

## European View

### **Europe's digital future: Navigating opportunities and challenges**

#### EDITORIAL

<b>Europe's digital future: Navigating opportunities and challenges</b>	<b>117</b>
Mikuláš Dzurinda	

#### EUROPE'S DIGITAL FUTURE: NAVIGATING OPPORTUNITIES AND CHALLENGES

<b>The new EU rulebook for online platforms: How to get it right, who will it impact and what else is needed?</b>	<b>121</b>
Eline Chivot	
<b>The European Parliament's role in EU digital governance: Aspiration and reality</b>	<b>131</b>
Kai Zenner	
<b>Cybersecurity post-COVID-19: Lessons learned and policy recommendations</b>	<b>140</b>
Iva Tasheva	
<b>Saving EU digital constitutionalism through the proportionality principle and a transatlantic digital accord</b>	<b>150</b>
Jan Czarnocki	
<b>The technology challenge in the transatlantic relationship</b>	<b>157</b>
Raluca Csernaton	
<b>Regulating artificial intelligence in the EU: A risky game*</b>	<b>166</b>
Dimitar Lilkov	
<b>Ethics and governance in the digital age</b>	<b>175</b>
Jana Mišić	
<b>The ethical dimension of human-artificial intelligence collaboration</b>	<b>182</b>
Michał Boni	

#### CURRENT AFFAIRS

<b>Back to Westminster: A new transatlantic agenda to defend democracy</b>	<b>191</b>
Igor Merheim-Eyre	

<b>Authoritarian consolidation in Belarus: What role for the EU?</b>	<b>201</b>
Giselle Bosse	
<b>Battle of the hearts: China's aim to become a soft (super) power and Europe's response</b>	<b>211</b>
Janne Leino	
<b>EU dialogue with Russian society: A reality check</b>	<b>220</b>
Robert Pszczel	
<b>The democratic deficit of the EU: Breaking the spell of a false analogy</b>	<b>226</b>
Svetoslav Malinov	
 SATIRICAL REVIEW	
<b>Another article on the Strategic Compass (kind of)</b>	<b>234</b>
George Pepios	
 EXECUTIVE SUMMARIES	
<b>Back to Geneva: Reinterpreting Asylum in the EU</b>	<b>237</b>
Vladimír Šimonák and Harald Christian Scheu	
<b>Qualified Majority Voting in EU Foreign Policy: Make It So</b>	<b>239</b>
Niklas Nováky	
<b>A Brussels-Based Dictatorship or a Paradise of Subsidiarity? National Prerogatives and EU Migration Policy</b>	<b>240</b>
Vít Novotný	
<b>Reforming the European Stability Mechanism: Too Much but Never Enough</b>	<b>242</b>
Anna Peychev	
<b>Getting Back to Basics: Four Centre Right Steps to Economic Recovery</b>	<b>244</b>
Eoin Drea	
<b>Me, Myself and I: Could Tax Individualisation Create Jobs and Reduce Inequality?</b>	<b>246</b>
Ronald Bachmann, Philipp Jäger and Robin Jessen	
<b>Artificial Intelligence and Governance: Going Beyond Ethics</b>	<b>248</b>
Michał Boni	



# Europe's digital future: Navigating opportunities and challenges

European View  
2021, Vol. 20(2) 117–120  
© The Author(s) 2021  
DOI: 10.1177/17816858211063961  
journals.sagepub.com/home/euv



**Mikuláš Dzurinda**

The digital and technological revolution is already well underway. As Ursula von der Leyen, President of the European Commission, declared in her 2021 State of the Union speech, ‘digital is the make-or-break issue’ (von der Leyen 2021, 6). Tangible proof of this statement is the 20% of Community funds earmarked for the digital space under the NextGenerationEU recovery programme. Such commitments by the member states and the institutions prove that digital solutions will be instrumental to the EU’s road to recovery and to safeguarding its competitive position in the global economy. Therefore, this issue of the *European View* could not have been timelier. It gathers together seven contributions on the overarching theme of ‘digitalisation and the future’ from practitioners, academics and researchers who explore the implications for policy, society and industry.

Before venturing into a discussion of the future and long-term potential of the digital transformation that is happening in the workplace, the economy, governance and education, it is necessary to take a step back. No one had expected or anticipated the digital overhaul that took place overnight in March 2020, when the whole continent was plunged into a state of paralysis due to the COVID-19 pandemic. I experienced this first-hand when I suddenly found myself unable to travel to Brussels for my usual engagements and—like millions of people across the world and Europe—had to adapt *tout de suite* to a new, exclusively digital state of working, interacting and socialising. Networking events, in-person meetings and conferences all came to a sudden halt and were soon moved to an online format. This not only altered the very nature of such interactive happenings but brought with it a whole array of novel difficulties and challenges. Although

---

**Corresponding author:**

M. Dzurinda, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1st floor, B-1000 Brussels, Belgium.

Email: [ev@martenscentre.eu](mailto:ev@martenscentre.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

it suddenly became possible to hold a real-time debate with people physically present in different corners of the world, this was often hampered by an unreliable Internet connection and inadequate network encryption. As the world is gradually returning to a state of pre-pandemic normality, it is becoming increasingly evident that this ‘new normal’ is more digital: some remote working is still in place, and hybrid (semi-physical, semi-online) events are currently preferred.

Nonetheless, what this experience has shown us is that technology has advanced to such a level that we—individually and collectively—can carry on regardless of any kind of disruption. This seismic shift towards digitalisation and the acceleration of new technologies brought to my mind an old slogan we used to have when promoting the structural reforms in Slovakia: ‘people should be given fishing hooks, not fish’. Today I tend to paraphrase this: people should be given a computer, a fast Internet connection and training. And not only people currently in employment, but also children from less well-off families, people living in regions with high unemployment rates, and people living along our borders and in the countryside. What makes this even more urgent is the staggering 42% of European citizens who, according to the Commission’s Digital Economy and Society Index (European Commission 2020), lack basic digital skills.

The sea change brought about by the pandemic has been matched by a range of new EU strategies and legislative proposals that both amplify and harness this paradigm shift: the EU tool-box on secure 5G, the EU digital strategy, the European strategy for data, the White Paper on Artificial Intelligence (AI) and subsequent proposal for an AI Act, and the flagship dual regulatory package of the Digital Services Act and Digital Markets Act. This high volume of legislative activity and policy initiatives over the past two years highlights that it is not by chance that the Commission has declared this ‘Europe’s digital decade’. Legislators in the European Parliament and member states must live up to the challenge of reshaping Europe’s digital landscape by ensuring that the EU remains a safe and healthy environment in which individuals and businesses can thrive. The Parliament’s decision to set up the Special Committee on Artificial Intelligence in a Digital Age, tasked with analysing and scrutinising the impact of AI on the EU economy, is already yielding positive results and has provided valuable input to the public debate.

Capitalising on this momentum in policymaking circles, this issue of the *European View* focuses on the impact of digitalisation on the future of Europe: on the economy, society, political systems and the direction of the European project itself. When it comes to future-proofing the digital transition, the path that policymakers have to tread is uneven, with multiple twists and turns, and this issue’s author contributions reflect this reality. In his article, Dimitar Lilkov unpacks the voluminous text of the Commission’s AI legislative proposal, through which the EU aspires to become the first global player to adopt a comprehensive regulatory framework for AI. Eline Chivot argues that the existing European rules for online platforms have not been designed to

anticipate the challenges posed by the growth of digital markets and the nature of competition therein. It is with this in mind, she reveals, that our political family—the European People’s Party—remains committed to the passage of the Digital Services Act and the Digital Markets Act, with the ultimate aim of benefiting both European companies and European consumers. In a similar vein, Jan Czarnocki talks about the importance of the emerging movement for EU digital constitutionalism: a Union-wide effort to address the challenges posed by digitalisation through regulation, which would then pave the way for striking a transatlantic digital accord. Iva Tasheva builds the case for a more ambitious European cybersecurity agenda that puts EU values at its core as a way to combat the growing number of malicious attacks effectively. She argues that the bloc has three instruments in its arsenal to achieve this: legislation, research and investment, and the mandate to act. Kai Zenner draws on the parliamentary activity record on EU digital governance to argue that, despite its enhanced legislative powers, the European Parliament still struggles to be recognised as an authoritative and reliable political actor. Contributing to the philosophical dimension of the discussion around digitalisation, Jana Mišić stresses that moral evaluation is necessary in the technological governance debate and needs to be incorporated in a non-superficial but anticipatory manner. Following a similar logic, Michał Boni advances the importance of grounding human–machine collaboration in ethical principles, regulated by law and managed by oversight.

Whilst digitalisation—as one of the key political priorities of the von der Leyen Commission—is the crux of this issue of the *European View*, contributions on other current developments that are altering the European political landscape have not been omitted. Janne Leino discusses ways for the EU to counterbalance China’s ambitions of becoming a global soft (super)power. Raluca Csernatonu delves into the challenges to the transatlantic relationship posed by technological innovation. Igor Merheim-Eyre makes a compelling case for renewing the transatlantic agenda as a way to defend democracy. Giselle Bosse maps out a future EU policy towards Belarus that takes a stronger stance against the Lukashenka regime. Robert Pszczel argues that the current state of Russian society does not allow for an ambitious EU engagement policy. Finally, Svetoslav Malinov lays out a critique of the concept of the democratic deficit of the EU.

It is my hope that the contributions to this issue of the *European View* will enable us to better navigate the challenges lying ahead as Europe enters its digital decade, a period of great possibility and opportunity for people and the economy alike. As the authors have illustrated, the Union has the tools to make this new reality a prosperous one and to translate its digital ambitions into tangible results—just as it has done before.

## References

- European Commission. (2020). Digital economy and society index report 2020 – Human capital. <https://digital-strategy.ec.europa.eu/en/policies/desi-human-capital>. Accessed 20 October 2021.

von der Leyen, U. (2021). 2021 State of the Union address by President von der Leyen. Strasbourg, 15 September 2021. SPEECH/21/4701. [https://ec.europa.eu/info/sites/default/files/soteu\\_2021\\_address\\_en\\_0.pdf](https://ec.europa.eu/info/sites/default/files/soteu_2021_address_en_0.pdf). Accessed 20 October 2021.

### Author biography



**Mikuláš Dzurinda** is President of the Wilfried Martens Centre for European Studies and a former prime minister of Slovakia.



# The new EU rulebook for online platforms: How to get it right, who will it impact and what else is needed?

European View  
2021, Vol. 20(2) 121–130  
© The Author(s) 2021  
DOI: 10.1177/17816858211050159  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Eline Chivot**

## Abstract

Online platforms are drivers of innovation, growth, employment, creativity and information exchange. But new advantages can also bring new risks, or further entrench existing issues. Europe's current rules have enabled the birth and growth of these companies, and of the free and open Internet as we know it. But they have not been designed to anticipate the challenges brought about by the growth of the digital economy, such as the spread of disinformation, and they are not fully adapted to the nature of competition in the digital markets. As the heart of its ambitious digital agenda, the EU is proposing new regulatory frameworks to maintain and improve its competitiveness, innovation and growth. This approach aims to protect its market from the side effects of digital markets dominated by large non-EU tech companies which, in some respects, are shielded from the rules of the game that the EU wants to set. It also aims to protect citizens and democracy. This is clearly a time to act, and a time to reform. It is also a time to strengthen its position: the EU has other battles and priorities that it must face along the way.

## Keywords

Platforms, Social media, Digital markets, Technology, Competitiveness, Online content, DSA, DMA

## Introduction

The global coronavirus (COVID-19) pandemic has brought to light the ways in which society and the economy increasingly depend on the digital economy. Many companies have had to accelerate the transition of their resources and organisational processes from

---

### Corresponding author:

E. Chivot, European People's Party (EPP), 10 Rue du Commerce, Brussels, B-1000, Belgium.  
Email: [ech@epp.eu](mailto:ech@epp.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

paper-based to digital solutions. People have moved most of their activities online. Through this transformation, many new opportunities and benefits have emerged. But so too have many challenges, some new, others exacerbated. The right policies can help to protect the economy and society, while continuing to support prosperity in this new reality.

This article explores some of the issues which the EU aims to tackle through its digital agenda, arguing that it is necessary to update the rules of the road for actors in the online economy. The article will particularly discuss some of the motives behind two policy proposals, namely the Digital Services Act (DSA) and the Digital Markets Act (DMA). It will explore some of the issues that these acts aim to solve, including illegal online content and disruptions to competition in the digital markets, as well as what they mean for citizens and democracy. In light of the changes these reforms would lead to for companies and citizens, the article will then outline a number of areas which require careful consideration by policymakers, and elements that they must avoid or address to ensure the EU's future competitiveness in the digital economy.

## **A time to act**

Digital platforms such as social media networks and online marketplaces have driven significant innovation in Europe. They have created jobs and growth by providing services to hundreds of thousands of businesses and millions of consumers. E-commerce accounts for an increasing proportion of enterprise turnover, having reached 20% by 2020 across the EU27 (Eurostat 2021b). Sixty-three per cent of individuals across the bloc made online purchases in 2019, up from 43% in 2013 (Eurostat 2021a). The COVID-19 pandemic has accelerated these trends. And while measuring the reach of the digital economy is not straightforward, sectors with high digital intensity generally make substantial contributions to employment growth across advanced economies. Social media platforms connect many people worldwide and facilitate the global exchange of information and goods by businesses and people. The pandemic has shown how critical the role of online companies is, and also how much societies and businesses rely on them. Digital platforms and technologies have become part of the collective effort to tackle health and economic crises and support new working and living realities. Such exceptional circumstances accelerated the use of digital or digitally enabled products and services by companies by seven years in Europe (*McKinsey Global Survey 2020*).

But this growing dependence on online companies, which helped to keep the economy afloat and daily lives bearable for many during the worst of the pandemic, has also shed more light on their negative externalities. Social networks have become one of the main vehicles for disinformation (European Commission 2018). The business models of some of these platforms, and the technologies they use, tend to reinforce the spread of disinformation, including through content personalisation and micro-targeting. Algorithms value time spent online and engagement (measured by comments, shares, 'likes' and clicks)—and content that inspires fear and anger often tends to attract attention and provoke more reactions. This amplifies exposure to potentially divisive and

emotionally charged debates, or in contrast, limits exposure to pluralism and diverse opinions (Lilkov 2019).

It is also important to acknowledge the concerns raised about digital markets. Competition must be effective and fair in the digital age, too. Currently, and even more so since their value and reach have increased during the pandemic, a set of large tech companies structure the online environment by controlling the flow of and access to information. In some cases, the market dominance of these platforms has led to issues such as unfair contract terms for business users (e.g. giving the platform the unilateral right to interpret any term in the contract it has signed with its business users) or self-listing ahead of competitors in search rankings.

Dominant tech companies also have a record of acquiring potential competitors at an early stage. While this so-called exit strategy is sometimes desired by start-ups, acquisitions should not happen at the expense of the entry and growth of a broader diversity of new players, large or small, in the market (Fletcher 2021).

Where competition is lacking, where technology fails to prevent the selling of dangerous goods or where it magnifies the spread of illegal speech, the few large companies that control those technologies and those platforms merit closer scrutiny.

## **A time to reform**

In Europe, the rules for competition and online content were adopted before the emergence and growth of the digital economy. They have enabled more transparency and fairness, which are key to competition. An example of this is the Platform-to-Business (P2B) Regulation, which aims to address concerns about the behaviour of large online platforms towards their business users, and requires the former to conform to specific standards when operating in the EU (European Commission 2021c). The European Commission has sanctioned large online companies for abuse of their dominant positions and continues to conduct investigations. But fines are just not enough to solve this problem, and there is a pressing need to go further by bringing more transparency, more fairness, new rights and more predictability to digital services. Indeed, while large online platforms still face competition in some markets, in the digital economy the success of many companies mainly depends on their ability to scale: consumers who make use of these platforms tend to derive additional value through the expansion of user networks. As a result, the most competitive businesses are those that can harness these ‘network effects’ (Gawer and Srnicek 2021). This has led to the growing dominance of a few platforms, pressing regulators to increase their scrutiny of the behaviour to which this dominance and market concentration could lead. Distortions to competition typically include unfair and anti-competitive practices such as predatory prices or exclusivity clauses.

Regarding online content, the EU’s e-Commerce Directive, which came into force in 2000, created rules that protect online companies from being unfairly targeted for what their users post or share on their platforms (European Commission 2021a). For instance,

travel-booking and shopping sites cannot be held liable for user reviews. This standard has enabled the growth of online platforms, along with the benefits that consumers have gained through their services. It has enabled the Internet to become an open place where there are many opportunities. But the growth of platforms and online information sharing has also been accompanied by the growth of illegal content, such as footage of real or simulated violence and child sexual abuse; materials that promote terrorism, radicalisation or hate towards groups or individuals based on religion, race, or sexual preference; and the sale of dangerous goods through marketplaces. Despite their progress and efforts, platforms have failed to prevent such content and products from appearing on their sites and, due to the sheer volume, such content has proven difficult to remove.

Given how fast the online environment has changed and still is changing, it is fitting that the EU and other countries such as the US are determined to update and strengthen their existing frameworks to address these challenges. The Digital Services Act (DSA) and the Digital Markets Act (DMA), proposed by the European Commission in December 2020, are currently being discussed and examined by the European Parliament and the Council (European Commission 2021d). These proposals reflect a consensus that ‘with size and power comes responsibility’. Both proposals are an opportunity to shape the digital economy in Europe, as they aim to ensure that platforms behave fairly and provide a safe environment for their consumers and business users.

The DSA aims to clarify the responsibilities of online platforms when it comes to policing the Internet, and to govern their content-management practices. In particular, the DSA will limit platforms’ exemption from liability for third-party or user content which they store and transmit, improve content moderation on social media to address issues such as online harassment and introduce transparency obligations for online platforms to combat disinformation. Its core principle is ‘What is illegal offline should be illegal online’.

The DMA aims to set specialised competition rules for large platform companies (called ‘gatekeepers’), target the disruptions to and lack of competition in the digital markets, and curb the power of these platforms by establishing a set of obligations and prohibitions to prevent them from imposing unfair conditions on the market (Madiega 2021a; Madiega 2021b; Anderson and Mariniello 2021; Broadbent 2020; Blankertz and Jaurisch 2021; One Policy Place 2021).

These proposals can ensure that the EU sets the standards for fair access and competition for all companies, including its small and medium-sized enterprises (SMEs). They can guarantee more transparency for users; improved consumer welfare; more protection, safety and choice for consumers; and more legal certainty for businesses. They can foster a safer and more open Internet for European citizens, a digital ecosystem which protects fundamental rights and democratic institutions.

But the EU must get these rules right. Many small companies and innovators in Europe are relying more and more on these large online platforms. Indeed, these

platforms may not be European, but they do support European businesses in a variety of ways, such as by enabling them to gain an immediate online presence, providing access to crowdfunding, and connecting developers with more users and sellers with more buyers.

These new digital rules will have to strike a very delicate balance. The challenge for regulators is to understand how platforms work and the (unforeseen) consequences of both legislation and the platforms' dominance. All this must be done without creating disproportionate burdens for smaller businesses, because they form the backbone of the European economy. Over-regulation and costly bureaucratic red tape would hamper technological development and put small firms at a competitive disadvantage. In addition, the new frameworks should seek to harmonise and unify regulations on digital services in order to address regulatory fragmentation across the EU. Uncoordinated measures would fuel legal uncertainty for businesses that cannot afford higher compliance costs.

While requirements and objectives such as more transparency are desirable, these should be meaningful, and should not come at the expense of companies' legitimate business secrets. In addition, regulation of illegal online content should safeguard freedom of expression, and achieving this is not always as straightforward as it sounds. For example, ordering online platforms to remove such content within a very strict deadline might be a difficult demand to meet in practice. Indeed this often requires a range of resources which small online platforms are unlikely to have, such as teams of online moderators and technology tools to filter content automatically. To ensure compliance, companies might err on the side of caution and remove content that may be lawful. It is also worth mentioning that automated filters remain quite rudimentary, and many are prone to errors (De Streel et al. 2020).

## **What does this mean for citizens?**

Along with how these new online regulatory proposals may affect corporate actors and freedom of expression, it is worth assessing their impact on citizens more broadly. The DSA and the DMA seek to improve the protection of fair markets and consumer welfare, which interplay with the key tenets of democracy and democratic governance, particularly in terms of popular control, online self-determination and individual choice.

Indeed, a key principle of democracy is about conveying power to the people. One ramification of this is that—in the digital era—people should have some degree of control over the personal information they share online and what happens to it, and some control over the way in which they use Internet-based services and an understanding of the consequences of such use. The EU's current frameworks provide tools to address this, but lack effective accountability and oversight mechanisms, and speed. Today, online platforms play an important role in setting rules and influencing standards. The power the platforms have over the markets may ultimately equate to the power they have over their consumers, thus impacting citizens' digital rights. Through greater and more

efficient oversight by public authorities, the implementation of the DSA and the DMA will provide an opportunity to enhance popular and institutional control and ensure the exercise of freedoms online.

In addition, these proposals may ensure consumers have more of a say about the choices platforms make on their behalf. For instance, the DMA would facilitate data portability for users, meaning that users would be able to switch more easily from one platform to another (OECD 2021). Not all may be interested in the new options that the EU proposals would create, but the idea is that users would be able to choose for themselves. At the same time, it is important to consider the impact that some of these rules would have on the convenience and user-friendliness of online services. These are key aspects of consumer welfare which must remain a core objective of EU policies.

Conversations on the impact of these proposals on democracy and on citizens may be overlooked, but they are necessary.

## **A time to strengthen the EU's position**

To achieve the goals of its digital agenda, the EU must also address problems other than the dominance of large tech companies. Policymakers should always discuss digital policies with a view not only to producing rules, but also to creating an enabling and coherent digital environment for European companies to flourish and grow in—while staying in Europe. The EU lacks indigenous global digital platforms of significant size, and has not been able to create more successful digital business models. Of the world's top 100 technology companies by market capitalisation, Europe is home to only 8 such firms, compared to 74 in the US and 6 in China (*CompaniesMarketCap.com* 2021). And while Europe has more than 10,000 platforms, 90% remain SMEs (European Commission 2021b). This is, in part, due to the lack of a truly harmonised digital single market.

