#FocusFuture

The 7Ds for Sustainability

Debt
Decarbonisation
Defence
Democracy
Demography
De-risking Globalisation

Digitalisation IN DEPTH

Wilfried
Martens Centre
for European Studies

The 7Ds for Sustainability - Digitalisation in Depth

Authors :

Amelia Andersdotter
Milda Kaklauskaitė
Dimitar Lilkov
Anastas Punev
Žiga Turk

Editors :

Peter Hefele
Dimitar Lilkov
Klaus Welle

April 2024

Credits

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party, dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

Wilfried Martens Centre for European Studies

Rue du Commerce 20
Brussels, BE 1000

For more information, please visit www.martenscentre.eu.

Assistant Editors: Sara Pini, Senior Research Officer & Theo Larue, Editorial and Publications Officer
Cover design: Gëzim Lezha, Brand and Visual Communications Officer
External editing: Communicative English bvba
Typesetting: Victoria Agency
Printed in Belgium by INNI Group

This publication receives funding from the European Parliament.

The European Parliament and the Wilfried Martens Centre for European Studies assume no responsibility for facts or opinions expressed in this publication or their subsequent use. Sole responsibility lies with the author of this publication.

Table of contents

Table of acronyms

5 G	Fifth generation technology standard for cellular networks
AI	Artificial Intelligence
CMU	Capital Markets Union
DSA	Digital Services Act
DSM	Digital Single Market
EV	Electric Vehicle
Fintech	Financial technology
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
ITU	International Telecommunications Union
O-RAN	Open Radio Access Network
R&D	Research and Development
SME	Small and Medium Sized Enterprise
STEM	Science, Technology, Engineering and Mathematics
TTC	Trade and Technology Council

Introduction

Peter Hefele

Alongside the Green Deal and the first steps towards a Defence Union, creating a single European digital space has been a key project of the outgoing European Commission (2019–24). This has 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 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 (R&D) 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 health care. 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.

In 2023, the Martens Centre published its *7Ds for Sustainability* strategy document. This text comprised 175 proposals for the next legislature to future-proof EU policy in the areas of debt, decarbonisation, defence, democracy, demography, de-risking globalisation, and digitalisation. Sustainability was chosen as the guiding principle to ensure that the policies reconcile the needs of both the present and the future, and systematically include the interests of the next generations.

The *7Ds* document has already inspired reflection on what to do over the next five years. These discussions are based on Christian Democrat and conservative thinking and the available in-house expertise of the Martens Centre. For the next phase of intense discussions about the programme to be implemented during the 2024–9 legislature, the Martens Centre has invited renowned external experts to put forward their own, more extensive proposals based on the original document, thereby deepening the available expertise. It is hoped that these proposals, published at the beginning of April 2024, will help to clarify the way forward at a critical juncture, when the European Parliament, the European Commission and the European Council are negotiating on and finalising their strategic priorities.

Rolling Out Secure Digital Infrastructure and Hardware

Amelia Andersdotter

To manage the complex cyber-environment around cloud infrastructures, the Internet of things and 5G networks, the EU will need to agree on a proactive strategy. Establishing and protecting EU capabilities 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).

This brief sets out nine areas of action for EU policymakers in the upcoming five years. They range from the practical, highlighting the need for the EU to build capacity in the governance of open technology collaborations, to the visionary, asking that Western European markets be opened to Central and Eastern European players (e.g. Revolut in Fintech, Workable in HR management, Seznam in Internet search, ESET in cybersecurity and Digi Communications in the mobile sector). 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. In a similar vein, the EU should explore how to enable service scaling directly in the European market. Too often, European companies scale their services by launching in their home state, then the UK and the US, before returning to launch in non–home-state EU markets.

Governance tools such as procurement, standardisation and certification are already in place, waiting to be used. But the EU is having to answer crucial questions about these, such as how to transform its legally established values into verifiably testable criteria for technology. On the fast-paced digital markets, product cycles are often shorter than the time required to certify. Self-certification against objectively established criteria would address such concerns. Adequately specified infrastructures can also serve to facilitate migration between or the simultaneous use of several technical infrastructures.

