a political standpoint because it is hardly imaginable that the Commission would reopen the AI Act for revision soon after its adoption. In sum, the EU should be strict only when it comes to measures that (1) offer real regulatory advantages over the Chinese model (or any other framework that may be developed in the future); and (2), if compliance with them cannot be guaranteed, at least cannot be easily circumvented.

19 G. S. Özdemir, 'Navigating the EU AI Act: Exploring Challenges Amidst the Evolving Global Regulatory Landscape', *SETA*, December 2023.
20 Edwards, Regulating AI in Europe, 2.
21 A. Zhang, 'The Promise and Perils of China's Regulation of Artificial Intelligence', *Columbia Journal of Transnational Law* (forthcoming), 36.
22 Özdemir, 'Navigating the EU AI Act'.
23 M. Almada and A. Radu, 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy', *German Law Journal 25/4 (2024), 647.*
24 Zhang, 'The Promise and Perils of China's Regulation', 7.
25 M. Mema, 'The EU AI Act: Two Steps Forward, One Step Back', *Global Governance Institute*, 19 March 2024.

Policy recommendations

The above considerations show that the EU AI Act should be treated cautiously at this initial stage of implementation. Although comprehensive regulation is needed, AI policy should be more concise and angled slightly differently. Whether these adjustments will happen depends largely not only on the Act's future application and interpretation by courts and the executive, but also on the interaction between it and its US and Chinese counterparts, and the upcoming supplementary acts detailing important aspects of the regulation. This is why there is still room for progress if the EU can demonstrate that the AI regulation will be adopted not against but in support of innovation.

The most important point is that the use of AI demands not only detailed regulation but also a workable solution that can be reasonably implemented. Therefore, the AI Act should address the capacity of SMEs to comply with the Act in terms of costs and organisational measures. This needs to be done before it is too late, because otherwise these companies will be forced to reckon with its far-reaching requirements. This necessitates minimal political intrusion from the EU authorities, mostly in labelling the risks posed by the various AI models, but also in avoiding making sudden and abrupt amendments to the regulatory framework. Here responsibility should be distributed between institutions at the EU and national levels after researching their potential interplay.

Considering the predictability of the AI Act, which is key to its success, the issue of liability should be treated more clearly, and the main strategy should be to shift the risk profile of an AI system away from its intended application. The distribution of liability between the service providers should be delineated so that there are no doubts about who is responsible for what during the AI life cycle. The most important reference point is that liability will be related to the use of the AI product and not to its foundation model. This implies that the focus of the AI Act will be shifted away from threatening and imposing large sanctions on companies and to consumers and their fundamental rights.

AI will in any case play an important part in the global role of the EU and its relationship with the US and China. Therefore, the AI Act is a matter not only of law but also diplomacy and leadership, which are even more important when it comes to global topics such as AI. For this reason, the enforcement of the AI Act should be supplemented by deepening EU–US cooperation and should use all the necessary instruments, including the transatlantic Trade and Technology Council and the G7 Hiroshima AI Process on priority risks.

Conclusion

The future is never certain. Nobody can be entirely prepared for the rapid technological progress of AI models and the unimaginable risks arising from their use. However, a good first step is to consider AI in its ever-changing nature: not as a danger to be reckoned with but as a necessary step in technological development. This step should be guided less by inflexible institutions than by free-market initiative and guarantees for individual rights. In any case, the EU AI Act might be one of the last chances for the Union to lead the way, and its success or failure will most certainly have a major impact on European policy.