In addition, competitiveness in the digital economy requires policies that encourage entrepreneurship and risk-taking. The EU also needs policies that incentivise more public funding and private-sector investment directed towards strategic emerging technologies. The completion of Europe's capital markets union is important in this respect. In Europe, venture capital investments as a share of GDP are 10 times lower than in the US; as a result, European firms are more likely to be acquired by US-based companies, particularly in the tech sector (Demertzis et al. 2021). The EU must strengthen public support for fundamental research and innovation. It has already committed unprecedented and ambitious investments, including the €7.5 billion Digital Europe Programme to support investment in artificial intelligence, supercomputing and data platforms. But these efforts are dwarfed by those of its competitors. For instance, of the €25 billion total investment in artificial intelligence and blockchain each year, the US and China account for more than 80%, while the EU's share amounts to only 7% or about €1.75 billion (Verbeek and Lundqvist 2021).

While it is home to a sophisticated workforce, the EU is faced with challenges relating to talent attraction and retention, and has yet to equip its population with digital skills and digital literacy. Both of these are essential for the EU to ensure employment in the digital economy, succeed in implementing its policies and, therefore, achieve economic and societal prosperity. In 2019, only 56% of EU citizens were equipped with basic digital skills, which most jobs now require (European Court of Auditors 2021). Digital literacy will be critical to ensure citizens embrace the opportunities of digital technologies, become data-savvy actors, have greater awareness of and control over their data, have knowledge of big data applications and data governance, and understand their digital environment and its risks.

Furthermore, a stronger and more sustainable digital infrastructure is a precondition for supporting the emergence of new technologies, delivering sound data governance, facilitating access to higher-quality data and ensuring better connectivity for all. Policies should create an environment of trust in which companies, public administrations and consumers will want to adopt digital solutions.

Finally, broader geopolitical factors are also at stake, as the EU and others, such as the US but also more recently China, aim to erode the dominance of large platforms. The EU has adopted the concept of ‘open strategic autonomy’, which aims to gain more control over these companies and achieve greater independence in the digital and technological spheres (Fleming 2021).

Changes to EU laws aimed at ensuring a level playing field for European SMEs and start-ups, and the larger quest for greater autonomy, should not, however, result in protectionist measures directed at non-European firms. To build a strong European digital economy, open strategic autonomy should mean establishing a level playing field for global trade and adding tools to ensure fair treatment for businesses in the marketplace, both at home and abroad. It means capacity: having the resources and ability to act independently—both for and within a common agenda, alongside our partners. As such, open strategic autonomy is not about trade barriers or disengaging from globalisation; it is about reducing dependencies, strengthening the EU’s ability to act on a legislative basis fit for the twenty-first century and integrating less-developed actors into global markets (European People’s Party 2021).

The DSA, the DMA and the other frameworks of the EU’s digital agenda offer opportunities for Europe to lead, but the bloc also needs to collaborate with its partners in areas where it is mutually beneficial to do so.

## **Conclusion**

COVID-19 has demonstrated the value of online platforms for consumers, and platforms will play a key role in supporting the EU’s green and digital transition. The DSA and the DMA have been drafted for the benefit of both companies and individuals, but they

should also be drafted with them, and factor in the impact they are bound to have on them.

Undeniably, the challenges the EU faces due to the growing digital economy, further exacerbated by the pandemic, require new responses and updated rules. The scale and speed of information sharing have made illegal online content more difficult to prevent and remove, and the entrenched market position of a few large, non-EU companies has led to growing concerns over how this may leave little space for smaller, European firms to join, establish themselves in the market and grow. At the same time, certain rules, their lack of harmonisation and the compliance burden they could entail may impact the very companies they aim to protect and promote. Furthermore, while more oversight could benefit citizens and would seek to remedy a troubling power shift, it could also inadvertently impact certain fundamental rights, freedoms and consumer interests. In addition, approaches to make the EU ‘fit for the digital age’ and more autonomous in the technological sphere will also need to address challenges beyond illegal online content and unfair competition.

The digital economy and its transformations are not going to slow down; hence, the work to seize their benefits and tackle their challenges can only be sped up. The European People’s Party is committed to helping to advance the passage of the DSA and the DMA constructively with its members and family, keeping in mind as the ultimate objectives and overarching principles the benefits for European companies and citizens, and the protection of democracy and fundamental rights. The possibilities for economic growth and societal prosperity in Europe in the digital economy are endless—if regulation is implemented correctly.

## References

- Anderson, J., & Mariniello, M. (2021). Regulating big tech: The Digital Markets Act. *Bruegel*, 16 February. <https://www.bruegel.org/2021/02/regulating-big-tech-the-digital-markets-act/>. Accessed 27 August 2021.
- Blankertz, A., & Jaursch, J. (2021). What the European DSA and DMA proposals mean for online platforms. *Brookings, TechStream*, 14 January. <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/>. Accessed 27 August 2021.
- Broadbent, M. (2020). *The Digital Services Act, the Digital Markets Act, and the new competition tool*. Center for Strategic and International Studies, 10 November. <https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool>. Accessed 27 August 2021.
- CompaniesMarketCap.com*. (2021). Largest tech companies by market cap. <https://companies-marketcap.com/tech/largest-tech-companies-by-market-cap/>. Accessed 27 July 2021.
- Demertzis, M., Domínguez-Jiménez, M., & Guetta-Jeanrenaud, L. (2021). *Europe should not neglect its capital markets union*. Bruegel, Policy Contribution 13/2021, June. <https://www.bruegel.org/wp-content/uploads/2021/06/PC-CMU.pdf>. Accessed 27 August 2021.
- De Streel, A., Defreyne, E., Jacquemin, H., Ledger, M., Michel, A., Innessi, A., Goubet, M., & Ustowski, D. (2020). *Online platforms’ moderation of illegal content online: Law, practices and options for reform*. European Parliament, Directorate-General for Internal Policies, Policy Department for Economic, Scientific and Quality of Life Policies, June. <https://www>.

- europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL\_STU(2020)652718\_EN.pdf. Accessed 27 August 2021.
- European Commission. (2018). *A multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation*. Luxembourg: Publications Office of the European Union. <https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation>. Accessed 27 August 2021.
- European Commission. (2021a). e-Commerce Directive. 10 June. <https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive>. Accessed 27 August 2021.
- European Commission. (2021b). Europe fit for the digital age: New online rules for platforms. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en). Accessed 27 August 2021.
- European Commission. (2021c). Platform-to-business trading practices. 9 June. <https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices>. Accessed 27 August 2021.
- European Commission. (2021d). The Digital Services Act package. 26 April. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. Accessed 27 August 2021.
- European Court of Auditors. (2021). *EU actions to address low digital skills*. Luxembourg. [https://www.eca.europa.eu/Lists/ECADocuments/RW21\\_02/RW\\_Digital\\_skills\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/RW21_02/RW_Digital_skills_EN.pdf). Accessed 27 August 2021.
- European People's Party. (2021). *Position paper – For a powerful, targeted EU global trade policy*. June. <https://www.epp.eu/papers/for-a-powerful-targeted-eu-global-trade-policy>. Accessed 27 August 2021.
- Eurostat. (2021a). Internet purchases by individuals (until 2019) [isoc\_ec\_ibuy], INDIC\_IS: Last online purchase: in the 12 months. <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>. Accessed 10 September 2021.
- Eurostat. (2021b). Value of e-commerce sales. [isoc\_ec\_evaln2], INDIC\_IS: Enterprises' total turnover from e-commerce sales, UNIT: Percentage of turnover, SIZEN\_R2: All enterprises, without financial sector (10 persons employed or more). <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>. Accessed 10 September 2021.
- Fleming, S. (2021). What is digital sovereignty and why is Europe so interested in it? *World Economic Forum*, March. <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>. Accessed 27 August 2021.
- Fletcher, A. (2021). Big tech: How can we promote competition in digital platform markets? *Economics Observatory*, June. <https://www.economicsobservatory.com/big-tech-how-can-we-promote-competition-in-digital-platform-markets>. Accessed 27 August 2021.
- Fletcher, R. (2020). The truth behind filter bubbles: Bursting some myths. *Reuters Institute*, 25 January. <https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths>. Accessed 27 August 2021.
- Gawer, A., & Srnicek, N. (2021). *Online platforms: Economic and societal effects*. European Parliamentary Research Service, PE 656.336, March. [https://www.europarl.europa.eu/think-tank/en/document.html?reference=EPRS\\_STU\(2021\)656336](https://www.europarl.europa.eu/think-tank/en/document.html?reference=EPRS_STU(2021)656336). Accessed 27 August 2021.
- Lilkov, D. (2019). *European Parliament elections: The disinformation challenge*. Wilfried Martens Centre for European Studies, In Brief. Brussels, May. <https://www.martenscentre.eu/wp-content/uploads/2020/06/european-elections-disinformation.pdf>. Accessed 27 August 2021.

- Madiega, T. (2021a). *Digital Services Act*. European Parliamentary Research Service, Briefing PE 689.357, March. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS\\_BRI\(2021\)689357\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf). Accessed 27 August 2021.
- Madiega, T. (2021b). *Digital Markets Act*. European Parliamentary Research Service, Members' Research Service, Briefing PE 690.589, May. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS\\_BRI\(2021\)690589\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf). Accessed 27 August 2021.
- McKinsey Global Survey. (2020). How COVID-19 has pushed companies over the technology tipping point—and transformed business forever. 5 October. <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever>. Accessed 27 August 2021.
- OECD. (2021). *Data portability, interoperability and digital platform competition*. OECD Competition Committee Discussion Paper. <https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf>. Accessed 27 August 2021.
- One Policy Place. (@OPPEUDigital). (2021). Twitter post. 18 February, 4.01 pm. <https://twitter.com/OPPEUDigital/status/1362416910349008896?s=20>. Accessed 27 August 2021.
- Verbeek, A., & Lundqvist, M. (2021). *Artificial intelligence, blockchain and the future of Europe*. European Investment Bank, Innovation Finance Advisory, June. <https://www.eib.org/fr/publications/artificial-intelligence-blockchain-and-the-future-of-europe-report.htm>. Accessed 27 August 2021.

## Author biography



**Eline Chivot** is a Senior Adviser on Digital Policy at the European People's Party. Her role includes consolidating and fostering the Party's knowledge and positions regarding the public policies that impact the technology sector, its actors and the data economy.



# The European Parliament's role in EU digital governance: Aspiration and reality

European View  
2021, Vol. 20(2) 131–139  
© The Author(s) 2021  
DOI: 10.1177/17816858211061840  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Kai Zenner**

## Abstract

Despite its enhanced legislative powers, the European Parliament still struggles to be recognised as an authoritative and reliable political actor. Its current role in EU digital governance serves as a good example to illustrate both the aspirations of the parliamentarians as well as their actual impact. Confronted with a horizontal policy issue that affects all sectors of the analogue and digital world parliamentary working methods have proven to be unfit for purpose. The European Parliament has so far been unable to assume leadership to guide the EU through the digital transformation process. Yet, its aspirations are not pulled out of thin air. Intellectual freedom, swift decision-making channels, and an open and pragmatic debating culture make it, in fact, predestined to define an overarching and balanced digital agenda for the EU. Before this is achievable, however, it is necessary to execute comprehensive internal reforms to overcome a list of structural, financial, political and external deficits.

## Keywords

Digital transformation, Horizontal policy issues, European Parliament, Working methods, Existing deficits, Necessary reforms

## Introduction

The European Parliament (EP) is a fascinating political actor. On the one hand, it has gradually extended its powers of decision-making over the past five decades. Starting as a mere assembly in 1952, each successive EU treaty has increased the EP's role, eventually transforming it into today's co-legislator, with powers almost equal to those of the Council of the EU (Csernaton and Laţici 2020). The *Spitzenkandidat* procedure and the claim for a right of initiative emphasise the new aspirations of the Members of the

---

### Corresponding author:

K. Zenner, European Parliament, ASP 15E140, Rue Wiertz, 1047 Brussels, Belgium.  
Email: [kai.zenner@ep.europa.eu](mailto:kai.zenner@ep.europa.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

European Parliament (MEPs). For them and their staff, the EP offers extensive intellectual freedom, swift decision-making channels and (mostly) hands-off political leadership, as well as an open debate culture and pragmatic togetherness. Compared to many national parliaments where, as illustrated by Koschnick (2019), political initiatives come directly from ministries or political parties, and party discipline is omnipresent, the independent mandate of each MEP is still worthy of its name.

On the other hand, the EP is sitting on a backlog of long-overdue reforms relating to its composition and its internal procedures, while facing traditionally low election turn-outs (von Ondarza and Schenuit 2018, 2). The principle of degressive proportionality, which ensures that small member states have a minimum level of representation, results in a situation in which a Luxembourg MEP represents about 80,000 inhabitants, while his or her German counterpart is responsible for more than 800,000. Some extremely emotional debates in the past, such as on the failed Transatlantic Trade and Investment Partnership, and the fact that the political groups could not agree on a *Spitzenkandidat* after the 2019 election, have not helped to convince EU citizens that the EP is an authoritative and reliable political player (Russack 2019, 10).

Every MEP or staff member has probably already met representatives of the other European institutions or of the member states who have mentioned that they cannot take the EP seriously. Despite its significant gain in legislative powers, they argue that it continues to function like a start-up: chaotically and unpredictably. A harsh assessment? Yes—but this article argues that, as with many things in life, there is also some truth in this overstatement. The initiative of the von der Leyen Commission to make the EU fit for the digital age offers an excellent case study to expound this argument in more detail.

## The digital challenges faced by the EU

Although this hollow phrase has been recited endlessly, it remains accurate: after the end of the Cold War, the world became multipolar and our lives became much more complex. Decision-makers of the past had only a few sources of information and, subsequently, took their decisions by choosing one out of two or three credible courses of action in order to address a clearly defined issue. Today, instead of a lack of information, there is an overload. Moreover, decision-makers are frequently confronted with horizontal topics that require them to take into account various interconnected players and related subtopics on a global scale in both the analogue world and in cyberspace. As explained by Stockdale-Otárola (2017, 28), it therefore becomes difficult to even agree on what the actual problem is, where it is rooted, who is responsible and how to address it best. The digital transformation of the EU falls into this category of overarching issues. Despite its excellent starting position in the late 1990s, Europe has not been able to keep pace with the US or China, has developed major deficiencies and has so far not been able to respond adequately to the following eight key challenges:

- *Mastering digital geopolitics.* Confronted with strategic dependencies, critical cyber-attacks and authoritarian regimes that are dominating the work of

international bodies and standardisation organisations, the EU needs to toughen its digital foreign policy (Aktoudianakis et al. 2021).

- *Building a resilient and sustainable digital economy.* Without a comprehensive action plan for its digital industry, the EU has fallen behind in the development of emerging technologies and high-performance infrastructure; has become dependent on foreign energy supplies, software and hardware; and has a huge digital investment gap compared with the US or China (Demetzis 2021).
- *Solving the EU data challenge.* While access to, and the sharing and reuse of data, as well as data analytics are crucial for emerging technologies and a genuine data economy, the EU struggles with vast amounts of unutilised data, a lack of common data spaces, excessive data protection rules and restrictions on international data transfers (Batura and Peeters 2021).
- *Establishing a level playing field.* The existing methods of enforcement and oversight are no longer applicable to a cyberspace that is dominated by digital gatekeepers which decide how to rank and present the infinite amount of information, while capturing most of its value (Renda 2021, 3).
- *Promoting digital expertise.* Besides the lack of globally leading digital companies, digitally skilled employees, and excellent testing and competence centres, the EU does not feature enough public–private partnerships or knowledge transfer from research to business (Castro and McLaughlin 2021).
- *Digitally transforming the state and society.* The digital expansion of public services has stalled, while the public sector and society have become increasingly vulnerable as the sharp rise in disinformation campaigns and election interference has shown (Renda 2021, 4).
- *Addressing new ethical questions.* Authoritarian regimes are already applying digital technologies to control, monitor and score their citizens; within the EU the dominance of platforms and the unprecedented technological capabilities available to states and societies are giving rise to ethical questions (Lilkov 2020, 17).
- *Ensuring reliable and future-proof law making.* Although legal certainty is crucial for digital innovation, EU policymakers regularly respond too late to new technological developments, eventually coming up with already outdated laws that also contradict the existing legislation (Metzinger 2020, 36).

## **The anachronistic working methods of the European Parliament**

How is the EP dealing with the horizontal issue of transforming the EU digitally? How is it addressing the eight key challenges? Twenty-nine months after the 2019 election, the policy output can—at best—be described as mediocre. A coherent and comprehensive digital agenda for the EP is still missing, while the legislative proposals of the European

Commission are often respectfully escorted through. Instead of offering creative and disruptive ideas, in most cases MEPs table minor and expected amendments. If *Politico* is reporting from the EP, it focuses on personal statements, competence conflicts or yet another non-legislative resolution. Why are MEPs still struggling to assume political leadership and hence missing the opportunity to shape the EU's digital transformation? Four categories of persistent deficits stand out: structural, financial, political and external.

The structural deficits are closely linked to the EP's Rules of Procedure. Traditionally, Annex VI assigns a clearly definable topic to the competent committee, while a few other designated committees assist with short opinions. However, this approach no longer works for horizontal issues. For example, with regard to artificial intelligence (AI), no less than 13 of the EP's 20 committees were able to make a credible claim to be involved as it is no longer possible for one committee to have a complete overview of all developments or the expertise to address all affected sectors. The Data Strategy, presented by the European Commission in 2020, is another example. For an overarching and future-proof data concept, several committees with equal rights would have needed to work closely together. In reality, the lead committee, Industry, Research and Energy, dominated the discussions. As a result, in-depth consideration of areas such as intellectual property rights, single market rules, international data flows and data protection are largely missing from the final report (European Parliament 2020).

The ambiguity of Annex VI has two concrete effects. First, finding agreement on how to allocate a report at the Conference of Committee Chairs becomes very difficult and can block the legislative work for up to five months, as happened with the Digital Services Act. Second, even after such an allocation, fruitful cooperation is regularly not possible and the opinion-giving committees are largely ignored. It becomes a very frustrating and time-consuming endeavour for everyone except the lead committee. Consequently, the final parliamentary position regularly lacks thematic diversity and political coherence.

The urgent need to reform the Rules of Procedures is also visible in other areas. Requests to postpone deadlines to do more research or to continue political discussions are normally declined. The rules do not allow much flexibility. This in turn heavily limits the ability of MEPs to draw on the European Parliamentary Research Service (EPRS) or policy departments as the supporting materials these branches provide are usually not ready in advance of the deadline. For example, regarding AI liability, while political agreement for the Legal Affairs Committee's report was reached on 18 September 2020, an EPRS study on the same topic was only published seven days later (Evas 2020). The fierce competition between committees generally prevents both better use of the EPRS as well as anticipatory and comprehensive legislative planning. Long-term projects, such as formulating a cross-committee plan to make our digital economy more resilient, are not feasible under these circumstances.

The second deficit is financial. The secretariats of the committees as well as the political group advisers are massively understaffed and have to deal with numerous legislative files in parallel. Instead, for instance, of carrying out extensive research on digital platforms, their workload forces them to draw back to positions established during previous terms. Burnout is the consequence, leading to even more work for colleagues.<sup>1</sup> The staffs of MEPs are—compared to those of US Congress members—rather small, consisting mostly of young professionals and trainees who only stay for a short period. Even the EPRS does not have enough manpower to scientifically prepare the most important legislative files, supervise the political negotiations and monitor the ultimate implementation of the laws. The result for the EP is a loss of quality and less room to develop innovative new policy ideas or overarching concepts.

Although the technical as well as office equipment was massively upgraded after the 2019 elections, it is still another factor that compromises parliamentary work. Compared to other political institutions, the equipment (i.e. databanks, collaborative tools, connectivity) lags miles behind, constantly leading to technical problems in official sessions.

The political groups in the EP are responsible for the third deficit. Believing that it is an excellent way of getting good publicity and pushing forward their political ideas, they tend to agree upon too many own-initiative reports and resolutions. Not only are such parliamentary activities time-consuming and the cause of new conflicts of competence, but they regularly lead to contradictory statements. Returning to the example of AI: after seven overlapping own-initiative reports on the same technology in 2020 alone, no political actor understands anymore what the EP's position on AI really is. The reports assessed AI-related ethical issues, for instance, very differently. To make matters worse, in the same year, the political groups decided to launch the Special Committee on Artificial Intelligence in a Digital Age. However, its mandate does not allow it to address the new AI Act of the European Commission or any topic covered by the seven previous AI reports.

The distribution of rapporteur and shadow rapporteur roles within the political groups can also lead to problematic outcomes. To fulfil certain quotas, an expert who might have already worked on a topic for 10 years and has a clear workable plan in mind is sometimes forced to pass on the role. Likewise, all political groups have problems with MEPs who are permanently absent. Despite their absence, these MEPs are, however, still rewarded with more and more responsibility over the years. As a result, other MEPs or group advisers have to cover for them, preventing them from fulfilling their own tasks.

Last but not least are the external deficits. The EP struggles with an information gap compared with the European Commission and the member states, as both are usually reluctant to share their empirical data. They do however use that very same data to justify their policy suggestions, thus making it impossible for the EP to verify their reasoning. If they do share the data, it is often too complex and the parliamentary resources too limited to review it adequately. In interinstitutional negotiations, the EP therefore often

has no other option but to trust the word of the Commission or the member state in question. Neither parliamentary hearings nor EPRS studies have the depth of knowledge to fill this information gap. In order to form an opinion on complex issues such as cybersecurity risks in 5G networks, MEPs are regularly forced to rely on their favourite newspaper or on input from stakeholders.