Finally, in applying these existing tools, the EU will have to develop a new culture of risk. Not every investment will succeed, but we can learn from all investments. It is through leveraging such learning that the EU can establish itself as a global leader in and internal enabler of cyber-excellence.

	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 to address shared challenges can 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, emphasising 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 properties 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 a national network. Make the operation of a commercial system independent from features available from only one, single upstream supplier (e.g. lock-in mechanisms, or vendor-specific application programming interfaces, *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 start-ups. 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 exploring 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: replicate experiences in the Fintech sector with open application programming interfaces for specific bank payment systems in the 2010s; or from the wireless local area network sector when microwave bands were opened up to licence-exempt use in the 1990s.

Completing the European Digital Single Market

Milda Kaklauskaite

The Digital Single Market (DSM) is a cornerstone of EU policy. The objective is to unify digital regulations and infrastructure across member states to promote innovation, economic growth and competitiveness. As the digital landscape evolves, it is imperative to refine and complete the DSM to address emerging challenges and capitalise on new opportunities. This chapter outlines policy priorities focused on fostering Europe's tech start-up and small and medium-sized enterprise (SME) ecosystem, attracting private investment, and enhancing technological independence and the cybersecurity posture across the EU. A strong DSM will ensure that Europe remains at the forefront of the global digital economy.

Streamlining bureaucracy and reducing fragmentation are paramount to nurturing Europe‘s tech start-up and SME ecosystem. By introducing an 'EU Company' status, the Union could pave the way for seamless cross-border operations, liberating businesses from the shackles of administrative burdens and enabling rapid market entry. Moreover, incentivising large businesses to embrace innovative European solutions is essential. Through collaborative platforms and targeted incentives, we could foster a culture of cooperation, empowering homegrown companies to gain market traction and credibility. Furthermore, democratising access to data is key. By facilitating data pooling and sharing, we empower smaller players, levelling the playing field and bolstering their competitiveness on a global scale.

Moreover, to fuel the growth of European start-ups, we must ensure a conducive investment environment. Completing the Capital Markets Union (CMU) is vital as this would eradicate barriers and facilitate the free flow of venture-capital investments across borders. Additionally, aligning European pension funds with the continent‘s burgeoning start-up scene holds immense potential. By incentivising these funds to support venture-capital firms and growth companies, we could unlock a vast pool of capital, driving innovation and economic growth. Furthermore, harmonising insolvency proceedings across EU member states would increase investors' confidence, fostering cross-border investment and a culture of risk-taking and entrepreneurship.

In an era defined by digital interconnectedness, cybersecurity stands as a cornerstone of our digital sovereignty. Thus, investing in cybersecurity training programmes is essential. By upskilling and reskilling our workforce, we could cultivate a robust cadre of cybersecurity professionals, equipped to defend against evolving threats. Furthermore, establishing a pan-European public–private fund-of-funds dedicated to cybersecurity is essential. This initiative would not only foster innovation but also safeguard Europe's digital landscape, ensuring resilience in the face of cyber adversaries. Finally, harmonising public procurement rules across member states would also bring added benefit. By incentivising the adoption of European cybersecurity solutions, we bolster our collective security and reduce dependencies on non-European suppliers.

	Programme 1	Programme 2	Programme 3
	Fostering Europe's tech start-up 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 a 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 to gain market traction and establish credibility among potential customers. Matchmaking platforms 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. By aligning the interests of pension funds with the growth of European start-ups, we can 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, it is imperative to promote collaborative investments among both public and private entities across the EU, ensuring robust protection against evolving cyber-threats and advancing Europe's digital agenda.
Project 3	Strengthen the access of European players 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 member states 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 the EU to provide more assurance among investors investing 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.