	Programme 1	Programme 2	Programme 3
	Enforcing the EU AI Act	**Reducing unpredictability and the excessive burden for businesses**	**Ensuring Europe's leading role globally**
Project 1	Evaluate the capacity of SMEs to comply with the Act before its entry into force. Limit the political intrusion of EU authorities into approving which organisations will review and certify high-risk AI systems.	Consider exempting from certain obligations open-source models which are decentralised and can vary in their purposes. Evaluate the fines imposed by the AI Act. Focus on how adequate they are and whether they might have a stifling effect, taking into account the amount of money involved and the stringency with which they are to be imposed.	Deepen EU–US cooperation on mitigating the global risks of AI proliferation and the nefarious use of advanced biotechnologies. Make use of the transatlantic Trade and Technology Council to expand joint work on risk taxonomies, common standards and aligning key policies. Reinforce the EU's role in expanding the G7 Hiroshima AI Process on priority risks, guiding principles for AI systems and responsible AI tools.
Project 2	Analyse the interplay between the AI Act and the GDPR so that they can be applied systematically to the collection of data by AI systems.	Promote legislation which outlines the distribution of liability between different service providers. Develop a genuine assessment of risk which is grounded in clear renewable criteria that mirror technological developments. Analyse the established case law on the GDPR concerning the allocation of responsibility and adapt it to the needs of AI providers.	Promote the EU model as a 'global first' by emphasising the AI Act's advantages, without highlighting the tough penalties to businesses as the major selling point. Expand international agreements on data and digital cooperation with like-minded countries and attempt to 'export' some of the main provisions of the AI Act.
Project 3	Evaluate the scope of powers of the EU-level authority in light of the budget required and the distribution of responsibility between the EU and the national institutions.	Safeguard the fundamental rights of users by focusing on their freedoms (e.g. from property rights to genetic data) instead of treating AI only in terms of product safety. Provide inviolable individual rights and efficient procedures for the protection of consumer rights, e.g. by consolidating patterns of complaints.	Adopt a more vertical approach to AI applications and groups, especially in comparison to the pragmatic Chinese model.

Bibliography

Almada, M. and Radu, A., 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy', *German Law Journal* 25/4 (2024), 646–63

Bravo, M. V., 'What U.S. Regulators Can Learn From the EU AI Act', *Electronic Privacy Information Center*, 22 March 2024, accessed at https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/ on 25 August 2024.

Breton, T., 'The European AI Act Is Here!', *LinkedIn*, 9 December 2023, accessed at https://www.linkedin.com/pulse/european-ai-act-here-thierry-breton-gcnre/ on 25 August 2024.

Djeffal, C., 'The EU AI Act at a Crossroads: Generative AI as a Challenge for Regulation', *European Law Blog*, 24 July 2023, accessed at https://www.europeanlawblog.eu/pub/the-eu-ai-act-at-a-crossroads-generative-ai-as-a-challenge-for-regulation/release/1?readingCollection=65b658d5 on 10 October 2024.

Edwards, L., *Regulating AI in Europe: Four Problems and Four Solutions*, Ada Lovelace Institute (March 2022), accessed at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf on 25 August 2024.

GDPR.EU, *2019 GDPR Small Business Survey* (May 2019), accessed at https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf on 24 August 2024.

Kaur, G., 'Concerns Remain Even as the EU Reaches a Landmark Deal to Govern AI', *CIO*, 11 December 2023, accessed at https://www.cio.com/article/1255863/concerns-remain-even-as-the-eu-reaches-a-landmark-deal-to-govern-ai.html on 24 August 2024.

Martens, B., 'The European Union AI Act: Premature or Precocious Regulation?', *Bruegel*, 7 March 2024, accessed at https://www.bruegel.org/analysis/european-union-ai-act-premature-or-precocious-regulation on 26 August 2024.

Mema, M., 'The EU AI Act: Two Steps Forward, One Step Back', *Global Governance Institute*, 19 March 2024, accessed at https://www.globalgovernance.eu/publications/the-eu-ai-act-two-steps-forward-one-step-back on 25 August 2024.

Özdemir, G. S., 'Navigating the EU AI Act: Exploring Challenges Amidst the Evolving Global Regulatory Landscape', *SETA* (December 2023), accessed at https://www.setav.org/en/assets/uploads/2023/12/P72En.pdf on 25 August 2024.

Papakonstantinou, V., 'The AI Act and a (Sorely Missing!) Right to AI Individualization; Why Are We Building Skynet?', *European Law Blog*, 16 July 2024, accessed at https://www.europeanlawblog.eu/pub/04y8qbam/release/1 on 10 October 2024.