Another major problem in terms of ensuring a comprehensive policy approach is the lack of competences on the EU level. The European treaties do not permit the EP to come up with a binding and comprehensive digital agenda. This would interfere with the competences of the member states on topics such as digital geopolitics or digital education. Likewise, the European treaties stand in the way of plans to reform the composition of the EP and its ambition to have a genuine right of initiative. Despite President von der Leyen's support for the latter, proclaimed in her speech on 16 July 2019 (European Commission 2019), the legislative proposals of the European Commission on topics such as AI or the Digital Services Act look quite different from the prior own-initiative reports of the EP.

## Conclusion

Remember the previous observation that there is a reason why certain Commission officials and national representatives are condescending towards the EP? Why they describe it as chaotic and unpredictable? The four persistent deficits—elaborated in the previous section—indicate why this overstatement still exists. However, the aspiration of the EP to shape Europe's digital transformation is not pulled out of thin air. The extended legislative powers, the intellectual freedom of its MEPs and the swift decision-making channels would in principle allow to address horizontal policy issues. With its open and pragmatic debating culture, the EP is, in fact, predestined to define a balanced and comprehensive digital agenda for the EU. Yet, in order to improve its current performance, it needs swift reforms. Encouragingly, in April 2021 the EP started a process to rethink the parliamentary democracy (Sánchez 2021). The preliminary results show an awareness of many of the deficits described above. Moreover, promising countermeasures have been proposed. However, much will depend on how the EP copes with internal and external resistance. To have a stronger impact on the EU's digital governance and to become a political player that the Commission and Council take seriously, the following points seem crucial.

To address the structural deficits, the EP should, first and foremost, reshape the setup of standing committees. A regularly reviewed Annex VI (Rules of Procedure) could help to assign clearly definable topics to just one lead committee. Instead of opinions, the coordinators of the political groups of the other designated committees could table amendments with the lead committee. Horizontal topics would, however, be processed exclusively in new ad hoc committees. Named after the political priorities of the European Commission (i.e. the Green Deal, a Europe fit for the digital age), each ad hoc committee would exist for the whole term and incorporate MEPs from all standing committees. To tackle the 'pacing problem', the digital ad hoc committee would need to apply flexible

working methods from the digital economy (Choi and Andresen 2020, 9–10). Temporary project teams formed of MEPs from different areas could reflect on the legal questions posed by new technological developments, making sure that the discussed policy solutions are not outdated. The adjusted Rules of Procedure should also offer more procedural flexibility to allow in-depth discussions, more consultations and an impact assessment of the final compromise amendments. Furthermore, the adjustments would give the EPRS and policy departments more time to scrutinise the risk of regulatory overlaps and prepare comprehensive supporting materials before the legislative work starts. The changes would minimise competition conflicts, free up resources, and strengthen the EP's policy output in terms of consistency and political support.

A higher budget is required to counter the financial deficits. MEPs, political groups, committee secretariats and the EPRS should be enabled to hire significantly more staff and pay higher salaries in order to secure highly qualified people who will stay for longer. At the same time, the EP should try to pool administrative tasks and responsibilities in order to speed up proceedings (CDU 2021, 7). Clear and realistic performance goals could help to maintain efficiency and workspace morale. Strong investment and a relocation of financial resources would also be necessary to offer better equipment and legislative assistance. Measures such as substantial legal advice during the legislative drafting process or the assignment of external experts would help to establish a quality level that is appropriate for the representative body of 477 million EU citizens.

The political groups are key to tackling the political deficits. Legislative work should become the new priority, while the number of own-initiative reports and resolutions should be massively reduced. More effort should be put into preparing the Joint Declaration with the Council and the Commission. The EP could strengthen its own position by introducing annual work programmes and a list of legislative priorities for the whole term. The political groups should also mandate the drafting of a strategic agenda or conceptual papers (i.e. an understanding of the European path to digitalisation) and pledge that their legislative work is principle-based, technologically neutral, innovation-friendly and future-proof. Another common goal should be to draft less new legislation and instead concentrate on evaluating, monitoring and adjusting already existing laws (CDU 2021, 4). To better deal with the dynamic digital sector, alternative governance approaches to our legislative toolbox should also be considered, such as regulatory sandboxes, embedding rules in code and public–private partnerships. Changes to the ways rapporteurs and shadow rapporteurs are assigned by the political groups seem equally crucial. The appointments should take place prior to the publication of the legislative draft by the European Commission so that the appointees can engage during the drafting process and find inter-institutional compromises on key issues *ex ante*. An MEP's track record and experience in the respective field should also be taken more into account when appointing rapporteurs. The proposed points would help to streamline the different working streams and would allow the EP to become a strategic political player that takes a long-term policy approach.

Solving the external deficits might be the most challenging task as this depends entirely on other political actors. To close the information gap, the EP should be closely

involved in impact assessments and in the European Commission's public consultation. Member states should also be encouraged to share and to explain their empirical data. After successfully removing the structural, financial and political deficits, the EP should eventually push for a treaty change. It will only become truly capable of determining the digital governance of the EU once it has a genuine right of initiative as well as legislative competences in all affected sectors (Madięga 2020, 8). At the same time, such a treaty change could be used to implement long-overdue reforms of its composition. The Conference on the Future of Europe could serve as a kick-off event. The execution of all the proposed reforms would ultimately turn the EP into the strong co-legislator that a successful digital transformation of the EU requires.

## Note

1. Some committees slightly adapted their working guidelines before the 2021 summer break as a response to continuous complaints over the workload and sessions outside of working hours.

## References

- Aktoudianakis, A., Vandenbussche, T., & Van der Loo, G. (2021). *The EU–US Trade and Tech Council: Mapping the challenges and opportunities for transatlantic cooperation on trade, climate, and digital*. European Policy Centre. Brussels.
- Batura, O., & Peeters, R. (2021). *European Union data challenge*. Briefing requested by the European Parliament, 28 July. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662939/IPOL\\_BRI\(2021\)662939\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662939/IPOL_BRI(2021)662939_EN.pdf). Accessed 30 August 2021.
- Castro, D., & McLaughlin, M. (2021). Who is winning the AI race: China, the EU, or the USA? 2021 Update. *Center for Data Innovation*, 25 January. <https://datainnovation.org/2021/01/who-is-winning-the-ai-race-china-the-eu-or-the-united-states-2021-update/>. Accessed 28 August 2021.
- CDU (Christlich Demokratische Union Deutschlands). (2021). *Deutschland mobilisieren, damit Gutes bleibt*. 9 June. <https://www.educsu.de/themen/deutschland-modernisieren-damit-gutes-bleibt>. Accessed 22 August 2021.
- Choi, M., & Andresen, S. (2020). *Das Neue Ministerium*. 18 December. <https://work.4germany.org/project/das-neue-ministerium-fellows-2020/>. Accessed 22 August 2021.
- Csernatonı, R., & Laıci, T. (2002). Empowering the European Parliament: Toward more accountability on security and defence. *Carnegie Europe*, 20 July. <https://carnegieeurope.eu/2020/07/20/empowering-european-parliament-toward-more-accountability-on-security-and-defense-pub-82309>. Accessed 22 August 2021.
- Demertzis, M. (2021). The four pillars of a digital strategy. *Bruegel*, 16 March. <https://www.bruegel.org/2021/03/the-four-pillars-of-a-digital-strategy>. Accessed 28 August 2021.
- European Commission. (2019). Opening statement in the European Parliament plenary session by Ursula von der Leyen, candidate for president of the European Commission. Strasbourg, 16 July. [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_19\\_4230](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_4230). Accessed 2 September 2021.
- European Parliament. (2020). *European strategy for data*. 2020/2217 (INI), 25 March. [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0098\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0098_EN.html). Accessed 2 September 2021.
- Evas, T. (2020). *Civil liability regime for artificial intelligence: European added value assessment*. EPRS Study PE 654.178, 25 September. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS\\_STU\(2020\)654178\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU(2020)654178_EN.pdf). Accessed 2 September 2021.

- Koschnick, W. (2019). Volksparteien: Selbsttötung per Fraktionszwang. *Heise.de*, 15 January. <https://www.heise.de/tp/features/Volksparteien-Selbsttoetung-per-Fraktionszwang-4271103.html>. Accessed 22 August 2021.
- Madiega, T. (2020). *Digital sovereignty for Europe*. EPRS Ideas Paper, PE 651.992, 2 July. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf). Accessed 23 August 2021.
- Metzinger, T. (2020). Towards a global AI charter. In G. Kolliarakis & I. Hermann (eds.), *Anticipatory governance for artificial intelligence* (pp. 33–8). DGAP Report no. 9, 19 April. [https://dgap.org/sites/default/files/article\\_pdfs/dgap\\_report\\_no\\_9\\_april\\_29\\_2020\\_60\\_pp.pdf](https://dgap.org/sites/default/files/article_pdfs/dgap_report_no_9_april_29_2020_60_pp.pdf). Accessed 23 August 2021.
- Renda, A. (2021). Making the digital economy ‘fit for Europe’. *European Law Journal*. doi:10.1111/eulj.12388.
- Russack, S. (2019). *EU parliamentary democracy: How representative?* Centre for European Policy Studies. 17 May. <https://www.ceps.eu/ceps-publications/eu-parliamentary-democracy/>. Accessed 22 August 2021.
- Sánchez, E. (2021). MEPs rethink EU Parliament future after Covid-19 pandemic. *EUobserver*, 17 May. <https://euobserver.com/democracy/151846>. Accessed 23 August 2021.
- Stockdale-Otárola, S. (2017). Navigating wicked problems. *OECD Insights*, 6 June. [https://www.oecd.org/naec/complexity\\_and\\_policymaking.pdf](https://www.oecd.org/naec/complexity_and_policymaking.pdf). Accessed 22 August 2021.
- Von Ondarza, N., & Schenuit, F. (2018). Reforming the European Parliament. *SWP Comment*, 20 February. <https://www.swp-berlin.org/en/publication/reforming-the-european-parliament>. Accessed 22 August 2021.

## Author biography



**Kai Zenner** is Head of Office for MEP Axel Voss (European People’s Party Group) in the European Parliament. Describing himself as a digital enthusiast, he focuses on emerging technologies, data sharing and the EU’s digital transition. He graduated in politics (University of Edinburgh) and in law (University of Münster). Before moving to the European Parliament, he worked as a research associate at the European office of the Konrad Adenauer Foundation in Brussels.



# Cybersecurity post-COVID-19: Lessons learned and policy recommendations

European View  
2021, Vol. 20(2) 140–149  
© The Author(s) 2021  
DOI: 10.1177/17816858211059250  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Iva Tasheva**

## Abstract

This article looks at the impact of the novel coronavirus crisis and increased remote work on cybersecurity and the priorities for EU action. Actions should include improving the cybersecurity of businesses, critical infrastructure and users, and creating an EU cybersecurity industry. As more and more aspects of our lives happen online, we are becoming more vulnerable to malicious attacks. This was demonstrated in 2020 when cyber-attacks increasingly disrupted the work of hospitals, service providers, government services and businesses across the globe. The frequency and scale of the attacks created a sense of urgency to improve our cybersecurity resilience. This article argues that the EU should reap the benefits of cybersecurity by pursuing a more ambitious cybersecurity agenda and putting EU values at the core of its approach. It also calls for cybersecurity to be included in all EU pillars, including the EU industrial research and innovation policy, as well as in EU investment plans and diplomatic strategy.

## Keywords

EU, Cyber, Security, Policy, Privacy, COVID-19, Democracy, Diplomacy

## Introduction

The novel coronavirus (COVID-19) pandemic hit the world in March 2020, changing how we live, work and communicate. Social distancing and working from home became the norm. In Europe, as in most of the world, everything had to be digitalised to continue government, social and economic activities. Digitalisation was already a trend, but the arrival of COVID-19 caused it to happen overnight. Thus, the security of our

---

### Corresponding author:

Iva Tasheva, CYEN, Avenue Paul Hymans 121, Brussels, 1200, Belgium.

Email: [iva.tasheva@cyen.eu](mailto:iva.tasheva@cyen.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

government, businesses and citizens, which had been developed over the centuries, became a matter of cybersecurity in just a few months.

During 2020 the intensity and scale of cyber-attacks increased. Malicious actors exploited our fears linked to the health crisis, sending fake COVID-19 updates and alarming phishing messages to collect user information or install malware on users' devices. The many new Internet users were not prepared for this threat, and nor had they been instructed on how to face it. Estimated global losses from cybercrime in 2020 hit a record of just under \$1 trillion (Malekos Smith and Lostri 2020). If measured as a GDP and compared with national economies, cybercrime turnover would rank thirteenth in the world right now (between Indonesia and Turkey). With everyone and everything now online, opportunities for attacks have increased. This and increased activity by malicious actors have made cybersecurity even more challenging to achieve. Naturally, therefore, integrating cybersecurity into all aspects of life, including remote work, has been an uphill battle.

This article, while presenting the current state of play, aims to define the opportunity that cybersecurity holds for Europe. It focuses on analysing the multiple facets of cybersecurity and the factors that play a role in achieving it, including the impact of the COVID-19 crisis and increased remote working. It argues that the EU should pursue a more ambitious cybersecurity agenda with the Union's values at the core of its approach, and calls upon policymakers to integrate cybersecurity into the EU's industrial innovation and research policy, as well as investment policies and diplomatic strategy. Finally, the article provides actionable policy recommendations for policymakers to help realise the opportunity that cybersecurity presents for the EU.

## **Cybersecurity during COVID-19**

During the first three months of the pandemic, information and communication technology (ICT) teams everywhere worked around the clock to deliver digitalisation projects that, under normal circumstances, would have taken years to put in place. They had to implement the basics of remote work: creating large-scale remote connections, and ensuring sufficient portable devices and network capacity to make it all work. They also had to integrate collaborative solutions, such as virtual meeting rooms and information management solutions (i.e. the cloud and cloud-based applications), to ensure that the quality of services could be maintained. Despite the short time frame, all these solutions also needed to work securely (i.e. protecting the confidentiality, integrity and availability of data they processed). Integrating cybersecurity into processes, products and services is necessary to protect users, in a similar way to how security and safety are expected in the physical world, for instance, when using vehicles, roads, postal services, clothing and domestic appliances.

However, in an emergency digitalisation situation it is very difficult to ensure the security of systems. Ensuring security requires an analysis of the risks and mitigating measures, implementation planning, the integration of all processes, the use of expertise

and the education of users. All of these are continuous processes and adaptations, which could not happen overnight despite the sense of urgency. Cybersecurity, or the lack of it, became one of the key issues and fastest-growing concerns of this emergency digitalisation. Preserving the availability, confidentiality and integrity of the information and systems built so far became key for all business operations. Whether a company was able to stay in business or not began to depend on the security of their operations, people and technology. One cyber-attack could take a whole business offline. As well as businesses coming to depend on cyberspace, more data and more sensitive information have also become available online, including (national) security, business and private discussions.

At the same time, the security of the weakest link defines the overall level of cybersecurity, not the individual or average level of security. Data and activities have become more vulnerable than ever due to the low-security maturity of many of the new actors in the digital space, such as local small and medium-sized enterprises (SMEs), public services and employees working online for the first time. Arguably too many new users have come online without taking the time to develop proper cybersecurity awareness and hygiene (Fernandez et al. 2020), that is, the knowledge and habits of following basic cybersecurity rules. It has been particularly challenging to integrate security into the massive remote-working transition. There have been constraints due to the limited resources (experts, infrastructure and time) available to bring everyone online. In addition, users were often not prepared for dealing with the security risks during the new and overwhelming pandemic situation. Fear was also a bad adviser for many of them.

SMEs brought their operations and data online too quickly, without security processes, plans or tools in place. Numerous less publicised but still expensive attacks disrupt businesses every day. According to the *UK Cybersecurity Breaches Survey 2021* (UK, Department for Digital, Culture, Media and Sport 2021), 40% of all businesses and 65% of medium-sized businesses (those employing 50–200 persons) have experienced cybersecurity breaches in the last 12 months. Seven underlying cybersecurity issues amongst SMEs have been identified by the EU Agency for Cybersecurity (ENISA), including

- low cybersecurity awareness among staff,
- inadequate protection of critical and sensitive information,
- lack of budget,
- lack of cybersecurity specialists,
- lack of suitable cybersecurity guidelines specific to SMEs, and
- shadow ICT, that is, a shift of the work in the ICT environment out of the SME's control (ENISA 2021).

These are all substantial issues, and dealing with them is basic to achieving any level of security. The second half of the list includes issues that are beyond the power of an

individual SME to rectify, for example, the lack of cybersecurity talent and guidelines, and the shift to ever more complex digital solutions—these are more difficult to control or secure. The EU needs to step in and support member states and SMEs to address these issues.

Finally, critical infrastructure that is vital for society and the economy continues to lag behind in cybersecurity: healthcare facilities, energy grids, food and water supplies, public transport and more. There have been cyber-attacks on hospitals (Irish hospitals were shut down), government services (the Italian COVID-19 vaccination centres were taken down and the Bulgarian National Revenue Agency was the victim of a cyber-attack that resulted in the disclosure of the personal and financial data of the majority of the country's adult population), network management suppliers (SolarWinds) and US oil pipelines (Colonial Pipeline). These cybersecurity compromises have had major impacts on citizens, making cybersecurity everyone's problem. They were enabled by the poor security of the infrastructure and/or the failure of employees to contribute to the security of the systems.

Alongside the security weaknesses of the infrastructure, the low level of cybersecurity awareness and hygiene among users poses a severe risk to security and privacy. Human error is still the top reason for a cybersecurity incident. According to a CybSafe (2019) analysis of data from the UK Information Commissioner's Office, human error was the cause of approximately 90% of data breaches in 2019. This was up from 61% and 87% in the previous two years. Journalists even exploited poor cybersecurity hygiene (weak passwords) to introduce themselves at a secret EU Security Committee by guessing the password of one of the EU ministers present. These factors have created a massive opportunity for cybercriminals to exploit this knowledge and control critical infrastructure in a few clicks. COVID-19 has just made this a reality sooner than expected. Moreover, a hack is easier than we would like to admit. As evidenced by the highlighted attacks, cyber-attacks have the potential to paralyse critical sectors of the economy and society, and arguably, the whole economy.

As a result, the need to act on cybersecurity has arrived at the top of government agendas. In the EU, policymakers have approached the cybersecurity issue in a standard legislative way—that is, with recent agreements for a Cybersecurity Competence Centre and network of coordination centres, a proposal for a revamped EU Network and Information System Security Directive (NIS2), a series of awareness-raising initiatives for SMEs launched by ENISA and the announcement of the Cyber Resilience Act by Commission President von der Leyen in her State of the Union Speech (European Commission 2021b). We also finally saw the first-ever EU cyber sanctions in 2020.

In the US, cyber attribution and sanctions are not a novelty, and the Executive Order on Improving the Nation's Cybersecurity was swiftly signed in response to the above-mentioned incidents. A massive plan for increased investment in the cybersecurity of government services followed to support the Executive Order. In addition, the US president called upon the key US digital services companies, including Google, Microsoft,

Amazon and Apple, and the financial services industry, to raise the cybersecurity bar and help create a much-needed cybersecurity workforce.

## Lessons learned

For many years, cybersecurity was treated as a niche ICT problem. This is not the case anymore. The COVID-19 pandemic has brought about accelerated digitalisation and helped government leaders, businesses and end-users understand the importance of cybersecurity in building a sustainable digital future. If we are to live up to the high standard of security in our developed society and participate in a growing cyber economy, we need to address cybersecurity as a top priority and act upon it in various policy areas.

In this regard, cybersecurity creates an economic opportunity. Integrating cybersecurity into all aspects of life will provide opportunities for economic growth. The defence of cyberspace is a lucrative business. Cybersecurity expenditure has dramatically increased since the arrival of COVID-19: from \$40.8 billion in 2019 to an expected \$54.5 billion in 2020. The trend will continue post-COVID, with cybersecurity expenditure forecast at just under \$60 billion for 2021 (*Statista* 2021a).

To bring these benefits to Europe, we first need to fix the cybersecurity talent issue. The existence of talent is crucial for the development of value-added sectors, including cybersecurity. With a zero-unemployment rate in the sector, talent is the number one barrier to growth. According to the Cybersecurity Ventures projects, we will end 2021 with an astonishing 3.5 million unfilled cybersecurity jobs globally, with 400,000 of those in Europe alone (Morgan 2019). There is a rapidly growing global skills gap, which has increased threefold since 2014. Statista provides an insight into the skills shortage through a survey, showing that the major gaps are in cloud computing security, security analysis and investigation, application security, and risk and compliance administration (*Statista* 2021b). Collaborative professional education, provided online by a network of EU universities and the private sector (e.g. the Ubiquity University), could help address the need for affordable, cutting-edge, large-scale training schemes for cybersecurity experts and practitioners (Tasheva 2017).

In parallel, we need more cybersecurity solutions to be developed in Europe—eventually supporting the uptake of new European global cybersecurity service providers. To quote Commission President Ursula von der Leyen (European Commission 2021b): ‘It should be here in Europe where cyber defence tools are developed. This is why we need a European Cyber Defence Policy’.

Cybersecurity is part of diplomacy. Cybercrime is by its nature a transborder crime, but we lack the robust rules, institutions and operational cooperation to counter cybercrime at scale. Progress in building common cybersecurity institutions has been made since 2013, with ENISA receiving a stronger mandate to support cybersecurity capacity building and awareness, and the EU Agency for Law Enforcement bringing its Joint

Cybercrime Centre into operation to support member states' law enforcement agencies' operations against cybercrime. These institutions have already helped improve cybersecurity. However, they could be further developed (Tasheva 2017).