Enhancing European Technological Excellence

Žiga Turk

This chapter is based on the policies encapsulated in the Europe Fit for the Digital Age initiative, the comprehensive strategies underpinning the 2021–7 Horizon Europe programme and the McKinsey analysis. It argues that the EU needs to ensure the resilience of its technological sector by empowering research and innovation across the Union, while also helping European businesses leverage these advancements for competitive advantage. To date, the commercial exploitation of what is generally quite good European research has been lacking. This had already been identified 30 years ago in the Bangemann report: ‘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; it does NOT mean more public money, financial assistance, subsidies, dirigisme, or protectionism’.

The strategy delineates efforts in three critical technological domains and adopts three overarching methodologies. First, Information and Communication Technologies (ICT) is a multiplier for productivity growth across the economy. When it comes to R&D spending in ICT, Europe is currently behind the US, which invests about four times more. Second, focus on cleantech technologies such as solar, wind, hydro power, nuclear fusion and hydrogen, which are crucial for the transition to a net-zero economy. The EU has the potential to lead in cleantech innovation, although it currently lags in production. Competitiveness in cleantech could generate significant economic value and is essential for achieving energy independence and sustainability goals. Lastly, the pharmaceutical industry is a critical sector. The EU needs to bolster its competitiveness, particularly given the global leadership of the US in public funding in this field. Enhancing investment and innovation in pharmaceuticals is vital for the EU to maintain and advance its health care systems, respond to public health challenges and secure its position in the global market.

Through a combination of strategic investment, regulatory refinement and international collaboration, the EU can regain its position as a global competitor in technology and innovation while adhering to principles that resonate with the liberal and conservative values of market freedom, individual rights and limited government intervention.

	Programme 1	**Programme 2**	**Programme 3**
	Growing ICT	**Making cleantech competitive**	**Bolstering pharmaceuticals**
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 across Europe to attract talent from abroad.	Establish programmes that will approach development from a rational viewpoint—focusing on sustainable development and growth and approaching the climate-change problem from the perspective of mitigation of the effects and reducing greenhouse gases where it is least expensive. In particular, focus on knowledge related to the circular and regenerative economies.	Enhance interdisciplinary training. The pharmaceutical industry is inherently multidisciplinary, requiring a blend of skills across scientific, technological and clinical domains. Policies should encourage academic institutions to offer interdisciplinary programmes that integrate areas such as pharmacology, data science and engineering. Such initiatives could be supported by industry–academic partnerships.
Project 2	Establish low–red-tape incubation programmes that provide resources, mentorship and funding to ICT start-ups. These programmes should catalyse innovation by supporting entrepreneurs to develop and scale viable technology solutions.	Support the establishment of cleantech innovation hubs that bring together researchers, start-ups and investors to accelerate development. These hubs can provide essential resources, mentorship and networking opportunities to foster innovation and commercialise sustainable technologies.	Strengthen intellectual property rights to incentivise innovation and research, ensuring that pharmaceutical companies have the security needed to invest in new and groundbreaking treatments.
Project 3	Carry out a regulatory review with a view to reducing the regulatory burden on the EU's digital industry. Deepen forms of regulation that ensure fair market access for emerging ICT companies to 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 environmental footprint, undermines its industrial foundation. Existing initiatives such as the European Sovereignty Fund and the Grean Deal Industrial Plan should evolve in this direction.	Streamline regulatory approval processes. Simplifying and expediting the approval processes for new drugs and treatments could reduce development costs and time to market, enhancing the industry's global competitiveness.

Artificial Intelligence

Anastas Punev

At the end of 2023, the agreed text of the EU's Artificial Intelligence (AI) Act laid down the architecture for the future use of AI within the Union. This chapter responds to the possible drawbacks of the Act, making recommendations on both internal governance and the EU's international role.