Papakonstantinou, V. and de Hert, P., 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI', *European Law Blog*, 1 April 2024, accessed at https://www.europeanlawblog.eu/pub/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/release/1 on 10 October 2024.

Prabhakar, A., 'The EU AI Act Is a Cautionary Tale in Open-Source AI Regulation', *Center for Data Innovation,* 20 November 2023, accessed at https://datainnovation.org/2023/11/the-eu-ai-act-is-a-cautionary-tale-in-open-source-ai-regulation/ on 24 August 2024.

Scott, M., 'The EU's Online Content Rulebook Isn't Ready for Primetime', *Politico*, 14 February 2024, accessed at https://www.politico.eu/article/european-union-digital-services-act-dsa-thierry-breton/ on 25 August 2024.

Türk, V., 'Open Letter From the United Nations High Commissioner for Human Rights to European Union Institutions on the European Union Artificial Intelligence Act', Office of the United Nations High Commissioner for Human Rights, 8 November 2023, accessed at https://www.ohchr.org/en/open-letters/2023/11/turk-open-letter-european-union-highlights-issues-ai-act on 24 August 2024.

Wadhwani, S., 'Last Mile Trouble: What Needs To Be Sorted in EU AI Act Before Next Week's Trilogue Talks', *Spiceworks*, 29 November 2023, accessed at https://www.spiceworks.com/tech/artificial-intelligence/articles/eu-ai-act-in-trouble/ on 25 August 2024.

Zhang, A., 'The Promise and Perils of China's Regulation of Artificial Intelligence', *Columbia Journal of Transnational Law* (forthcoming), accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4708676 on 27 August 2024.

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.

About the authors

Amelia Andersdotter is Senior Advisor at Swedish cloud-service provider Safespring. Previously she was the Senior Standards Manager at Sky Group, ensuring the strong representation of operator interests in wireless local area network standardisation, especially with regard to energy saving in home networks. Amelia was a Member of the European Parliament in the seventh legislature and a member of the Multistakeholder Advisory Group of the Internet Governance Forum between 2013 and 2016. She is a graduate in Mathematics and Mathematical Statistics from Lund and Uppsala Universities, and has a degree in Business Law from Lund University.

Anastas Punev holds a Ph.D. in Law and is a practising lawyer in the field of civil and commercial law. He is also an Honorary Assistant Professor in Sofia University's faculty of law. His main interests are in the field of civil procedure, as well as the new legal challenges posed by technological innovation. Anastas is a Research Associate at the Wilfried Martens Centre for European Studies.

Dimitar Lilkov is a Senior Research Officer at the Wilfried Martens Centre for European Studies. His research focuses on energy and climate as well as digital policy. His specific fields of expertise cover the European Energy Union, energy security and decarbonisation policies. On the digital front, his research topics include novel European regulation in the online domain, privacy and disinformation, as well as technological competition with the People's Republic of China. Dimitar has a master's degree in Politics and Government in the EU from the London School of Economics and holds a BA in International Relations from Sofia University.

Milda Kaklauskaitė is a Senior Manager at the European Cyber Security Organisation. Her fields of expertise cover support for small and medium-sized enterprises, market deployment, cybersecurity investments and international cooperation. She has previous professional experience at the Wilfried Martens Centre for European Studies and in the Parliament of the Republic of Lithuania. Milda holds a degree in International Relations from the Central European University and is also a graduate of Vilnius University.

Žiga Turk is a Professor at the University of Ljubljana, Slovenia. He holds degrees in Engineering and Computer Science. As an academic he studies design communication, Internet science and future global development scenarios, particularly those related to the role of technology and innovation. He is an internationally recognised author, public speaker and lecturer on these subjects. Žiga has been Minister for Growth and Minister of Education, Science, Culture and Sports in the government of Slovenia, and was Secretary General of the Felipe Gonzalez's Reflection Group on the Future of Europe.