We need to expand the circle and engage more member states and third-country partners in fighting cybercrime together. Building EU cybersecurity resilience capacity will not only help us to protect but also support global cybersecurity development. We can leverage the EU's experience in setting globally recognised standards, such as the EU General Data Protection Regulation. An opportunity for this could be the design of the announced EU Cyber Resilience Act, which aims to set a common standard for cybersecurity (European Commission 2021b). Setting the standard for cybersecurity cooperation and defining cyber norms could benefit the global community and sustain the EU's soft power in the post-COVID world. A recent EU Institute of Security Studies report, *International Cyber Capacity Building: Global Trends and Scenarios*, concludes that there is growth in the field of cyber capacity in terms of investment, which is attracting more investment and new donors and depth: initially focused on cybercrime, cyber capacity has gradually expanded to include further areas of expertise, such as critical infrastructure, incident response, public awareness and diplomacy, amongst others. The report sees this growth as a sign that a new field of international cooperation is slowly being formed (Collett et al. 2021).

Cybersecurity is key to preserving human rights and democracy. Personal data were the number one attack target in 2020, with such breaches forming 58% of all data breaches (Verizon 2020). In 2021 personal data moved down to second place, after credential disclosure (Verizon 2021). Therefore, cybersecurity, that is, preserving data confidentiality, is vital for privacy. Furthermore, since COVID-19, most communication, including private conversations and relationships, has moved online. This has made the protection of communication channels and the confidentiality of data more important than ever in order to preserve users' privacy. We have observed, however, that multiple security weaknesses in online communication channels have been exploited, for example hacking Zoom passwords has allowed malicious actors to reveal the details of private meetings and even to take part in such gatherings. Moreover, autocratic government leaders have taken advantage of cybersecurity weaknesses. As revealed by the Pegasus scandal, a malicious code (spyware) developed by a private company was deployed by several autocratic governments, including European member states (Hungary), to intensively surveil the digital communications of their opponents, civil society leaders and even their own families. The spyware was very powerful, with the ability to activate the camera and microphone on demand. All content of messages, calls and agendas, and the GPS coordinates of those targeted by the spyware, were accessible to the attacker. This circumvented all privacy and democracy protection mechanisms, and the information obtained created a major risk for the targets.

Cybersecurity is necessary to ensure the success of democratic processes, such as evidence-based public debate and fair elections. Disinformation is still a major issue when it comes to the COVID-19 public debate. As a result, many have chosen not to

believe in the scientific data, acknowledge COVID-related health risks and/or be vaccinated against the disease (European Commission 2021a).

As for fair elections, we have seen several clear examples of attempts to hack the election process since 2016. Both the EU and the US have been affected by unprecedented election scandals triggered by security incidents—email leaks, spying, and website and infrastructure take-downs (distributed denial-of-service attacks) (NIS Cooperation Group 2018, Annex 1). In addition, there has been mass disinformation during elections (ENISA 2019; Benkler et al. 2020; Council of Europe 2020). However, while intensive cyber-attacks continue to target election processes, we seem to have learned a lesson. In subsequent elections—for instance, those for the European Parliament (2019), and the US (2020) and German (2021) national elections—the national security services have been better prepared and have countered cyber-attacks in time to avoid significant disruptions. Nevertheless, we must evolve and ensure continuous improvement to keep up with the ever-growing threats.

Finally, the way in which we implement cybersecurity also matters for human rights. While having the good intention of protecting data and infrastructure, we should not forget that security needs to work for people and not against them. We should avoid security tools that are too restrictive, abusive or involve mass surveillance. Diversity in the development processes (in terms of gender, race and language) can help us to develop better solutions with fewer discriminatory biases. We should also aim to make cybersecurity more inclusive—it should be affordable and accessible for everyone, not a luxury item available only to the young and the rich. More transparency and solutions are needed to ensure we achieve the above goals.

## Conclusions

The massive digital transition has posed cybersecurity challenges on three fronts: there are too many new users online, the digitalisation of SMEs and public services has been too rapid, and the level of cybersecurity resilience in critical infrastructure has been too low. There is significant room for improvement, and the EU has three instruments to achieve this—legislation, research and investment—and the mandate to act. The EU could lead the way in introducing a minimum level of cybersecurity, providing cybersecurity solutions and investment, and supporting and leveraging the capacity of the 27 member states to build true EU cyber resilience.

Europe should act swiftly to capitalise on the growing opportunity to boost the development of its modern cybersecurity industry. Efforts should focus on creating an environment for EU cybersecurity champions by upskilling and re-skilling cybersecurity talent, removing trade barriers and creating local cybersecurity demand.

With European cybersecurity solutions, we can export our values. The ability to protect the human right to privacy, sustain democracy and carry out effective diplomacy all depend on the security solutions we deploy at home and export globally. Setting the

standard for diversity in the development processes (in terms of gender, race and language) could help us to develop better solutions with no discriminatory biases. We should also aim to make cybersecurity more inclusive—it should be affordable and accessible for everyone, not only for the young or the rich.

As well as economic interest, the EU has the chance to deliver the high levels of security expected from its citizens and businesses. For instance, it could invest in increasing the minimum level of cybersecurity for government services, provide SMEs with cybersecurity tools and tax breaks, and fund cybersecurity education and awareness-raising for citizens.

To sum up, these are the key recommendations for EU policymakers' immediate action:

1. Agree on and adopt the ambitious EU NIS2 Directive and the Cyber Resilience Act with no delay. After their adoption, coordinate the transposition of the NIS2 Directive and its enforcement among the member states to ensure timely and effective implementation. Results should be better than in the past (e.g. the transposition of the NIS Directive, which has been ongoing since 2016).
2. Develop democracy, diversity and inclusion standards for cybersecurity tools and services. Encourage the uptake of solutions that correspond with our values through public procurement and societal awareness-raising on the topic.
3. Continue the cybersecurity awareness-raising and hygiene campaigns and translating materials into all EU languages to enable their easy reuse and dissemination in all member states.
4. Engage with major government and private-sector actors on the topic of cybersecurity.

In the medium term, EU policymakers should

1. develop the European cybersecurity industry through providing tax incentives, facilitating the accumulation of public market data, creating cybersecurity demand through legislation and public investment, and supporting the upskilling and re-skilling of talent;
2. support the development of robust cybersecurity rules, institutions and cooperation to counter cybercrime; and
3. lead the debate on global cyber norms and develop globally accepted cybersecurity standards.

## References

Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J., & Schmitt, C. (2020). *Mail-in voter fraud: Anatomy of a disinformation campaign*. Berkman Centre

- Research Publication no. 2020-6. 2 October. <https://ssrn.com/abstract=3703701>. Accessed 29 September 2021.
- Collett, R., Barmpalious, N., & Pawlak, P. (2021) *International cyber capacity building: Global trends and scenarios*. EU Institute of Security Studies. Luxembourg. <https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios>. Accessed 26 September 2021.
- Council of Europe. (2020). Democracy hacked? How to respond? Resolution 2326. <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28598&lang=e>. Accessed 29 September 2021.
- CybSafe. (2020). Human error to blame for 9 in 10 UK cyber data breaches in 2019. 7 February. <https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/>. Accessed 27 September 2021.
- ENISA. (2019). *Election cybersecurity challenges and opportunities*. February. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities>. Accessed 29 September 2021.
- ENISA. (2021). *Cybersecurity for SMEs – Challenges and recommendations*. 28 June. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>. Accessed 24 September 2021.
- European Commission. (2021a). Fighting disinformation. [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_en). Accessed 29 September 2021.
- European Commission. (2021b). State of the Union address by President von der Leyen. 15 September. [https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH\\_21\\_4701](https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701). Accessed 27 September 2021.
- Eurostat. (2021). ICT specialists – Statistics on hard-to-fill vacancies in enterprises. June. [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT\\_specialists\\_-\\_statistics\\_on\\_hard-to-fill\\_vacancies\\_in\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises). Accessed 26 September 2021.
- Euractiv. (2021). Germany probes claims of pre-election MP hacking by Russia. 10 September. <https://www.euractiv.com/section/global-europe/news/germany-probes-claims-of-pre-election-mp-hacking-by-russia/>. Accessed 29 September 2021.
- Fernandez, S., Jenkins, P., & Vieira, B. (2020). Europe's digital migration during COVID-19: Getting past the broad trends and averages. *McKinsey*, 24 July. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages>. Accessed 28 September 2021.
- Malekos Smith, Z., & Lostri, E. (2020). *The hidden cost of cybercrime*. McAfee. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>. Accessed 13 September 2021.
- Morgan, S. (2019). Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021. *Cybercrime Magazine*, 24 October. <https://cybersecurityventures.com/jobs/>. Accessed 14 September 2021.
- NIS Cooperation Group. (2018). *Compendium on cyber security of election technology, Annex I*. CG Publication 03/2018, July. [https://www.ria.ec/sites/default/files/content-editors/kubertur/cyber\\_security\\_of\\_election\\_technology.pdf](https://www.ria.ec/sites/default/files/content-editors/kubertur/cyber_security_of_election_technology.pdf). Accessed 29 September 2021.
- Statista. (2021a). Areas with biggest shortage of cybersecurity skills within organizations worldwide in 2021, by technology category. <https://www.statista.com/statistics/1259502/cybersecurity-skills-shortage-tech-categories-worldwide/>. Accessed 29 September 2021.
- Statista. (2021b). Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted). <https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending>. Accessed 14 September 2021.

- Tasheva, I. (2017). *European cybersecurity policy: Trends and prospects*. EPC Policy Brief, 8 June. [https://www.epc.eu/content/PDF/2017/European\\_cybersecurity\\_policy.pdf](https://www.epc.eu/content/PDF/2017/European_cybersecurity_policy.pdf). Accessed 26 September 2021.
- UK, Department for Digital, Culture, Media and Sport. (2021). *Cyber security breaches survey 2021*. 24 March. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>. Accessed 26 September 2021.
- Verizon. (2020). *2020 data breach investigations report*. <https://enterprise.verizon.com/resources/reports/dbir/2020/dbir-report/>. Accessed 27 September 2021.
- Verizon. (2021). *2021 data breach investigations report. Results and analysis*. <https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/>. Accessed 7 October 2021.

### Author biography



**Iva Tasheva** is the co-founder and cybersecurity lead at CYEN, a consultancy. She is a member of ENISA's Ad-Hoc Working Group on Enterprise Security and a board member of the DPO Circle.



# Saving EU digital constitutionalism through the proportionality principle and a transatlantic digital accord

European View  
2021, Vol. 20(2) 150–156  
© The Author(s) 2021  
DOI: 10.1177/17816858211055522  
journals.sagepub.com/home/euv



**Jan Czarnocki**

## Abstract

The article explains the importance of the emerging movement for EU digital constitutionalism (EUDC), which reflects a Union-wide effort to address through regulation the challenges posed by digitalisation. The article outlines the core legislative acts that have been introduced by proponents of EUDC. It describes why EUDC is important for fundamental rights protection and European foreign policy, and how the ‘Brussels effect’ extends the impact of EUDC. It enquires into whether EUDC is sustainable, taking into consideration waning EU global influence and the need for economic growth. The EU needs to strike a balance between fundamental rights protection and economic growth. The proportionality principle is the right tool for this. A proportional approach should be followed in establishing a transatlantic digital accord with the US—an agreement on the basic principles governing the digital space. A more proportional approach will pave the way to such an agreement—giving EUDC a global scope.

## Keywords

Digital constitutionalism, Digitalisation, Digital single market, EU–US relations, Information technology law, Proportionality principle

## Introduction

EU digital constitutionalism (EUDC) is a regulatory movement which aims to address the challenges posed to society by digitalisation (De Gregorio 2021). The movement also aims to counteract the growing power of data, which jeopardises the sovereignty of the

---

### Corresponding author:

Jan Czarnocki, KU Leuven Centre for IT & IP Law – imec; Sint-Michielsstraat 6 box 3443, Leuven, 3000, Belgium.

Email: [jan.czarnocki@kuleuven.be](mailto:jan.czarnocki@kuleuven.be)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

state and threatens fundamental rights. EUDC aims to adopt the values of contemporary constitutionalism and apply them to the digital society (Celeste 2019, 1–5). The ‘digital’ in EUDC refers to the development of the digital space, based on the progress in information technologies and their application. ‘Constitutionalism’ refers to defining the fundamental principles and rules governing society and the state. EUDC does not seek to change the most basic normative principles and rules governing society, such as the constitutions of the member states or the treaties. However, the challenge posed by digitalisation, and the scope and impact of new regulations, legitimise comparison to constitutional norms.

Digitalisation and the merging of interactions in the physical world with those online have compressed geographical distances and bridged physical barriers. They have enabled the flow of volumes of information that were previously unthinkable. The resultant infosphere has created a new space for humans to flourish in and for economic growth (Floridi 2014; Rifkin 2014). On the other hand, digitalisation challenges the social structure, creating numerous tensions. Concepts such as platform, informational or surveillance capitalism (Srnicek 2017; Cohen 2019; Zuboff 2019), and data power (Lynskey 2019) describe some of the ways in which the infosphere may threaten our fundamental rights. For example, nudging, manipulation (Sunstein & Thaler 2009; Yeung 2017) and monopolies are omnipresent in the platform economy (Stucke and Ezechachi 2016).

The EU has taken on the role of a global leader in addressing these challenges. It is the only governing power that has found the will to effectively regulate the growing power of Google, Amazon, Facebook, Apple and Microsoft (‘GAFAM’, as per Rikap 2021). Moreover, it is the only governing power that has not allowed the good of society to be overtaken by either the oligarchic interest of powerful digital capital, as in the US, or by a totalitarian will to use digital tools to subjugate the population, as in China. The EU’s global leadership in regulating the digital world has so far been fuelled by the ‘Brussels effect’—the ability of the EU to leverage and externalise its demanding rules by setting high-level standards for access to the single market (Bradford 2012). However, it is not clear how long the EU will be able to maintain its economic might or whether loosening the regulatory burden may be necessary to foster the economic growth needed to protect social stability and cohesiveness. Also, the overall decline of Europe as a global player may damage its ability to be a leader in setting the rules in the digital space.

The success of EUDC will mean the protection of EU citizens from the dangers posed by digitalisation. However, for EUDC to succeed, the EU must take a more pragmatic approach. First of all, this means showing more respect for the proportionality principle—that is, setting clear priorities and avoiding overregulation. Second, we need a transatlantic digital accord, meaning an international treaty with the US on the basic principles governing the digital space. While this would probably result in less ambitious regulation, such an agreement would ensure that EUDC has a truly global scope. Without this, the EU would remain the only jurisdiction with high and ambitious standards, but would be operating in an uneven environment for economic competition.

## What does EUDC consist of?

So far, EUDC consists of a few cross-sectoral regulations which have set up a partial framework for conduct in the digital space. Initially the achievements of EUDC consisted of rudimentary laws regulating, for example, the flow of goods and services online, such as the eCommerce Directive (European Parliament and Council 2000), and the protection of personal data, such as the Data Protection Directive (European Parliament and Council 1995). During the first decades of the twenty-first century the pace of digitalisation accelerated, and so did the regulatory initiatives to tackle it. Entering into force in 2018, the General Data Protection Regulation (GDPR) (European Parliament and Council 2016) is a shining example of the success of EUDC and its global clout. The regulation impacted thinking about how to regulate and protect personal data all around the world. This is evidenced by the copying of some of the rights and obligations of the GDPR in, among others, China, Turkey and Colombia. In addition to legislation, the decisions of the European Commission and the jurisprudence of the European Court of Justice contributed to forming the movement for EUDC. These were also decisions and cases against GAFAM companies.

Currently the EU is in the middle of designing and enacting a comprehensive regulatory package that will revolutionise the digital economy. This effort was spearheaded by the publication of the *Digital Single Market Strategy* (European Commission 2015), which set the agenda for the development of the digital economy in the EU. The planned measures aim to set a level playing field for the future. They range from laws to protect competition in the digital economy, enhance data protection, and create data markets and repositories, to safeguarding the safety of artificial intelligence (AI) systems.

The GDPR will soon be supplemented by the ePrivacy Regulation (European Commission 2017)—a law setting out the rules for the confidentiality of electronic communication, including machine-to-machine communication. The work on the ePrivacy Regulation is taking longer than expected due to an inability to find political consensus. However, if its basic tenet is retained—the need for providers to ensure the confidentiality of electronic communication data and meta-data—it will have an impact on what kinds of data can be used for analytical purposes and how they can be used. For example, the use of communication data and meta-data to target advertisements will be curtailed, and pop-up ads on social media directly related to the content of your communications will no longer be possible.

The Digital Markets Act (DMA) (European Commission 2020b) will define a catalogue of behaviours harmful to online competition. The DMA aims to protect weaker economic actors from abuses by platform owners and other digital services providers. For instance, the DMA will oblige platform owners to disclose data related to the activity of the businesses on its platform to those businesses, which previously they have not had to do—something which is the source of a major economic and contractual power imbalance. The implementation of such a rule will mean that smaller players will be less dependent on the platform owner and have access to more business intelligence. But the

DMA goes much further than this, also translating the principles of competition law doctrine into the digital space—an important tool in fighting monopolies online.

The Digital Services Act (European Commission 2020a) will establish rules for content provision and moderation in the digital space. It will also establish clear rules of responsibility for the content. By obliging service providers to comply with transparent terms of service and setting rules for content moderation, as well as obliging service providers to notify the relevant authorities of possible crimes, the Act will end the discretionary power of major players, that is, GAFAM, to censor content. People will no longer be at the mercy of the platform owners to allow their freedom of speech and access to digital town squares, which these platforms currently act as.

The AI Act (European Commission 2021a) will set the rules and conditions for introducing AI systems into the single market. It aims to safeguard a dignity-centred approach to the development of AI systems. This will involve prohibiting AI systems that pose a risk to fundamental rights. The AI Act will establish due diligence and compliance rules but will also ban risky AI systems. For example, the act will probably ban most facial recognition systems and will oblige the users of AI to notify citizens if they are exposed to an algorithm able to materially distort their behaviour.

Finally, the Data Governance Act (European Commission 2020c) and Data Act (European Commission 2021b) will create rules for sharing data and creating data hubs. Both regulations aim to enable orderly and free data sharing in order to unleash the potential of data flows and their applications in the European economy. The Data Governance Act will regulate the rights and obligations of data intermediaries, while the Data Act will regulate and facilitate the process of data sharing. Both regulations are the means through which a new data market is to be established. This is the EU's way of regaining the competitive edge that it has already lost in the field of commercial platforms, which are dominated by US-originating companies.

## **Proportionality and the global impact of EUDC**

The Brussels effect has so far sustained the global reach of the EU's ambitious digital agenda (Bradford 2012) by leveraging the market power of the EU to force entities wishing to enter the single market to accept higher legal standards. For cost reasons, once a company intends to comply with EU standards, it makes much more sense for it to do so in all of its operations. The consequence is that some companies based outside the EU also comply with the EU's higher legal standards. So far, the Brussels effect has had an impact in fields such as product and food safety, data protection, the exploitation of natural resources, plane emissions and antitrust. It is an open question as to what extent the Brussels effect will impact EUDC, because of the many different areas it will regulate.

Still, there is no doubt that the global leadership of the EU is necessary to secure democratic values and the protection of fundamental rights against both unrestrained capitalism and digitally enabled totalitarian tendencies in the digital realm. However, to

support this agenda the EU must cooperate globally and reach an agreement with other key players—with the US as a priority—to make sure that European values are as strongly held outside of the EU. This will guarantee a stable and secure digital space for Europeans in the years to come. But to reach a transatlantic agreement on the digital space, the EU must bear in mind both what unites us with and what divides us from our cousins across the ocean.

The neoliberal ideology found in *The Closing of the American Mind* (Bloom 1987)—which justifies, for example, extreme social inequality and a lack of public healthcare—is alien to Europeans, who are habituated to the social market economy. However, the EU's proclivity to regulate does indeed constrain innovation and economic growth. Thus, as much as protecting fundamental rights against the dangers of the digital space is imperative, this needs to be balanced against the need for economic growth, which sustains the stability and cohesiveness of our society. And that is why a more American, laissez-faire approach might be needed. At present the EU is not considered a business-friendly environment, especially when it comes to setting up a company in the digital economy. The compliance burden that has to be met by new businesses forces them to hire lawyers from the outset of operations as the regulatory wall is otherwise incomprehensible. This hampers EU growth and innovation.

Therefore, the EU needs to set its priorities and use the proportionality principle more. This means only imposing regulatory burdens where it is essential. Such an approach, aiming to simplify the rules and putting more emphasis on the freedom to innovate and conduct business, would necessarily lower the scope of protection. But it would also open up the field for establishing a transatlantic consensus on the digital space—the only way in which, in the long term, our most basic fundamental rights in this space can be effectively protected.

## Conclusion

A transatlantic digital accord should be a pillar of the free, democratic world extended into the digital realm. But striking it will not be an easy task. The US has so far failed to properly safeguard the fundamental rights of its citizens in the digital space. It is a long way behind the EU in this regard. This can clearly be seen in the lack of comprehensive privacy and data protection, as well as in the problems faced when trying to set up a legal regime to regulate platforms and their monopolistic practices. The enormous political and lobbying power of digital giants and the strong oligarchic tendencies within the US democracy hinder the process. The ongoing Department of Justice antitrust lawsuits against the owners of the platforms are just the first steps to better regulation. However, it is American scholars and civil society that have taken action and conceptualised the dangers of the digital space (Zuboff 2019; Cohen 2019; Kapczynski 2020).

The geopolitical situation is forcing like-minded partners to come together to fight for freedom in the digital space. We are at present witnessing the emergence of the great digital divide between the democratic and the authoritarian worlds. The former is

addressing the social challenges posed by digitalisation and trying to streamline the development of the digital space in a way that serves democracy. In the latter, we are seeing the weaponisation of the digital space to control society on the one hand, and on the other, to use it as a tool against the free world. The digital authoritarianism of China (Lilkov 2020), followed by Russia and the other acolytes of authoritarianism, will naturally bring the EU and the US together. But this political will should lead to an agreement on contentious issues in order to seal the transatlantic relationship in the digital realm.