The AI Act can be compared to the General Data Protection Regulation (GDPR), which was similarly hailed as a 'global first' piece of legislation that balanced fundamental rights and innovation, in this way fostering the EU's global role. Unfortunately, the GDPR's ambitious goals have been undermined by poor enforcement. Millions of European SMEs have reportedly not complied with the excessive burdens, and this has thrown into question the purpose and future impact of the regulation. The AI Act would involve certain comparable levels of market surveillance at both the national and supranational level, as a new institution—an EU AI Office—would be established. There was a considerable lack of consistency among the member states in implementing the GDPR without falling into unnecessary bureaucracy. This suggests that something similar can be expected when it comes time to implement the AI Act. Moreover, the elaborate risk-sharing formula established by the AI Act might be unsuitable for open-source foundation models since they 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. Such a one-size-fits-all approach is impractical for providers of mostly decentralised open-source AI systems, especially given the excessive regulatory burden, such as, the requirement to maintain ten years of documentation.

Furthermore, while the levels of risk are defined in the Act, the allocation of responsibility between the different providers throughout the AI life cycle remains vague and thus unpredictable for businesses from the outset. The fundamental question of liability remains open. Moreover, the regulation has been designed in accordance with the product safety legislation, and end users have been left in the dark as their role as right-holders is not expressly guaranteed and protected.

Finally, 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, as China has already introduced its AI legislation and the US is still considering its own approach. In any case, the Chinese model does not aim for global supremacy but is mostly pragmatic in its aims, adhering to a 'vertical strategy' where regulations are tailored to certain AI applications. Consequently, the EU AI Act would enter into competition with the Chinese legislation in terms of its agility. And even if it is adapted to the current technological advances, its ability to deliver future-proof results is far from guaranteed.

	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 by EU authorities in approving organisations that would 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 global risks of AI proliferation and 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/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. 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.

European Digital Leadership on the Global Stage

Dimitar Lilkov

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 AI systems. The old continent is making an ambitious attempt to pioneer the global golden standard in legislation for the online realm.

This ambition, however, is being put to the test. Rule-setting and global influence are functions of technological excellence and market share. 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.

This concept has three pillars. First, the EU must upgrade its blueprint for digital deterrence. Enhancing supranational tools here is not driven by federalist zeal but rather by practical necessity. The European Commission needs to have an improved mandate to implement security standards for critical digital infrastructure and to prohibit high-risk vendors from penetrating sensitive networks. An expanded toolkit is necessary to limit the threats from compromised ICT products/services (and apps) which could serve the purposes of foreign adversaries.

Second, the EU needs to expand its digital outreach internationally. Within this decade, the European institutions need to deepen strategic engagement on technology and multiply existing agreements. The recently concluded EU–Japan data agreement and EU–India Trade and Technology Council (TTC) are important milestones that need to be replicated. Such a proactive agenda internationally will produce positive spillovers, enhancing bilateral trade, reinforcing important 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.

Lastly, Europe’s international digital agenda must retain a strong transatlantic component. Both Europe and the US must remain committed to driving the digital transformation, cooperating on breakthrough technologies and promoting joint standards internationally. The EU–US Trade and Technology Council remains an important mechanism for achieving these goals. There is a shared agenda of common interests, and also common concerns about the proliferation of advanced technologies and how to respond to joint threats. The EU–US relationship is a key artery of the global economy; improved digital circulation and boosted immunity need to remain a priority for both economic blocs.

	Programme 1	Programme 2	Programme 3
	Ensuring digital deterrence against 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 an 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 for 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 going against pre-defined European standards.	Engage with international standards-setting bodies (i.e. ISO, IEC) and the UN (i.e. ITU) to promote European digital standards. Oppose China's targeted 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 warning on semiconductors and secure supply chains. Adopt joint standards on EVs and clean technologies.
Project 3	Strengthen foreign direct investment 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 with 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.

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 WLAN 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.

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.

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.

Anastas Punev holds a Ph.D. in law and is a practicing lawyer in the field of civil and commercial law, and an Senior Assistant Professor at Sofia University's faculty of law. His main interests are in the field of civil procedure, as well as in the new legal challenges posed by technological innovation.

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 was 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.

Wilfried
Martens Centre
for European Studies

The 7Ds for Sustainability

Debt
Decarbonisation
Defence
Democracy
Demography
De-risking Globalisation
Digitalisation IN DEPTH