A few of the critical issues regarding the digital space that the EU and the US need to resolve are personal data protection, responsibility for content, taxation, competition protection and the regulation of AI systems. Reaching agreement on all of them will not be easy, and signing an international treaty will take years. But we need to start this process. Only by coming together can we face the challenges posed not only by the digital space itself but also by our adversaries using it as a tool against us. The EU should start by moderating EUDC through a more conscious use of the proportionality principle and then sit down at the table with the Americans to start negotiating the Transatlantic Digital Accord.

## References

- Bloom, A. (1987). *The closing of the American mind*. New York: Simon and Schuster.
- Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, 107(1), 1–68.
- Celeste, E. (2019). Digital constitutionalism: A new systematic theorization. *International Review of Law, Computers & Technology*, 33(1), 76–99.
- Cohen, J. (2019). *Between truth and power: The legal constructions of informational capitalism*. New York: Oxford University Press.
- De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70.
- European Commission. (2015). *A digital single market strategy for Europe*. Communication, COM (2015) 192 final, 6 May.
- European Commission. (2020a). Proposal for a regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM (2020) 825 final, 15 December.
- European Commission. (2020b). Proposal for a regulation on contestable and fair markets in the digital sector (Digital Markets Act). COM (2020) 842 final, 15 December.
- European Commission. (2020c). Proposal for a regulation on European data governance (Data Governance Act). COM (2020) 767 final, 25 November.
- European Commission. (2021a). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM (2021) 206 final, 21 April.
- European Commission. (2021b). Public consultation on the Data Act. 3 June. <https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act>. Accessed 22 September 2021.
- European Parliament and Council. (1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L281 (23 November), 31.

- European Parliament and Council. (2000). Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). OJ L178 (17 July), 1.
- European Parliament and Council. (2016). 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). OJ L119 (27 April), 1.
- European Parliament and Council. (2017). Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM (2017) 010 final, 10 January.
- Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford: Oxford University Press.
- Kapczynski, A. (2020). The law of informational capitalism. *The Yale Law Journal*, 129(5), 1460–1515.
- Lilkov, D. (2020). *Made in China: Tackling digital authoritarianism*. Wilfried Martens Centre for European Studies. Brussels. Accessed 7 October 2021.
- Lynskey, O. (2019). Grappling with 'data power': Normative nudges from data protection and privacy. *Theoretical Inquiries in Law*, 20(1), 189–220.
- Rifkin, J. (2014). *The zero marginal cost society: The Internet of Things, the collaborative commons, and the eclipse of capitalism*. New York: Palgrave Macmillan.
- Rikap, C. (2021). *Capitalism, power and innovation: Intellectual monopoly capitalism uncovered* (1<sup>st</sup> edition). London: Routledge.
- Srnicek, N. (2017). *Platform capitalism*. Oxford: Polity Press.
- Stucke, M. E., & Ezrachi, A. (2016). *Virtual competition*. Cumberland: Harvard University Press.
- Sunstein, C. R., & Thaler, R. H. (2009). *Nudge: Improving decisions on health, wealth, and happiness*. London: Penguin.
- Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–36.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1<sup>st</sup> edn.). New York: PublicAffairs.

## Author biography



**Jan Czarnocki** is a doctoral researcher and Maria Skłodowska-Curie Fellow at the KU Leuven Centre for IT & IP Law. He studies IT law, with a focus on privacy, data protection (biometric data in particular) and digital policy.



# The technology challenge in the transatlantic relationship

European View  
2021, Vol. 20(2) 157–165  
© The Author(s) 2021  
DOI: 10.1177/17816858211059251  
journals.sagepub.com/home/euv



**Raluca Csernaton**

## Abstract

Technological innovation has become a critical element of international cooperation and geopolitical rivalry. This has impacted key areas of the transatlantic partnership, presenting both opportunities and challenges for EU–US relations, either rejuvenating a relationship mired in rifts or deepening those rifts. Instead of examining how these structural cracks have emerged and are growing, this article zooms in on the challenge to transatlantic relations posed by technological innovation, both as a driver of cooperation and a cause for further rivalry. In doing so, the article explores three interrelated elements: the transatlantic technology gap and the EU's quest for technological sovereignty, approaches to technological innovation and the role of emerging and disruptive technologies, and the values-based governance of digital and technology issues. As fast-paced technological transformation continues to disrupt societies and economies on both sides of the Atlantic, technology should be at the heart of a revived phase in EU–US cooperation and trust.

## Keywords

Transatlantic relationship, EU–US cooperation, Technological sovereignty, Emerging and disruptive technologies, Regulation

## Introduction

‘Happy families are all alike; every unhappy family is unhappy in its own way,’ Leo Tolstoy wrote as the opening line of his nineteenth-century novel, *Anna Karenina*. This description is clearly applicable to the transatlantic partnership. The relationship sometimes shares a common set of attributes leading to enhanced cooperation; yet any of a variety of diverging elements can cause friction. Indeed, there has been a recurrent pattern of rapprochement, cooperation, tension and conflict in much of the transatlantic

---

### Corresponding author:

R. Csernaton, Carnegie Europe, 15 Rue du Congrès, 1000 Brussels, Belgium.  
Email: [raluca.csernaton@ceip.org](mailto:raluca.csernaton@ceip.org)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

relationship across the decades. Scholars have branded it an entangling alliance, a deepening rift, a case of mutual dependence, and a special or even the most important strategic relationship (Kaplan and Honick 2007; Anderson et al. 2008; Peterson and Pollack 2003; Smith 2011; Haar et al. 2021). Thus, viewing the transatlantic link from a longer-term perspective makes one more cautious about making judgements about how healthy the relationship is and whether it is changing for the better or the worse. Often the rhetoric surrounding rifts is overcharged (Jones 2004), making it difficult to assess the situation accurately.

In this article the transatlantic relationship is defined as the overall set of relations between the US and the EU, relations that are maintained via engagements in institutions such as NATO (Smith 2018, 539). This relationship has been intimately linked to the ebbs and flows of two interconnected structural changes. First, since the end of the Cold War era, systemic changes in the international arena have seen successive US administrations and European leaders alternate between fully embracing shared views and interests, with limited disagreement on certain issues, and episodes of acute discord and crisis. To name a few points of disagreement, the US-led invasion of Iraq; nuclear strategy; and international development, monetary and trade policies have caused many furrowed brows in both European capitals and Washington. These issues all arose long before the US strategic pivot towards Asia, disagreements over China, the lingering effects of former President Donald J. Trump's transactional approach to foreign policy, data privacy and the recent responses to the novel coronavirus pandemic.

Second, structural changes in the EU integration project and the increasing supranationalisation of the EU's defence policy have also had powerful repercussions. The growing role of the European Commission in defence technological and industrial matters and the launch of the European Defence Fund, an unprecedented funding scheme financed directly from the EU budget to support homegrown European collaborative defence research and development (Håkansson 2021), have raised concerns across the Atlantic. In recent years, a new momentum in EU defence integration has taken shape around the concept of European strategic autonomy, coupled with pragmatic policy steps and initiatives prioritising European sovereignty in defence industrial areas, as well as technological and digital matters (Csernaton 2021b). This growing supranationalisation has been partly triggered by the combination of former President Trump's vitriolic stance towards the EU and NATO, the EU losing its strongest transatlantic link with the UK's departure, and the evolving international technological rivalry between the US and China. Such challenges have called for a critical reappraisal of European autonomy and dependency in key technological areas, from defence, emerging and disruptive technologies (EDTs), and the digital domain, to space. Conversely, EU talk and action to spend more on military and technological power have provoked fears that European defence and technological cooperation will lead to industrial rivalry with the US or a duplication of NATO's efforts.

Against this backdrop, instead of broadly examining how the structural cracks in the transatlantic bond have emerged and are growing, this article zooms in on the challenges

to the relationship posed by technological innovation, both as a driver of cooperation and as a cause for further rivalry. In doing so, the article explores three core and interrelated dimensions:

- the transatlantic technology gap and the EU's quest for technological sovereignty—namely the desire to strengthen Europe's technological competitive edge, support a strong industrial base and reduce dependencies in critical technology areas and value chains;
- differing approaches to technological innovation and the role of emerging and disruptive technologies; and
- the values-based governance and regulation of digital and technology issues.

In the shifting geopolitical context, the EU and the US share values and have a common interest in navigating the current and emerging technology challenges together by leveraging their common strengths and operationalising a transatlantic technology agenda. As fast-paced technological and digital transformations continue to disrupt societies, economies and geopolitics, technology must be at the heart of a revived phase in EU–US cooperation and trust. Granted, this will be easier said than done.

## **Tech transatlanticism in perspective**

In early 2021 there was widespread optimism in Europe that the end of the Trump era would also put an end to toxic transatlanticism (Soare 2020), especially once the new Biden administration had taken office in the White House. After all, no ties between two strategic partners are as closely knitted in economic, security and political affairs as those between the EU and the US (Alcaro et al. 2016). While it is too early to tell whether a change in the White House will usher in a new momentum for trust and partnership or rivalry in transatlantic relations, several developments paint conflicting pictures. On the one hand, the EU–US summit in Brussels in June 2021 (European Council 2021) marked a sea change in tone and overall rhetoric, expressing a desire to revive and deepen transatlantic relations. This was further substantiated by the summit's announcement of the establishment of an EU–US Trade and Technology Council (TTC). This body will serve as a forum for the US and the EU to coordinate approaches to key global trade, economic and technology issues based on their shared democratic values (European Commission 2021b). On the other hand, the US's chaotic withdrawal from Afghanistan in August 2021 and scant prior consultation with its European and NATO allies, coupled with the launch of AUKUS, a security alliance between the US, the UK and Australia, through which Australia will acquire US nuclear-powered submarines at the expense of scrapping a previous agreement with France (Balfour 2021), forebode a grimmer reality. Rhetorical reassurances aside, these realities spell a sobering realisation in Europe that it risks becoming a mere instrument (Brattberg 2021) or an expendable partner and foreign-policy afterthought in the US's geopolitical calculations and rivalry with China.

### *The EU's quest for technological sovereignty*

The Biden administration is marching headlong into restructuring the transatlantic alliance. While the diplomatic tone has been normalised, Washington is broadly following in the footsteps of the Trump administration and its attitude towards European efforts to achieve greater strategic autonomy in defence and technological sovereignty. The Biden administration also aims to prioritise outright opposition to China, including in technological and industrial matters, while the EU is taking a more nuanced approach. The technology dossier sees the US and the EU sharing common concerns, from the protection of Western democratic values in trade and tech relations, and mitigating threats such as unfair competition and the misuses of new technologies by authoritarian regimes, to strengthening transatlantic technological and industrial leadership and expanding bilateral investments (European Council 2021). Yet the US and the EU are divided by differing approaches to technological innovation and regulation, and the relationship between the public and private sectors. In addition, there is an overall technological gap between the EU and the US (Locatelli 2007). In this respect, the EU's ambition has been to gain greater autonomy and increase its capacity to act in the global tech race (Sahin and Barjer 2021), as well as to catch up in some technological niches such as drone technologies (Csernatoni 2021a), artificial intelligence (AI) (Brattberg et al. 2020) and, more recently, semiconductors (Poitiers and Weil 2021). How the EU can square its ambitions for more European technological and digital sovereignty with strengthening cooperation with the US is an interesting puzzle. Unsurprisingly, calls for more European strategic autonomy and technological sovereignty were perceived as expressions of anti-Americanism and a Europe-first rationale during the Trump administration, and these perceptions are not likely to change under the Biden administration.

With this in mind, it remains to be seen whether such perceptions will take a positive turn or become even more corrosive in the long run. The launch of the EU–US TTC seems to be a constructive step in the right direction, and towards more cordial and pragmatic transatlantic ties. To be clear, transatlanticism and European strategic autonomy and technological sovereignty are not mutually exclusive geopolitical concepts (Soare 2020). Behind the EU's strategic autonomy and technological sovereignty agendas is a need to stay ahead of the curve when it comes to innovation and development, as well as to achieve a new level of EU engagement in the global (tech) balance of power. Technological and digital sovereignty, even if they are conceptually vague notions (Csernatoni 2021b), are at the very heart of such ambitions. They are equally complemented by EU statements that support deeper collaboration with the US and like-minded partners on issues related to the democracy–technology nexus (Brattberg 2021).

Overall, the increasing technological gap is detrimental to the health of the transatlantic relationship. The gap poses several technological and (geo)political challenges and, most importantly, it is up to Europe to take on the burden of bridging it. Paradoxically, such European efforts will also vex US officials and complicate transatlantic cooperation. It is undeniable that the US is in a class of its own in terms of technological advancement, while the EU and its member states have only recently started to think strategically

about a more structured and comprehensive approach to Europe's technological and digital sovereignty. To this end, the Commission's February 2021 Action Plan, the 'Three-Point Belt Plan' (European Commission 2021a), on creating synergies between the civil, defence and space industries, is one way ahead. It proposes a top-down and cross-domain approach to boosting research, technology development and the EU's overall innovation power. The 17-page-long action plan mentions 'technological sovereignty' no less than eight times.

### *Emerging and disruptive technologies*

EDTs range from AI, big data, future-generation wireless technologies, quantum computing, new advanced materials and hypersonic weapons, to autonomous robotics, to name just a few. They have become central elements in political and policy discussions at the EU level (Calcara et al. 2020). American and Chinese tech giants such as Google, Apple, Microsoft, Facebook, Baidu, Alibaba, Huawei and Tencent are leading the latest developments in these strategic fields, advancing the US's and China's quests for global tech supremacy. The European Commission's 2021 Three-Point Belt Plan also identified EDTs (European Commission 2021a, 2) as a critical area for EU intervention, due to their relevance across the defence, space and related civilian industries, and as essential to Europe's technological sovereignty by reducing the risk of over-dependence on external players, including the US.

The above EU-led approach to technological innovation and development is indicative of a distinctive strategy that combines a structured approach to establishing appropriate EU-level processes and mechanisms for tech and digital-related instruments and funding opportunities, with efforts to rationalise member states' efforts to reduce duplication and maximise added value. The strategy aims to foster synergies among the relevant EU-funded instruments and facilitate civilian–space–defence cross-fertilisation (spin-ins and spin-offs), especially in terms of cross-border collaboration between EU member states and supporting small and medium-sized enterprises. Taking something between a more laissez-faire approach and a top-down dirigiste one to technological innovation, the EU, and especially the European Commission, seems to be adopting a hands-on style and a more centralised rationality in governing the innovation and funding of EDTs at the supranational level. The arguments in support of such a top-down harmonised approach are usually about the significant 'costs of non-Europe' in the areas of research and innovation, the failure of Europe's tech innovation system to rationalise efforts and deliver the expected economic impact, and the fragmented nature of public and private research between individual EU member states and the European Commission.

Conversely, in terms of public–private dynamics, the US has traditionally been steeped in a laissez-faire spirit of entrepreneurial innovation and has cultivated a business-friendly environment with minimal involvement from the US administration—which has traditionally delegated power to industry and service providers. This bottom-up policy approach to innovation is an extension of the technology-neutral stance of state non-interference and limited regulation. It also follows the broader US cultural strokes

that prioritise competitive entrepreneurship over governance. Yet, when it comes to critical technology areas and the combined power of American big tech, it could be argued that there has been a shift in US policymaking regarding state action to preserve national security and geopolitical interests, as well as to rein in the influence of tech giants. With respect to geopolitical reasons, this shift is accounted for by the fact that much of the tech agenda during recent years has focused on supporting US competitiveness against China. The US has further urged other countries and the EU to follow the same strategy, while also identifying critical and emerging technologies in which it can compete against China (Brattberg 2020). However, when it comes to regulating tech giants, the US seems to be following the EU's lead. Biden's July 2021 'Executive Order on Promoting Competition in the American Economy' states that the US will address challenges to competition in the American information technology sector created by dominant Internet platforms that 'use their power to exclude market entrants, to extract monopoly profits, and to gather intimate personal information that they can exploit for their own advantage' (US, White House 2021).

### *Values-based regulation of tech*

Both the EU and the US have taken steps to set new standards for responsible innovation in EDTs, particularly in the case of AI development (Brattberg et al. 2020). Steps have also been taken to limit the monopolistic surveillance and data-harvesting power of big tech and digital platforms by ushering in a new era of regulation. These are important areas of transatlantic technology cooperation, focusing on the proper regulation and evaluation of potential misuses of EDTs, as well as on their human rights, democratic and ethical implications. Concerning the regulation of tech giants, the EU has been a first mover (Csernatori 2021b). There are also signs of converging attitudes in the transatlantic debate on anti-trust issues, competition policy, and the human-centric and responsible development of EDTs such as AI. Data governance, digital regulation and establishing technological standards were set out as areas for potential collaboration at the EU–US summit on 15 June 2021, both for the envisaged EU–US TTC and for the respective working groups dealing with the various technology and digital-related portfolios.

The underlying goals of transatlantic technological cooperation are (1) to promote shared approaches to responsible innovation and human-centric models for research on, and the development and deployment of EDTs (especially AI); (2) to ensure the democratic accountability of online digital platforms; (3) to facilitate the free flow of data and its governance; and (4) to collaborate on building the resilience of digital and technology global supply chains. In terms of regulatory interventions, the EU has certain advantages that it should seek to better capitalise on when it comes to international engagement and building and reinforcing partnerships. The EU's experience with data privacy regulation, with its flagship General Data Protection Regulation, could serve as an example for establishing global norms for emerging technologies and the private sector. Indeed, the EU's 'White Paper on AI' (European Commission 2020c) and the proposed AI regulation (the 'AI Act') (European Commission 2021c), as the first-ever attempts to regulate AI, are likely to influence the global regulatory debate.

EU leaders have argued that technological and digital sovereignty is also about protecting European culture and values (European Commission 2020b), in which fundamental rights are prioritised. With the new strategy of a Europe Fit for the Digital Age (European Commission 2020a), the European Commission wants to deliver on the promise of human-centric and risk-based tech regulation as part of a comprehensive regulatory package that includes the European Digital Strategy, the European Data Strategy, the Digital Services Act, the Digital Markets Act and the proposed AI Act (European Commission 2021c). The aim is to create a safer and more open digital space, establish a level playing field when it comes to gatekeeper online platforms and propose comprehensive legislation targeting AI uses. The White House has also released its AI Principles, which focus on a strategy for engaging in the creation of AI technical standards, and an AI regulatory document intended to ensure the trustworthy development, testing, deployment and adoption of AI technologies (Brattberg 2020).

Thus, aligning transatlantic strategies on tech regulation, including on the issue of responsible AI innovation and data privacy, is very much needed to promote the stronger global democratic governance of EDTs. While respecting some differences and challenges across the Atlantic when it comes to data privacy debates, data transfers, data taxation and regulation, the EU and the US should endeavour to actively combine the EU's global regulatory prowess and the US's commercial competitive edge in technology (Bradford and Csernatoni 2021). Indeed, the Biden administration appears to be willing to collaborate with the EU on the broad strokes of responsible technological innovation and digital regulation. But some of the EU's actions, especially concerning data privacy, digital taxation and antitrust, are still issues that need to be ironed out in the transatlantic relationship (Brattberg 2020). The new EU–US TTC forum might be the best place to politically address such sources of friction, as well as to lead the values-based governance of the technological and digital transformation.

## Conclusion

The ghosts of crises past are likely to shape contemporary and future realities in EU and US relations. Should the EU and the US not reconcile their differences concerning the technology challenge, there could be severe economic consequences in store for the future of transatlantic trade and economic relations. The global governance of EDTs would also benefit from stronger multilateral international and transatlantic cooperation, especially in a world where technology is increasingly emerging as a key driver of great-power rivalry and authoritarianism. What is also certain is that the negative perception across the Atlantic that the EU is becoming increasingly supranationalised in key fields such as defence and technological innovation, coupled with the EU's regulatory interventions when it comes to (mostly American) tech giants, could cement in place a complicated dynamic in the transatlantic relationship. Alongside views that the EU is becoming an economic, tech and security competitor to the US, such worrying perceptions will likely continue to fuel a sceptical attitude in Washington. Yet, differing US and EU perspectives should not preclude cooperation on technological and digital matters, but instead be taken as the starting point for key areas of deeper dialogue amid a broader

context of global geopolitical rivalry. In the end, the transatlantic relationship, however structurally estranged or challenged, remains one of the most integrated bonds from the democratic, economic and security points of view.

## References

- Alcaro, R., Greco, E., & Peterson, J., eds. (2016). *The West and the global power shift: Transatlantic relations and global governance*. London: Palgrave Macmillan.
- Anderson, J. J., Ikenberry, G. J., & Risse, T. (2008). *The end of the West?: Crisis and change in the Atlantic order*. Ithaca, NY: Cornell University Press.
- Balfour, R. (2021). What the U.S.–British–Australian security pact means for Europe. *Judy Dempsey's Strategic Europe*, 21 September. <https://carnegieeurope.eu/strategieurope/85392>. Accessed 27 September 2021.
- Bradford, A., & Csernaton, R. (2021). Toward a strengthened transatlantic technology alliance. In R. Balfour (ed.), *Working with the Biden administration: Opportunities for the EU*. Carnegie Europe, 26 January. <https://carnegieeurope.eu/2021/01/26/working-with-biden-administration-opportunities-for-eu-pub-83560>. Accessed 27 September 2021.
- Brattberg, E. (2020). *Reinventing transatlantic relations on climate, democracy, and technology*. Carnegie Endowment for International Peace, 23 December. <https://carnegieendowment.org/2020/12/23/reinventing-transatlantic-relations-on-climate-democracy-and-technology-pub-83527>. Accessed 27 September 2021.
- Brattberg, E. (2021). Transatlantic relations after Biden's first 100 days. *Carnegie Endowment for International Peace*, 6 May. <https://carnegieendowment.org/2021/05/06/transatlantic-relations-after-biden-s-first-100-days-pub-84472>. Accessed 27 September 2021.
- Brattberg, E., Csernaton, R., & Rugova, V. (2020). *Europe and AI: Leading, lagging behind, or carving its own way?* Carnegie Endowment for International Peace, 9 July. <https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236>. Accessed 27 September 2021.
- Calcara, A., Csernaton, R., & Lavallée, C., eds. (2020). *Emerging security technologies and EU governance. Actors, practices and processes*. Abingdon: Routledge.
- Csernaton, R. (2021a). Between rhetoric and practice: Technological efficiency and defence cooperation in the European drone sector. *Critical Military Studies*, 7(2), 212–36.
- Csernaton, R. (2021b). The European Union's sovereignty agendas: A quest for technological power: From strategic autonomy to technological sovereignty. *Carnegie Europe*, 12 August. <https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134>. Accessed 27 September 2021.
- European Commission. (2020a). Europe fit for the digital age: Commission proposes new rules for digital platforms. Press release, 15 December. [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2347](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347). Accessed 27 September 2021.
- European Commission. (2020b). Europe: The keys to sovereignty. 11 September. [https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty\\_en](https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en). Accessed 27 September 2021.
- European Commission. (2020c). *On artificial intelligence – A European approach to excellence and trust*. White Paper. COM (2020) 65 final, 19 February. [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf). Accessed 27 September 2021.
- European Commission. (2021a). *Action plan on synergies between civil, defence, and space industries*. Communication. COM (2021) 70 final, 22 February. <https://ec.europa.eu/info/>

- files/action-plan-synergies-between-civil-defence-and-space-industries\_en. Accessed 27 September 2021.
- European Commission. (2021b). EU–US launch Trade and Technology Council to lead value-based global digital transformation. Press release, 15 June. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_21\\_2990](https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990). Accessed 27 September 2021.
- European Commission. (2021c). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM (2021) 206 final, 21 April. [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF). Accessed 19 September 2021.
- European Council. (2021). EU–US summit, Brussels, 15 June. <https://www.consilium.europa.eu/en/meetings/international-summit/2021/06/15/>. Accessed 27 September 2021.
- Håkansson, C. (2021). The European Commission’s new role in EU security and defence cooperation: The case of the European Defence Fund. *European Security*. doi:10.1080/09662839.2021.1906229.
- Kaplan, L. S., & Honick, M. (2007). *NATO 1948: The birth of the Transatlantic Alliance*. Lanham, MD: Rowman & Littlefield.
- Locatelli, A. (2007). The technology gap in transatlantic relations: A cause of tension or a tool of cooperation? *Journal of Transatlantic Studies*, 5(2), 133–54.
- Peterson, J., & Pollack, M. A. (2003). *Europe, America, Bush. Transatlantic relations in the twenty-first century*. London: Routledge.
- Poitiers, N., & Weil, P. (2021). A new direction for the European Union’s half-hearted semiconductor strategy. *Bruegel*, 15 July. <https://www.bruegel.org/2021/07/a-new-direction-for-the-european-unions-half-hearted-semiconductor-strategy/>. Accessed 27 September 2021.
- Sahin, K., & Barker, T. (2021). *Europe’s capacity to act in the global tech race. Charting a path for Europe in times of major technological disruption*. DGAP Report no. 6, 22 April. <https://dgap.org/en/research/publications/europes-capacity-act-global-tech-race>. Accessed 27 September 2021.
- Soare, S., ed. (2020). *Turning the tide. How to rescue transatlantic relations*. European Union Institute for Security Studies. Paris. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Transatlantic%20relations%20book.pdf>. Accessed 27 September 2021.
- Smith, M. (2011). European responses to US diplomacy: ‘Special relationships’, transatlantic governance and world order. *The Hague Journal of Diplomacy*, 6(3–4), 299–317.
- Smith, M. (2018). The EU, the US and the crisis of contemporary multilateralism. *Journal of European Integration*, 40(5), 539–53.
- US, White House. (2021). Executive Order on promoting competition in the American Economy. White House Briefing Room, 9 July. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/>. Accessed 27 September 2021.

## Author biography



**Raluca Csernatoni**, is a visiting scholar at Carnegie Europe in Brussels, where she leads the workstreams on European security and defence, as well as emerging and disruptive technologies. She is also a guest professor with the Brussels School of Governance of the Free University of Brussels. She co-edited the book, *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*, which was published by Routledge in 2020.

# Regulating artificial intelligence in the EU: A risky game\*

European View  
2021, Vol. 20(2) 166–174  
© The Author(s) 2021  
DOI: 10.1177/17816858211059248  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Dimitar Lilkov**

## Abstract

The EU continues its quest to draw the contours of innovative legislation for the digital domain. The European Commission's draft Regulation on artificial intelligence (AI) is a clear departure from previous 'soft' attempts to set the rules through ethical principles and industry pledges. The EU aspires to be the first global player to adopt a comprehensive framework that classifies and regulates the roll-out of AI software and hardware within its internal market. The draft rules try to provide legal certainty for public and private bodies across the EU, while making sure that potential risks to its citizens are minimised. This article sketches out some of the most important provisions of the draft Regulation and tries to critically assess its potential shortcomings related to implementation and enforcement. The final version of the AI proposal should avoid the mistakes of previous attempts to draft transnational rules for the online space and establish a sufficiently flexible legal framework.

## Keywords

Artificial intelligence, Ethics, European Commission, Regulation, Risk

## Introduction

The advent of complex algorithms, machine learning and automated decision-making processes is no longer a prospect of the distant future. Smart software and hardware are steadily being rolled out across the EU in order to provide convenience, connectivity and new services to users. From a regulatory perspective, however, this opens the door for new challenges and frictions. How do you reap the benefits of artificial intelligence (AI) and advanced technology, while ensuring that they do not cause societal harm? It would

---

## Corresponding author:

D. Lilkov, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, Brussels, B-1000, Belgium.  
Email: [dli@martenscentre.eu](mailto:dli@martenscentre.eu)

\*An earlier version of this article was published on the AI Policy Consulting Blog and can be found at [www.aipolicyconsulting.com/the-eu-s-new-rules-on-ai](http://www.aipolicyconsulting.com/the-eu-s-new-rules-on-ai)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

appear that this was the foundational question that guided the experts behind the European Commission's latest regulatory proposal on AI (European Commission 2021).

In the last few years, the debate on AI governance has mostly been centred on ethical frameworks and pledges for foundational AI principles. Leading international organisations (OECD 2019) and international fora (*G20 Information Centre* 2019) have issued their considerations for the ethical and trustworthy application of AI, while a number of multinational digital companies have raced ahead to announce the principles of AI application and development in their services too (Pichai 2018; Amershi et al. 2019). The EU's own initial efforts led to the creation of a high-level expert group on AI, which presented its *Ethics Guidelines for Trustworthy AI* in 2019. The EU's initiative received a positive welcome, even though there were allegations that private industry had had too much of an influence within the expert group and that the final result was one of 'ethics-washing' (*Tagesspiegel* 2019).

All of these documents or pledges share a similar commitment to human dignity and protecting basic rights, as well as to providing unbiased algorithms, accountability and the safeguarding of user privacy. Interestingly, similar noble commitments to ethics and trustworthiness can be found in the white papers of Chinese scientific organisations, private companies and government-affiliated Chinese think tanks (MERICS 2021). One can only wonder if any of these commitments is tenable, given China's grim human rights track record and its unique model of state-led digital authoritarianism (Lilkov 2020).

For EU policymakers, it has become apparent that neither self-regulation by the industry nor ethical standards will suffice in such a complex field. With its April 2021 legislative proposal (European Commission 2021), the Commission takes a clear step beyond ethics by introducing binding rules for AI systems placed on the EU market. The draft AI Regulation would apply to both public and private actors, providers and users of such systems, irrespective of whether they are established within the Union or in a third country. Given the size and importance of the European internal market, EU policymakers intend to create a spillover effect and nudge other countries to develop similar frameworks. It is noteworthy that the horizontal rules proposed by the Commission were not developed in a vacuum—there is an upcoming update on EU rules to address liability issues related to new technologies (European Commission 2020b), as well as a revision of the relevant sectoral safety legislation.

This article tries to provide a brief overview of the voluminous draft text and its innovative framework for regulating the potential risks and harms generated by specific uses of AI. It is important to note that the Commission does not aim to regulate the advanced technology itself. The goal is to create future-proof harmonised rules on the use of AI that will ensure trust among users, increase its uptake, and provide legal certainty for public bodies and private companies. The following sections try to assess some of the most important provisions of the Commission's proposal.

## Pyramid of risk

While the Commission's draft does not give a definition of the term 'artificial intelligence', it defines AI systems as software that is developed with certain machine learning, knowledge-based or statistical approaches (the full list can be found in European Commission 2021, Annex I). The proposal recognises that while AI systems can be a driver for economic and societal advancement, they can also 'bring about new risks or negative consequences' (European Commission 2021, 1). Consequently, the centrepiece of the AI proposal is the introduction of four categories of risk, which set different obligations for the providers of AI systems.

At the top of this 'risk pyramid', the draft Regulation establishes an explicit list of prohibited AI practices which create 'unacceptable risk' (European Commission 2021, Title II) as they violate fundamental rights or go against EU values. The prohibitions cover AI applications that have a high potential to 'manipulate persons through subliminal techniques beyond their consciousness' (European Commission 2021, 12) or exploit the susceptibilities of specific vulnerable groups in a manner that could cause them or others physical or psychological harm. This provision is laudable, but open to interpretation. What is the objective threshold for psychological harm? How will this explicit prohibition apply to certain algorithms for behavioural nudging that are commonly found online (Matz et al. 2017)? Some of these techniques go beyond simple digital marketing tools for generating additional clicks. For example, complex recommendation algorithms in social media and on video-sharing platforms can lead users to polarising disinformation or extremist online content (Bradshaw et al. 2020). Given the likely challenges related to ascertaining a direct link between algorithmic manipulation and obvious harm to the user, it is questionable whether this outright prohibition will actually have practical value in the future.

An additional prohibition applies to AI-enhanced social scoring by public authorities for measuring the trustworthiness of individuals based on their social behaviour or predicted personality characteristics. The EU wants to signal that data-driven societal management, similar to China's nascent social credit system (Drinhausen and Brusse 2021), would pose unacceptable risks for European citizens. It seems that this provision also aims to prohibit future experiments which may lead to the creation of 'digital welfare states'. For instance, in 2020 a Dutch court ruled against attempts to optimise the country's social welfare system through the use of an algorithmic risk-scoring system (Lomas 2020a).

Real-time remote biometric identification systems (i.e. facial recognition systems) in public spaces for the purpose of law enforcement also appear in the list of banned AI systems. However, the Commission has envisaged several exceptions to the ban when this type of technology could be used to search for the victims of crime, to prevent imminent threats to life or to identify criminal perpetrators (European Commission 2021, art. 5). This provision remains contentious for many stakeholders, for instance civil society campaigners, who advocate a stronger ban on facial recognition in public spaces, as it is

allegedly prone to misuse and could potentially discriminate against certain societal groups (EDRI 2020). There are also shortcomings related to the scope of the prohibition—it applies only to ‘real-time’ systems, which excludes systems that could biometrically analyse footage from a recording and could have a ‘chilling effect on the exercise of fundamental rights and freedoms’ (EDPB and EDPS 2021, para. 31). An additional caveat is that the prohibition does not preclude actors from using such biometric identification for non-law enforcement purposes, such as crowd control or public health (Veale and Borgesius 2021, 9).

Title III of the draft can be seen as an essential section of the Regulation as it deals with the classification of AI systems which are considered to be ‘high risk’. The Commission’s proposal considers an AI system to be high risk if it is either a safety component of a product falling under certain EU harmonised legislation (machinery, toys and medical devices) or a stand-alone AI system in other defined sectors which could pose a high risk to the safety or health of EU citizens (the full list can be found in European Commission 2021, Annex III). The Commission would be able to update this list through delegated acts.

High-risk AI systems would need to comply with a set of stringent *ex ante* requirements, including a conformity assessment, before their rollout within the EU. A bundle of mandatory obligations is also envisaged *ex post*; for example, the provision of high-quality datasets, detailed technical documentation, comprehensive record-keeping and an appropriate level of human oversight. Chapters two and three of the section on high-risk systems provide an exhaustive list of all the responsibilities and obligations that fall on the providers of such systems. The assessment should be conducted by an independent national ‘notified body’ or by the provider of the AI system, depending on its specific type.

What would be the cost of compliance with such a stringent set of requirements? A study requested by the European Commission suggests that the estimated cost for an AI product to comply with the potential new requirements would be close to €10,000, while the purchase of additional services or staff could increase the cost to €30,000 (Renda et al. 2021). These are, of course, approximate figures, which depend on many future factors that might push costs up or down. Here, one can make the valid supranational argument that the absence of harmonised legislation might bring about a fragmented system of national requirements, which would lead to even higher compliance costs for European businesses as they would have to deal with a patchwork of AI regimes and national standards.

At the bottom of the ‘risk pyramid’, the draft text sets out the obligations for AI systems which are regarded as posing ‘limited’ or ‘minimal’ risk. AI systems which directly interact with real people (e.g. chatbots) and present a risk of potential manipulation would need to comply with transparency obligations. Such systems would be considered of ‘limited risk’ and users should be fully aware that they are interacting with a machine or software algorithm.

Lastly, all other AI systems will be viewed as posing ‘minimal risk’. According to the Commission, these will comprise the vast majority of future AI systems. However, providers of such systems could voluntarily apply the mandatory requirements for high-risk AI systems or adhere to voluntary codes of conduct.

## **Governance and enforcement**

EU member states would have to designate one or more national competent authorities to oversee the implementation of the new Regulation (European Commission 2021, art. 59). Each EU country would have to appoint a national supervisory authority, which would act in two important capacities. First, it would act as the ‘notified body’ which would be responsible for drawing up the necessary procedures and appointing the independent authorities that would verify the myriad requirements for the high-risk AI systems discussed above. The notified bodies would be able to issue certificates for compliance with the mandatory requirements. These certificates would be valid for a period of no longer than five years. All official notified bodies would need to be registered on a list created by the European Commission.

Second, the national supervisory authority would also act as a market surveillance authority, controlling the national market and investigating compliance with the necessary rules for high-risk AI systems. This would ensure *ex post* enforcement of the rules and provide public authorities with the necessary powers to ‘intervene in case AI systems generate unexpected risks, which warrant rapid action’ (European Commission 2021, 15).

Additionally, the draft rules provide for the creation of a European AI Board comprised of representatives from the member states and chaired by the Commission. It would be responsible for facilitating the harmonised application of the Regulation across the EU and ensuring smooth cooperation between the national supervisory authorities.

For breaches of the Regulation’s provisions, the Commission has proposed certain thresholds for sanctions, similar to those for the General Data Protection Regulation. Infringement of prohibited practices or non-compliance related to data requirements would lead to administrative fines of up to €30 million or 6% of the company’s worldwide annual turnover in the preceding financial year (whichever is higher) (European Commission 2021, art. 71). Non-compliance with any other requirement or obligation could lead to fines of up to €20 million or 4% of global annual turnover (European Commission 2021, art. 71).

## **Future considerations**

These are just some of the most noteworthy provisions of the proposed Regulation. The text has yet to be subjected to the legislative scrutiny of the European Parliament and Council. The final Regulation will apply after a further transition period of two years after the text is officially adopted.

One of the biggest challenges to implementing the EU's future AI rules is the setting up of a coherent and effective governance framework across the continent. The intricate web of national bodies entrusted with the implementation of the Regulation might face budgeting or technical capacity issues. As a comparison, a number of national data protection authorities across the EU member states have struggled to enforce the General Data Protection Regulation (Lomas 2020b) due to problems with inadequate staffing or limited resources (Ryan and Toner 2020). In a similar way, EU member states might diverge in the way that they supervise and enforce AI rules within their jurisdictions.

At the same time, the Commission has tried to boost its own role and promote a more supranational approach to governance. For instance, it is expected that the Commission will have a strong role in the proposed European AI Board. Additionally, the Commission would be able to officially challenge the competence of national notified bodies if there were substantial reasons to doubt whether they were complying with the necessary requirements. These are valid steps, but a general concern remains about the adequate implementation and enforcement of the new AI rules across the EU.

Something curious can be observed here. The newly created European AI Board will function in parallel with the existing European Data Protection Board (European Parliament and Council 2016, art. 68). Additionally, the draft Digital Services Act (European Commission 2020a) proposes the creation of a European Board for Digital Services, which would contribute to the oversight of large online platforms. All of these structures will be comprised of national representatives with the support of the Commission. It will be interesting to observe how these quasi-federalist structures will interact in the future and whether this unique governance framework will yield the required results.

The AI proposal tries to address the potential regulatory burden on small businesses and start-ups. The Commission (2021, art. 53) has suggested the creation of regulatory sandboxes which would foster innovation by providing a controlled environment for the development and testing of new AI systems. The national competent authorities would be at the forefront of creating such sandboxes, meaning that smaller companies would rely on the proactivity of their respective national administration. It is unclear whether this would create time constraints or would actually be beneficial. European policymakers should explore additional options for supporting small and medium-sized enterprises and start-ups and reducing their costs for compliance with the new rules.

In terms of AI funding or improving the EU's standing globally, the European Commission has put forward the 2021 Coordinated Plan on AI. The plan maps out ways to accelerate private and public investment and foster better synergies between member states. The Commission is committed to ensuring the EU's 'global leadership in trustworthy AI' even though Europe is still lagging behind in comparison to actors such as the US or China (Castro and McLaughlin 2021). The draft Regulation is the first global attempt to legislate on AI and set up the necessary obligations for the providers of complex systems. Even though these issues are also being debated in the US, Washington has

placed more emphasis on the implications of AI for national security and how the country can claim leadership in a domain heavily contested by China (NSCAI 2021).

In closing, it should be mentioned that the Commission's AI proposal joins ranks with other draft pieces of EU legislation in search of a fragile regulatory balance in the digital domain. How can innovation be fostered and allow for new services, while also protecting users from the negative externalities of invasive data-driven technologies? The draft AI Regulation is neither a panacea which will automatically guarantee Europe's leadership in AI nor a draconian legislative over-reach that will stifle innovative potential across the continent. It should be seen as a unique attempt to welcome new technologies but also embed basic European values in a chaotic digital universe that is expanding beyond our comprehension. It is essential that European policymakers learn from previous regulatory mistakes and develop a flexible-enough but binding framework with the help of all concerned stakeholders. This endeavour is risky but much needed as it will send a clear signal to the global community that the AI race should not be allowed to become a race to the bottom.

## References

- Amershi, S., Weld, D., Vorvoreanu, M., Fournery, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P., Inkpen, K., Teevan, J., Kikin-Gil, R., & Horvitz, E. *Guidelines for human-AI interaction*. Microsoft Research. doi.org/10.1145/3290605.3300233.
- Bradshaw, S., Bailey, H., & Howard, P. (2020). *2020 global inventory of organized social media manipulation*. Oxford Internet Institute. <https://demtech.oii.ox.ac.uk/wpcontent/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf>. Accessed 6 October 2021.
- Castro, D., & McLaughlin, M. (2021). Who is winning the AI race: China, the EU, or the United States? — 2021 update. *Information Technology and Innovation Foundation*, 25 January. <https://itif.org/publications/2021/01/25/who-winning-ai-race-china-eu-or-united-states-2021-update>. Accessed 6 October 2021.
- Drinhausen, K., & Brusse, V. (2021). *China's social credit system in 2021: From fragmentation towards integration*. Mercator Institute for China Studies. 3 March. <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>. Accessed 6 October 2021.
- EDPB & EDPS (European Data Protection Board & European Data Protection Supervisor). (2021). *Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. 18 June. [https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en). Accessed 6 October 2021.
- EDRI (European Digital Rights Initiative). (2020). EU's AI law needs major changes to prevent discrimination and mass surveillance. April. <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/>. Accessed 6 October 2021.
- European Commission. (2020a). *Proposal for a Regulation on a single market for digital services (Digital Services Act)*. COM (2020) 825 final, 15 December 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>. Accessed 6 October 2021.
- European Commission. (2020b). *Report on the safety and liability implications of artificial intelligence, the Internet of Things and robotics*. COM (2020) 64 final, 19 February. <https://eur-lex>.

- europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064. Accessed 6 October 2021.
- European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence*. COM (2021) 206 final, 21 April 2021. [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF). Accessed 6 October 2021.
- European Parliament and Council. (2016). Regulation (EU) no. 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). OJ L119 (27 April), 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Accessed 6 October 2021.
- G20 Information Centre. (2019). Ministerial statement on trade and digital economy. 9 June. <http://www.g20.utoronto.ca/2019/2019-g20-trade.html>. Accessed 6 October 2021.
- Lilkov, D. (2020). *Made in China: Tackling digital authoritarianism*. Wilfried Martens Centre for European Studies. Brussels, 11 February. <https://www.martenscentre.eu/publication/made-in-china-tackling-digital-authoritarianism/>. Accessed 6 October 2021.
- Lomas, N. (2020a). Blackbox welfare fraud detection system breaches human rights. Dutch court rules. *Techcrunch*, 6 February. <https://techcrunch.com/2020/02/06/blackbox-welfare-fraud-detection-system-breaches-human-rights-dutch-court-rules/?renderMode=ie11>. Accessed 6 October 2021.
- Lomas, N. (2020b). GDPR's two-year review flags lack of 'vigorous' enforcement. *Techcrunch*, 24 June. <https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/>. Accessed 6 October 2021.
- Matz, S. C., Kosinski, M., Nave, G., & Stillwel, D. (2017). Psychological targeting in digital mass persuasion. *Proceedings of the National Academy of Sciences*. doi:10.1073/pnas.1710966114.
- MERICs (Mercator Institute for China Studies). (2021). *Lofty principles, conflicting incentives: AI ethics and governance in China*. 24 June. <https://merics.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china>. Accessed 6 October 2021.
- NSCAI (National Security Commission on Artificial Intelligence). (2021). *Final report: National Security Commission on Artificial Intelligence*. 19 March. <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>. Accessed 6 October 2021.
- OECD. (2019). *Recommendation of the Council on artificial intelligence*. 22 May. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Accessed 6 October 2021.
- Pichai, S. (2018). AI at Google: Our principles. *Google Blogs*, 7 June. <https://www.blog.google/technology/ai/ai-principles/>. Accessed 6 October 2021.
- Renda, A., Arroyo, J., Fanni, R., Laurer, M., Sipiczki, A., Yeung, T., Maridis, G., Fernandes, M., Endrodi, G., & Milio, S. (2021). *Study to support an impact assessment of regulatory requirements for artificial intelligence in Europe*. 21 April. <https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195>. Accessed 6 October 2021.
- Ryan, J., & Toner, A. (2020). *Europe's governments are failing the GDPR*. Brave. <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf>. Accessed 6 October 2021.
- Tagesspiegel. (2019). Ethik-Waschmaschinen made in Europe. 8 April. <https://background.tagesspiegel.de/ethik-waschmaschinen-made-in-europe>. Accessed 6 October 2021.
- Veale, M., & Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4). <https://ssrn.com/abstract=3896852>. Accessed 6 October 2021.

**Author biography**

**Dimitar Lilkov** is a research officer at the Wilfried Martens Centre, where he is responsible for matters involving the digital economy, energy and the environment. Dimitar is the host of the Martens Centre's 'Brussels Bytes' podcast series on technology and European policy.



# Ethics and governance in the digital age

European View  
2021, Vol. 20(2) 175–181  
© The Author(s) 2021  
DOI: 10.1177/17816858211061793  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Jana Mišić**

## Abstract

This article argues that ethics need not be toothless or side-lined in the technology governance debates. Rather, moral evaluation is necessary, even when legal compliance is already possible. Moral evaluation supplies answers not only to what is legal or illegal, but also to what is good and better for society. The article first defends a pragmatist ethics approach to uncovering the inevitability of values and norms embedded in digital technologies and related to their design and use. It then makes the case for policymakers engaging in the anticipatory ethics of technology. This approach provides a toolbox to tackle moral dilemmas and better understand what trustworthiness and ethics mean in certain contexts. The convergence of ethics and policy is not only worth pursuing but a necessity for good technology governance if we are to achieve a Europe fit for the digital age.

## Keywords

Ethics, Governance, Emerging technologies, Anticipatory ethics of technology

## Introduction

Controversies related to issues such as fake news and voting manipulation, privacy and surveillance, algorithmic discrimination and bias (to name a few) have prompted increased public scrutiny of digital technologies over the last decade. It has become clear that both end-users and those associated with technology development are eager to part with the ‘move fast and break things’ mentality of Silicon Valley and have found an alternative by shifting the focus to ethics and the ethical design and use of these technologies. The pertinence of advancing the ethical approach was solidified in 2019 when then newly elected President of the European Commission, Ursula von der Leyen, set a 100-day deadline for her Commission to propose policies to shape the future digital

---

### Corresponding author:

J. Mišić, Rathenau Instituut, Anna van Saksenlaan 51, 2593 HW Den Haag, The Netherlands.  
Email: [j.misic@rathenau.nl](mailto:j.misic@rathenau.nl)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

policy of the Union. Furthermore, making ‘Europe fit for the digital age’ was inaugurated as one of the six key areas of her agenda for Europe (European Commission 2021).

Yet, almost as quickly as ethical technology discourse has proliferated across the digital world, it has become apparent that changing the mantra will not suffice. The limitations of making ethics a buzzword have become discernible: ethics is often too abstract and toothless; it can be subsumed into corporate logics and incentives, or it can be kept in the echo-chambers of either the policymakers or the individual engineers who are now expected to build it into their everyday work (Green 2021). As a result, critics have voiced concerns about ‘ethics washing’ and ‘ethics bashing’ (Bietti 2020), that is, the promotion of ethics research to defuse criticism and regulation without committing to ethical behaviour.

While it has become clear that there is a significant gap between the theory of ethics principles for artificial intelligence (AI) or the Internet of Things, and the practical design and governance of these systems, this article argues that their convergence is not only worth pursuing but a necessity for good technology governance if we are to achieve a Europe fit for the digital age. To do so, two preconditions have to be met. The first defends the *ethics approach* to uncovering the inevitability of the values and norms embedded in digital technologies and surrounding their design and use. The second, then, is this approach’s contribution to the anticipatory governance of technology. The key proposal of this article is that ethics does not need to be superficial and depoliticising; rather, a practical, pragmatist ethics for emerging digital technologies would be a useful resource for the better anticipation and future governance of technology.

## The importance of ethics in technology debates

It was only a few decades ago that the development of the ethics of technology as a discipline in its own right began (Franssen et al. 2018). This late emergence may seem odd given the importance technology has played in human progress, especially since the industrial revolution. However, without going into the rich history of the field, it is important to note two things. Initially, the dominant stance was one of technological determinism, or the value-neutrality thesis, that attributes consequences to the users of technology, rather than to the technological tools themselves, their designers or the design process.

As Joseph Pitt (2014, 95) famously asked, ‘Where are the values?’ in a specific bridge, smartphone or algorithm. Indeed, the physical manifestation of values, particularly in the age of digital technologies, is a tricky business. Pitt argued that people, their actions and the context contain or express values, *not* artefacts. Depending on how technology is used, the plethora of values it embodies are subject to change—an algorithm can be used for the better synthesis of information, but it can also be used as a tool of discrimination. Intuitively, however, it seems insufficient to claim that the artefact itself is void of values in its design or use. Consider Amazon Rekognition, facial recognition software that matched 28 members of Congress, disproportionately people of colour, with criminal

mugshot images (Snow 2018). If the algorithm discriminated, is it not possible that this was (inadvertently) built into its data training set, the choice of algorithmic models or perhaps its deep learning logic?

The stance that technologies embody, advance or hinder certain values countered the value-neutrality thesis rather promptly. Novel views include conceptualisations of technology as a political phenomenon, a social activity, a cultural phenomenon, a professional activity (engineering ethics) or a cognitive activity (Franssen et al. 2018). In this article, we zoom in on the idea that technology can embody specific forms of power and authority. Langdon Winner (1980), the proponent of the political artefacts thesis, claims that certain technologies can indeed show us where values are, in the sense that they demand compatibility with certain social and political relations. For example, nuclear power plants or autonomous warfare drones seem to require a hierarchical, authoritative management structure. This structure is often closed, exclusive and a cause of moral dilemmas among policymakers and the public. Technology as a political artefact can also embody political bias. Winner refers to the Long Island overpasses which were designed in such a way that public buses could not pass underneath. This meant that the main users of public transportation, that is, the poorer black classes, were less likely to access Manhattan's public parks. Thus, while the design fulfilled the task of highway transportation, it also encompassed 'purposes far beyond original use' (Winner 1980, 125). To avoid such a negative political function, what is needed is a certain level of democratisation of technological development, that is, the inclusion of ordinary people in its shaping. This is not always possible, and so we are left with the open-ended question of how to ensure 'democratic' innovation.

Democratic innovation demands awareness from users of how to value the trade-offs (privacy versus autonomy, safety versus sustainability, etc.) that are inherent in governing technologies. Value trade-offs, on the other hand, can only be revealed by engaging with the ethics or normativity of digital technologies. Ethics answers the question of what ought to be done and aids us in delineating the notions such as trustworthiness, justice, fairness or privacy that permeate discussions on policymaking and technological innovation. It does so in at least one important way. The ethicists of technology may make or choose to abstain from prescribing a certain course of action, but their work brings clarity about which values are asserted as a rationale for choices at the forefront of the design or implementation of technology.

As an analytical approach, infusing ethics into the assessment process thus helps to articulate norms and value assumptions. Beyond the hard impacts that we can measure, such as formal procedures (e.g. risk impact assessments) or legal regulation (e.g. the General Data Protection Regulation), ethics draws out the soft impacts as well (Swierstra 2015). Examples of the soft impacts of technology can be the consequences for wellbeing, relationships, quality of life, identity or social order. For example, with the proliferation of cameras and facial recognition, privacy takes on the form of a struggle for intimacy and control over one's identity. Along these lines, some have argued that soft and hard ethics are complimentary—that pure regulation is not enough, and that what is

legal is not necessarily conducive to the idea of a good society or a good life (Floridi 2018).

## **Navigating the soft and hard ethics of technology**

What digital innovation will bring next is an exciting prospect. Innovation in its own right is something that we value, and technological innovation especially so, particularly in modern society. The question is, what comes next? A new essential healthcare app reliant on AI? A quantum computing smartphone in everyone's pocket? Or a smart assistant that goes beyond informing us about the weather or playing a favourite song? In any case, the future seems to be riddled with disruptive digital and emerging technologies. Unlike mature technologies, emerging technologies such as deep learning algorithms are still in their infancy—the research and development phase—and their exact impact is uncertain and difficult to predict. This disruption is both exciting and challenging since it presupposes that innovation leads and everything else follows: expectations, labour conditions, habits, norms, business models and standards of living (Floridi 2018).

To understand the disruptive effects of emerging digital technologies, we need to turn to practice-oriented forms of ethics. These kinds of ethics emphasise that norms and values are a part of our engagement with the world. Engagement is not only theoretical but practical as we continuously have to make value judgements: is autonomy more valuable than giving away our personal choice to AI recommendation systems for the sake of comfort? Pragmatist ethics offers a way to understand the interaction between technology, values and the world as a lived practice. It stresses the process instead of the values as objective entities and implies that values are interactive, dynamic and tied to doing. The argument is as follows: bearing in mind all other factors, but zooming in on technology, the introduction of new technologies creates consequences that require new moral responses (e.g. the value of sustainability has become very pronounced lately), but also creates new opportunities, new moral dilemmas (e.g. predictive genetics) and new experiences (e.g. online dating). Arising from these, new morally problematic situations require new moral solutions, and thus we can speak of technologically induced value change.

Without going into epistemological and ontological questions about values, we can agree that human interactions and experiences lead to a certain conceptualisation of what the right thing to do is and how this might change over time or with context, leading to a chance to review our actions. People might still use the terms 'privacy' or 'autonomy', but the meanings attached to them might change. Before the introduction of algorithms into the decision-making process, the ability to make judgements and decide on 'fairness' was reserved for people. Today, however, some consider that an algorithm might be better suited to making fairer, more bias-free decisions than a human. The value judgements that people make are not necessarily entirely subjective, nor would pragmatists require them to be. But they would stress their function as evaluative devices in specific situations from which we learn. As time goes by, morality then tends to go unnoticed as it has been routinised in regular evaluations of what should or should not be done. However, this is also why emerging technologies cause a reflection on morality:

something that we have never considered before challenges the routine. An example would be the use of autonomous drones for military purposes, which cause a shift in a soldier's moral experience and in the moral responsibility assigned to/felt by soldiers (Boenink and Kudina 2020). This continuous evolution and interaction between morality and technology has been called 'technomoral change' (Swierstra et al. 2009) and is essential to any debate about the ethics and governance of any technology. The question now becomes: how should we imagine future governance in lieu of technomoral change to achieve what the EU has called a human-centric approach?

## **Anticipatory ethics and governance**

The key point of this article is that ethics need not be superficial and depoliticising; rather, it can be conducive to good technology governance. Let us consider the validity of this claim in the context of the governance of AI, a key emerging digital technology today. A great many public and private actors have issued statements on how AI will change society, culminating in the advent of ethical guidelines (Jobin et al. 2019). However, as noted earlier, a significant gap exists between the theory of principles and practical design and governance. High-level principles are vague and difficult to operationalise in the 'what' and 'how' of AI governance. That being the case, we then turn to tools such as ethical impact assessments or privacy assessments as ethics checklists, which are often too strict and unresponsive to specific contexts. Privacy within the family and at home has a different value to us compared to privacy in public, for example.

As argued above, digital technologies are morally disruptive, and since they are currently in their nascent phase, it is difficult to evaluate just what societal impact they will have. It is therefore important to seek out future concerns and the likely technomoral value change. This is where ethics comes in. This article proposes that not only engineers but policymakers should be involved in the anticipatory ethics of technology (AET) (Brey 2012). The AET approach combines ethical analysis and foresight methods with public and stakeholder engagement. As such, it provides enough interaction between future policy and ethics, as well as addressing the three levels of technology in society: the type of technology, the features of the specific artefact and its application level (Brey 2017, 187). In simpler terms, the process should analyse (1) the risks of AI as an emerging technology, (2) the algorithms and their inherent properties, and (3) their application in a specific context. The analysis starts with foresight, identification and the weighing of ethical issues. In the final stage, after the evaluation, ethicists engage with other stakeholders, such as policymakers. In the governance stage, recommendations are made specifically for each context, avoiding the vagueness of ethics principles and the strictness of generic impact assessments. What is more, the toolbox of foresight methods is rich: stakeholders can engage in horizon scanning, scenario-based methods, expert consultations, relevance trees, the Delphi method, trend analysis, road mapping and participatory deliberation (Brey 2017, 185–6).

While policymakers do consider the future in their evaluation, the dominant narrative is that moral evaluation is not necessary when legal compliance is already available. The

debates surrounding the General Data Protection Regulation exemplified this. However, legal compliance is not enough if the policy is to steer society in the right direction. Moral evaluation then supplies the answer to not only what is legal or illegal, but also what is good and better for society. Such an endeavour should be the preferred state for both ethics (values and judgements) and governance (the management of technology).

## Conclusion

What does it mean for an emerging technology to be ‘fair’ or ‘non-discriminatory’ in terms that can be operationalised? Providing a rigorous understanding of these terms has long been a preoccupation of moral and political philosophers, and their work can help illuminate policymaking. It can also help to guide societal discussions on how we want to proceed with innovation and the use of emerging technologies. This article has advocated that ethics is not toothless, but can be constructive and pragmatic in the best sense possible. A forward-looking analysis such as AET can better inform both the design and policy negotiations that are necessary for the acceptable introduction of digital technologies in society.

By engaging in AET, a broad cross section of stakeholders—policymakers, designers, lawyers and citizens—can work towards more robust and ethically sound governance in at least three ways. First, by revealing the values and value judgements that unavoidably arise with the introduction of new technologies. Second, by articulating not only the hard but also the soft impacts of technologies, and weighing their desirability. And third, by bringing the future closer through foresight and future studies. Future technology policy debates should take all three into account. The anticipatory governance of emerging technologies provides the toolbox to tackle moral dilemmas and reveal what trustworthy and ethical technology means. Understanding these notions helps us to better understand ourselves and our relationships with technological artefacts, and as such should form the foundation of any desirable governance framework.

## References

- Bietti, E. (2020). From ethics washing to ethics bashing: A view on tech ethics from within moral philosophy. In Association for Computing Machinery, *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT\* '20)* (pp. 210–19). New York: ACM.
- Boenink, M., & Kudina, O. (2020). Values in responsible research and innovation: From entities to practices. *Journal of Responsible Innovation*, 7(3), 450–70.
- Brey, P. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13.
- Brey, P. (2017). Ethics of emerging technologies. In S. O. Hansson (ed.), *Methods for the Ethics of Technology* (pp. 175–192). London: Rowman and Littlefield International.
- European Commission. (2021). *The European Commission's priorities: 6 Commission priorities for 2019–24*. [https://ec.europa.eu/info/strategy/priorities-2019-2024\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024_en). Accessed 16 September 2021.
- Floridi, L. (2018). Soft ethics and the governance of the digital. *Philosophy & Technology*, 31(1), 1–8.

- Franssen, M., Lokhorst, G. J., & van de Poel, I. (2018). Philosophy of technology. In E. N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/archives/fall2018/entries/technology>. Accessed 16 September 2021.
- Green, B. (2021). The contestation of tech ethics: A sociotechnical approach to ethics and technology in action. *SSRN*. doi:10.2139.3859358.
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–99.
- Pitt, J. C. (2014). ‘Guns don’t kill, people kill’; Values in and/or around technologies. In P. Kroes & P. P. Verbeek (eds.), *The moral status of technical artefacts* (pp. 89–102). Philosophy of engineering and technology. Dordrecht: Springer.
- Snow, J. (2018). Amazon’s face recognition falsely matched 28 members of Congress with mugshots. *American Civil Liberties Union*, 26 July. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>. Accessed 16 September 2021.
- Swierstra, T. (2015). Identifying the normative challenges posed by technology’s ‘soft’ impacts. *Etikk i Praksis*, 9(1), 5–20.
- Swierstra, T., Stemerding, D., & Boenink, M. (2009). Exploring techno-moral change: The case of the obesity pill. In P. Sollie & M. Duwell (eds.), *Evaluating new technologies* (pp. 119–38). Dordrecht: Springer.
- Winner, L. (1980). Do artifacts have politics? *Daedalus*, 109(1), 121–36.

### Author biography



**Jana Mišić** is a PhD candidate in ethics and technology at the University of Twente and the Rathenau Institute, The Hague. She is also a Marie Skłodowska-Curie fellow within the PROTECT project. Her research focuses on ethical risk frameworks for algorithmic decision-making in the public sector.

# The ethical dimension of human–artificial intelligence collaboration

European View  
2021, Vol. 20(2) 182–190  
© The Author(s) 2021  
DOI: 10.1177/17816858211059249  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)  


**Michał Boni**

## Abstract

The development of artificial intelligence (AI) has accelerated the digital revolution and has had an enormous impact on all aspects of life. Work patterns are starting to change, and cooperation between humans and machines, currently humans and various forms of AI, is becoming crucial. There are advantages and some threats related to these new forms of human–AI collaboration. It is necessary to base this collaboration on ethical principles, ensuring the autonomy of humans over technology. This will create trust, which is indispensable for the fruitful use of AI. This requires an adequate regulatory framework: one that is future proof, anticipates how AI will develop, takes a risk-based approach and implements *ex ante* assessment as a tool to avoid unintended consequences. Furthermore, we need human oversight of the development of AI, supported by inter-institutional partnerships. But first we need to create the conditions for the development of AI digital literacy.

## Keywords

Artificial intelligence, Human–machine collaboration, Ethical AI, AI digital literacy, *Ex ante* assessment, Future-proof regulation

## Introduction

Human–machine collaboration is one of the key challenges of the digital age. The success of this cooperation will bring many advantages for both humans and technology. Modern machines that use artificial intelligence (AI) have the ability to be much better adjusted to humans’ needs, and consequently to work much more effectively. As a result,

---

### Corresponding author:

M. Boni, Wilfried Martens Centre for European Studies, 1st floor, 20 Rue du Commerce, Brussels, B-1000, Belgium.  
Email: [miboni54@gmail.com](mailto:miboni54@gmail.com)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

models of societal collaboration can be adjusted, leading to greater efficiency and productivity in many areas. Viewed from this perspective, the European public discourse on the role of AI is inspiring.

The many potential uses of AI systems mean that we can find new areas of collaboration, in which ‘trustworthy AI’ will allow humans to maintain control over the technology and build a healthy coexistence. According to the European Commission’s High-Level Expert Group on AI, ‘trustworthy AI’ refers to AI that is lawful (based on regulations), ethical (follows ethical principles) and robust (does no harm) (European Commission 2019). We can build either a coexistence between humans and AI in which humans do not have control and do not fully understand the principles of operation, or a coexistence based on conditions and principles that create trust.

One analysis of the role of AI in society highlights citizens’ views on the impact of AI (Funk et al. 2020). On average 53% of the population view AI as a good thing, while those who view it as a negative development constitute 33%. However, there are many differences in opinions between continents. These views also relate to opinions about the impact of robotics on job automation: according to Funk et al. (2020), ‘(a) median of 48% say such automation has mostly been a good thing, while 42% say it has been a bad thing’.

These opinions could be a reference point for public discussions about AI development and the potential opportunities for a new relationship between humans and machines. The aim of these discussions would be to minimise feelings of being at a disadvantage that those in a variety of roles may harbour. AI systems can and will affect everybody, everywhere, and this should be taken into account when working on the regulatory aspects of AI in the EU.

This article argues that human–machine/AI collaboration must be based on ethical principles. The expected framework for this is through management by law and, at the same time, management by oversight. The latter gives responsibility for the oversight of all AI development processes to partners (in a collaborative way), including science, business, public institutions and civic organisations, with the aim of encouraging innovation within rules that uphold fundamental and consumer rights. The solutions discussed and implemented in the EU can build future competitive advantages for the Union. In the subsequent sections, this article will review the key drivers of the discourse on the AI ecosystem, and highlight the problem of future-proofing legislation with guarantees of equilibrium between human autonomy and technological innovation. In addition, it will define AI digital literacy, describe the significance of *ex ante* impact assessments<sup>1</sup> in ensuring the ethical behaviour of AI functionalities and offer useful recommendations for policymaking in the area of AI development.

## The AI ecosystem discourse

It is important to note that work on AI development has been undertaken in a holistic manner, taking into account a wide variety of factors, including science and business

measures (i.e. creating an ecosystem of excellence) and trust building as an important social challenge. To establish an ecosystem of trust is a crucial challenge (European Commission 2020a; 2021a; 2021b; 2021c). This ecosystem should be focused on human values, rights, societal needs, aspirations and ensuring that AI works effectively for people. This theme is clearly presented in the annex to the Communication *Fostering a European Approach to Artificial Intelligence* (European Commission 2021b).

How then, can we make AI systems trustworthy and ensure that AI works with people and for people without having negative impacts and causing concern? Certain features are essential for fruitful collaboration between AI and humans, especially regarding the ethical development of AI.

First, AI is fundamental for the development of certain sectors and for their improved efficiency. AI systems have started to change, *inter alia*, the manufacturing and service industries, financial services, the workplace, social care, education, healthcare, security systems, management strategies, climate and environmental policies, administrative services, migration and asylum policies, agricultural policies and mobility solutions. In all these areas, a new model of relationship between humans and robots/AI is starting to be established. And the essential factor in this new relationship is *trust*. This is especially important with regard to the changing ways of working (e.g. new collaborative models, shift arrangements and job sharing, including between humans and robots/AI) with regard to the emotional aspects of work.

Second, it is necessary to understand what kind of regulatory framework will be most suitable for developing AI systems. In many areas, the traditional view is focused on a static regulatory framework (Evas 2020), which is sufficient to solve some problems of harm (e.g. mental, physical or material) potentially caused by humans (e.g. in car accidents, through violence against women and children etc.). Currently, a crucial debate is taking place on the responsibility of social media platform providers for the dissemination of illegal content and disinformation, and the phenomenon of hate speech which have arisen on social networks. In this case it is clear that we can use the universal norms incorporated into regulatory frameworks to indicate challenges and help people tackle problems. This also offers consumers redress mechanisms to allow space for the implementation of rights and to deliver remedies.

In many scientific and political debates in which the significance of AI as a game changer is strongly emphasised, the problem of the possible autonomy of AI is raised. This requires a different kind of response from the legislative side. One option, adaptation, would mean the adjustment of existing legal principles in order to apply them to the functioning of AI systems, as in the case of the EU's Machinery Directive (European Parliament and Council 2006; Tuominen and Festor 2021). The second option, anticipation, would mean that existing legal systems and new proposals need to be able to provide dynamic legal mechanisms to safeguard against new risks (Evas 2020). Future-proof solutions are necessary, and the only way to avoid unintended consequences is through *ex ante* impact assessments. There are currently some obligations regarding *ex post*

impact assessments, that is, those that are carried out after the introduction of new solutions (including technological ones)—for instance, in order to understand how new devices and functionalities are working, both in terms of being in accord with the legal framework and their influence on people. Including in the regulations the obligation to conduct *ex ante* impact assessments would be an innovation, but it would be a more effective way of eliminating certain threats.

Third, it is important to find a dynamic model for the regulatory framework for AI due to the dynamism of AI's developing functionalities. The concept of the 'risk pyramid' presented by the European Commission (2021a) is the best solution. For concretely high-risk AI systems, it would establish the requirement to fulfil all obligations of the conformity assessment before market entry. This would mean that all decisions assessing the level of possible threat to humans would use a 'risk-based approach', supported by evidence, not by intuition.

One of the key components from the ethical perspective is the model of the *ex ante* impact assessment. It should be based on full respect for human autonomy: dignity and agency are unique attributes of human beings, and form the foundation of human rights. In this respect, it must be noted that 'to manage and decide about humans in the way we manage and decide about objects or data, even if this is technically conceivable' would be inappropriate (European Group on Ethics in Science and New Technologies 2018, 9). A key factor in the development of AI systems is, of course, data-related: the quantity that is available as well as the quality of it. The normative assumption ought to be clear: humans should not be reduced to the data dimension.

Fourth, it is important to defend human autonomy by establishing that the actions of AI systems can only be based on principles which guarantee respect for fundamental and consumer rights, and by having a transparent discussion about the anticipation of AI systems development and innovation in maintaining values. We need to define all examples of potential breaches of ethical principles. There are many possible threats to human autonomy that could have adverse impacts on a plurality of people, in all kinds of applications (European Commission 2021a; 2021d)—the use of AI that embodies these threats is considered 'high risk' and some types of AI are banned in the European Commission's AI regulation proposal. These include, *inter alia*, the use of autonomous weapons, the presence of AI systems in the management of critical infrastructure, the use of AI to automate certain decision-making processes (e.g. the allocation of social benefits and loans), mass surveillance technologies and the use of AI in law enforcement (Dumbrava 2021).

A lack of ethical principles could undermine the relationship between humans and AI. All the reviewed cases and AI uses clearly show an increased risk to citizens' fundamental rights and the potential for the violation of EU values; threats to human dignity and the violation of personal autonomy; concerns over a reduction in privacy protection despite the existence of the EU's General Data Protection Regulation; the visible growth of discriminatory outcomes led by algorithms; and the operation of 'black box' models

which do not use explainable mechanisms. These examples show the unbalanced relationship between humans and AI.

Fortunately, the European Commission's proposal on AI regulation, which would establish the risk pyramid concept and conformity assessment procedures, aims to minimise some risks and limit some dangerous solutions. The minimal transparency obligations for non-high-risk AI systems presented in the proposal is very valuable. The proposal offers a proper response to the need for an equilibrium between the threats and advantages of AI, based on transparent rules and common principles, and translated into technical and business models for the functioning of AI.

## **AI digital literacy and awareness**

The above-mentioned 'equilibrium' also means creating sustainability for both sides: human and machine/AI. The human side relates to reality and potentiality. Humans have many fears about the unknown world of technology and AI. What is unknown is uncertain, and this uncertainty leads to insecurity. How can we change these negative feelings?

The answer became clear during consultations in 2020 (European Commission 2020c): 90% of respondents indicated that improving skills would be the most important action to prepare people to use AI in a better way (the adoption of a training programme was crucial for 86% of respondents). Stakeholders, especially business actors, also raised the issue of AI digital literacy (Digital Europe 2020), which should be integrated in a comprehensive way into all educational formats (building the potential for adaptability).

In addition, when raising awareness of AI, it is important to know as much as possible about the impact of AI on human psychology and behaviour. In some professions there is the possibility of challenging problems, such as emotional attachments to robots, the loss of the ability to think for yourself and to be introspective, the danger of deception and manipulation, the risk of becoming psychologically dependent on robots, and the unpredictability of forming human–robot/AI relationships, which could lead to violent behaviour under the informal, 'intimate' pressure of the AI device, especially in humanoid form. Yet, there are also opportunities: interactions between humans and AI can change human-to-human interaction models and improve the collaborative competences of humans in relation to other humans through the supportive oversight of AI. Knowledge of these problems and advantages, coming from understanding the new opportunities of AI systems development, should form part of AI digital literacy.

## **Ex ante impact assessments**

In establishing trustworthy human–machine collaboration, we have to emphasise the importance of 'soft' instruments. These will be crucial not only for the better adaptability of humans to the increasing presence of machines, but also for the machine/AI side as a

way to adjust to users' needs and expectations. This means that the architects, developers and deployers of AI solutions need to integrate new technologies into their work to guarantee an acceptable standard of operation that is in line with ethical principles.

A significant component of avoiding breaches of fundamental rights and discriminatory solutions is linked to the quality of the datasets which are generated using the power of AI. Using faulty or badly compiled data for algorithmic work can create a significant risk of discrimination, whether intended or unintended. The data training volumes held by developers can include unintended social bias, which is then reproduced and automatically reinforced by AI systems. On the one hand, the response to this should focus on applying proper standards to the data selection used for AI training. On the other, there is a need to establish European guidelines for data usage, which is likely to be the subject of the Data Governance Act (European Commission 2020b) and the Data Act expected in late 2021. How users can be given some tools to control their own data is an additional factor for consideration.

Checking the quality of the datasets used for AI training is fundamental to ensuring its appropriateness: the reference data of all high-risk AI systems must be checked for conformity with fundamental rights, privacy protection and ethical values. The obligation to do this should be placed on both the providers (to ensure compliance with AI requirements, registration, quality and risk management, post-market monitoring and reporting to competent authorities) and the users (human oversight, documentation, completion of a Data Protection Impact Assessment) of high-risk AI systems (European Commission 2021d, 53–4).

During consultations on the European Commission's 2020 AI White Paper, it was agreed to focus on self-assessed *ex ante* analysis and conformity assessments carried out by the developer. To ensure the trustworthiness of AI, various impact assessment models were discussed. One of the key proposals is the introduction of a Human Rights Impact Assessment, which should be carried out and documented (Panoptikon Foundation 2020, 4) for all AI systems as a mandatory solution, as proposed by many civil society and consumer organisations. This assessment regime should introduce a mandatory disclosure scheme, describe the role and tasks for external reviewers (an external report should be required), and increase real engagement from those affected (communities, individuals and civil society groups).

This model of compliance would be very resource-heavy, both for companies and public authorities. Additional proposals were also brought to the table. In cooperation with the European Parliament, several scientists (Van Wyngsberghe, 2020) presented on the need for the implementation of an ethical Technology Assessment and the concept of Data Hygiene Certification.

The requirement for *ex ante* procedures in the European Commission's proposal are paramount to the whole process of the conformity assessment. The more companies and

people become involved in *ex ante* measures, the more trust will become the fundament of human–AI collaboration.

## Conclusion

It should be clear that to ensure future human–AI collaboration and to make solutions much more visible and oriented towards building trust, we have to find the best instruments for AI management. Some of these should come from the formulation of management by law. However, some should be created as a new tool, that is, management by oversight, constructed and used practically and institutionally by all partners (Boni 2021). In addition is also important to check and support the credibility of the institutions responsible for the evaluation of conformity assessments, registration systems and *ex post* market surveillance, especially at the national levels—wherein will lie the enforcement and supervision of the new rules.

However, the overall objective is to achieve transparent conditions for the human oversight of AI mechanisms and functionalities as the key to future fruitful collaboration between humans and machines, and also human–machine/AI teaming. Such conditions need to be adaptable to new challenges and kept as a constant foundation for the benefit of the humans who will play many roles *vis-à-vis* AI systems opportunities. These humans will include doctors, who will work in cooperation with AI on personalised diagnosis and therapies; officers in public institutions developing automated decision-making processes for public services (including in terms of the scoring of people, with the risk of discriminatory actions); and city managers, who will use AI systems to make security solutions much more effective in many areas without breaching residents' rights.

In this sense, some policies are needed at the EU level. They should ensure that fragmented solutions (separate national models) are avoided; create a holistic view of AI development (supplemented by data governance); and build future-proof regulations to make European AI growth a reference point (in terms of norms and standards) in transatlantic cooperation. To achieve the best oversight, EU policies should bring together the efforts of all stakeholders (from business, science, civil society and European institutions). At the same time action is needed to build the educational capacity of the workforce and improve AI digital literacy in all societies, and financial investment (both public and private) is needed to develop AI functionalities. Moreover, promotion of AI will be indispensable during the process of implementing the new regulations, especially to convince small and medium-sized enterprises to use all the possibilities AI offers. Finally, political will is going to be needed to bring all debates to an effective conclusion and begin implementation of the new rules. Implementation should be monitored since it will open up opportunities for further current uses and reveal future challenges.

## Note

1. In the EU context, *ex ante* impact assessment refers to 'an attempt to provide, in advance of legislating, a coherent analysis of the reasoning that lies behind, and the foreseeable effects of, any proposed measure or policy initiative' (Dunne and Eisele 2020).

## References

- Bird, E., Fox-Shelley, J., Jenner, N., Leveloy, R., Weikkamp, E., & Winfield, A. (2020b). *The ethics of artificial intelligence: Issues and initiatives*. European Parliamentary Research Service, PE 634.452. March. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS\\_STU\(2020\)634452\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf). Accessed 6 September 2021.
- Boni, M. (2021). *Artificial intelligence and governance: Going beyond ethics*. Wilfried Martens Centre for European Studies. Brussels. <https://www.martenscentre.eu/publication/artificial-intelligence-and-governance-going-beyond-ethics/>. Accessed 6 September 2021.
- Digital Europe. (2020). *Digital Europe comments on the European Commission's AI White Paper*. 12 June. <https://www.digitaleurope.org/wp/wp-content/uploads/2020/06/DIGITALEUROPEs-response-to-the-AI-White-Paper-consultation.pdf>. Accessed 6 September 2021.
- Dumbrava, C. (2021). *Artificial intelligence at EU borders: Overview of applications and key issues*. European Parliamentary Research Service, PE 690.706. July. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS\\_IDA\(2021\)690706\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf). Accessed 6 September 2021.
- Dunne, J., & Eisele, K. (2020). *Ex-ante impact assessment in the EU*. European Parliamentary Research Service, 13 May. <https://epthinktank.eu/2020/05/13/ex-ante-impact-assessment-in-the-eu-2/>. Accessed 6 October 2021.
- European Commission. (2019). Ethics guidelines for trustworthy AI. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Accessed 6 September 2021.
- European Commission. (2020a). *Artificial intelligence: A European approach to excellence and trust*. White Paper. COM (2020) 65 final, 19 February. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065&from=EN>. Accessed 6 September 2021.
- European Commission. (2020b). Proposal for a Regulation on European data governance (Data Governance Act). COM (2020) 767 final, 25 November. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>. Accessed 6 September 2021.
- European Commission. (2020c). *Public consultation on the AI White Paper – Final report*. 30 November. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=68462](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68462). Accessed 6 September 2021.
- European Commission. (2021a). *Annexes to the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. COM (2021) 206 final, 21 April. [https://ec.europa.eu/transparency/documents-register/api/files/COM\(2021\)206\\_1/de00000000993583?rendition=false](https://ec.europa.eu/transparency/documents-register/api/files/COM(2021)206_1/de00000000993583?rendition=false). Accessed 6 September 2021.
- European Commission. (2021b). *Fostering a European approach to artificial intelligence*. Communication. COM (2021) 205 final, 21 April. <https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=COM:2021:205:FIN>. Accessed 6 September 2021.
- European Commission. (2021c). *Impact assessment accompanying the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Staff Working Document. SWD (2021) 84 final, 21 April. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2021:84:FIN>. Accessed 6 September 2021.
- European Commission. (2021d). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM (2021) 206 final, 21 April. [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2021\)206&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=en). Accessed 6 September 2021.

- European Group on Ethics in Science and New Technologies. (2018). *Statement on artificial intelligence, robotics and 'autonomous' systems*. 9 March. <https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1>. Accessed 6 September 2021.
- European Parliament and Council. (2006). Directive 2006/42/EC on machinery, and amending Directive 95/16/EC (recast). OJ L157 (9 June), 24. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0042>. Accessed 6 September 2021.
- Evas, T. (2020). *European framework on ethical aspects of artificial intelligence, robotics and related technologies: European added value assessment*. European Parliamentary Research Service, PE 654.179. September. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS\\_STU\(2020\)654179\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf). Accessed 6 September 2021.
- Funk, C., Tyson, A., Kennedy, B., & Johnson, C. (2020). Science and scientists held in high esteem across global publics. *Pew Research Center*, 29 September. <https://www.pewresearch.org/science/2020/09/29/science-and-scientists-held-in-high-esteem-across-global-publics/>. Accessed 6 September 2021.
- Panoptykon Foundation. (2020). *Panoptykon Foundation's submission to the consultation on the 'White Paper on artificial intelligence – a European approach to excellence and trust'*. Warsaw, 10 June. [https://panoptykon.org/sites/default/files/stanowiska/panoptykon\\_ai\\_whitepaper\\_submission\\_10.06.2010\\_final.pdf](https://panoptykon.org/sites/default/files/stanowiska/panoptykon_ai_whitepaper_submission_10.06.2010_final.pdf). Accessed 6 September 2021.
- Tuominen, M., & Festor, S. (2021). *Revising the Machinery Directive*. European Parliamentary Research Service, PE 694.208. July. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694208/EPRS\\_BRI\(2021\)694208\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694208/EPRS_BRI(2021)694208_EN.pdf). Accessed 6 September 2021.
- Van Wyngsberghe, A. (2020). *Artificial intelligence: From ethics to policy*. European Parliamentary Research Service, PE 641.507. June. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641507/EPRS\\_STU\(2020\)641507\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641507/EPRS_STU(2020)641507_EN.pdf). Accessed 6 September 2021.

## Author biography



**Michal Boni, PhD**, is a senior research associate at the Wilfried Martens Centre for European Studies and an assistant professor at the Warsaw University for Social Sciences and Humanities. He is a former Member of the European Parliament from Poland and a former Polish Minister of Administration and Digitisation.



# Back to Westminster: A new transatlantic agenda to defend democracy

European View  
2021, Vol. 20(2) 191–200  
© The Author(s) 2021  
DOI: 10.1177/17816858211053696  
journals.sagepub.com/home/euv



**Igor Merheim-Eyre**

## Abstract

Across the transatlantic area and, indeed, across the democratic world, democracy is under strain from domestic and external factors, while throughout the world, authoritarian and totalitarian forces continue to quash people's desire for freedom and human dignity. In this context, this article takes stock of the ongoing challenges, and argues for a renewed transatlantic agenda that returns to the spirit of President Ronald Reagan's 1982 Westminster Speech. It should achieve this by developing an ambitious programme that defends democracy within the transatlantic area and supports people's desire for freedom globally, while avoiding the dogmatic approaches and ossification that have characterised democracy promotion over the past two decades.

## Keywords

Democracy, Reagan, Westminster, West, Freedom

## Introduction

In 1982, at the height of the Cold War and the struggle between the Free World and Marxist totalitarianism, US President Ronald Reagan delivered a speech to the British Parliament during an official visit to Great Britain in which he outlined his vision for putting the Marxist dialectics in reverse, and supporting those who wished to live freely: 'The objective I propose is quite simple to state: to foster the infrastructure of democracy, the system of a free press, unions, political parties, universities, which allows a people to choose their own way to develop their own culture, to reconcile their own differences through peaceful means' (Reagan 1982).

---

## Corresponding author:

Igor Merheim-Eyre, School of Politics and IR, Rutherford College, University of Kent, Canterbury CT2 7NX, UK.

Email: merheim.eyre@gmail.com



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

The context in which President Reagan delivered his remarks was hardly favourable to such an endeavour. The country he was visiting was battling high inflation and unemployment at home, and Argentine forces in the South Atlantic; Islamic revolutionaries had overthrown the Shah of Iran three years earlier; the Sandinistas had taken over Nicaragua; Cuban troops were engaged in Angola; and the Solidarity movement was battling the dark days of martial law in Poland. Moreover, the Soviet empire, though economically in decline, was dominating Central and Eastern Europe, and spreading its influence from Afghanistan to Latin America.

Yet as British Prime Minister Margaret Thatcher (1993, 258) noted, ‘the speech itself was a remarkable one’. According to her,

It marked a decisive stage in the battle of ideas which he and I wished to wage against socialism, above all socialism of the Soviet Union. Both of us were convinced that strong defence was a necessary, but not sufficient, means of overcoming the communist threat. Instead of seeking merely to contain communism, which had been the West’s doctrine in the past, we wished to put freedom on the offensive. (Thatcher 1993, 258)

Contrary to some misconceptions, this call to arms was not liberal internationalist in character but reflected a profoundly conservative outlook. It aimed to defend a historically proven social order, and traditions and institutions including peace, freedom, law, civility, public spirit, the security of property and family life. It was cautious about the pace of change, supported civil society against the totality of power and top-down interference, and indulged people’s *oikophilia*, that is, their inclination to cherish their home, family or nation.

Today, across the transatlantic area and, indeed, across the democratic world, democracy is under strain from domestic and external factors, while the desire for freedom and human dignity felt by people throughout the world continues to be quashed by authoritarian and totalitarian forces. In this context, this article takes stock of the ongoing challenges and argues for a renewed transatlantic agenda that returns to the spirit of the Westminster Speech. It should achieve this by developing an ambitious programme that defends democracy within the transatlantic area and supports people’s desire for freedom globally, while avoiding the dogmatic approaches and ossification that have characterised democracy promotion over the past two decades.

Just as in 1982, not simply defending but also supporting democracy around the world may seem overly ambitious. Indeed, it is. It is even more so at a time when the Free World lacks the leadership, moral guidance and vision of individuals such as Ronald Reagan, Margaret Thatcher or Pope John Paul II. Nevertheless, as this article argues, such ambitions are also necessary when our own democratic societies are under assault both from within and from outside. As US Senator Marco Rubio (2021) recently warned, we may soon ‘live to see a future in which the world’s most powerful nation is a totalitarian genocidal Communist dictatorship.’ To defend democracy, and to see it flourish worldwide, a transatlantic agenda is necessary because the transatlantic space still

remains the bedrock of the Free World, capable of bringing democratic states across the world together in a commonwealth.

## Defending democracy

As the Centre for Historical Analysis and Conflict Research (2016, 3), a think tank of the British Army, soberly concluded: ‘At a national level, and without being overly alarmist, we should also start the process of preparing society for an era of confrontation that perhaps presents the greatest risk to our security and prosperity since the end of the Cold War.’

From the macro to the micro-level, the world order as we know it (or, perhaps, as we imagine it) is in flux. The term world order is often used to characterise the existing balance of power, hierarchy and ‘rules of the game’ underpinning world politics. However, what is and what constitutes such an order is contested (Merheim-Eyre 2019b, 27). According to Malcolm Chalmers (2019), this order is composed of three systems:

1. A universal security system that is embodied by the UN charter, and includes the right to self-determination, the inviolability of borders and so on.
2. A universal economic system that includes a set of international agreements and institutions such as the International Monetary Fund and the WTO. This also includes regimes to address climate change and global diseases. Its membership has grown over time to be almost universal.
3. A Western system, that is, a more exclusive community of shared political, economic and security interests in North America, Europe and the Asia-Pacific region.

As Chalmers (2019, 4) further notes, major power relations, such as the bloc system and the mutually agreed spheres of influence during the Cold War, exist independently but also have the ability to shape the three systems. Furthermore, for the English School of International Relations, and the late British international relations theorist Hedley Bull in particular, an order presupposes at least some degree of social relations, and acceptance (however minimal) of a set of shared rules and practices, such as the inviolability of borders between states. Bull sees institutions such as the balance of power, international law, diplomacy, war and major powers as essential to producing order in the international system (including the universal security system and, to some extent, the universal economic system). Of the international system, Trine Flockhart (2016, 17) argues, that it ‘is likely to have some social attributes that are likely to be similar to those in an international society’. An international society, or a society of states, however, bears more resemblance to the Western system, which ‘exists when a group of states, conscious of certain common interests and common values, form a society in the sense that they conceive themselves to be bound by a common set of rules in their relations with one another, and share in the working of common institutions’ (Flockhart 2016, 17).

Indeed, it is these various systems, including the Western system, that are increasingly being challenged. For decades, the engagement of democracies within and beyond the Western system was based on two assumptions. The first was that growing interdependence between states and the modernisation of developing countries would bring about the economic and political transformation of countries outside the Western system (that is, by them being increasingly absorbed into the Western system, which was becoming confused with the universal system). The second was that it would create a more stable world order, and perhaps even lead to the disappearance of international anarchy.

Such was the premise even before the end of the Cold War, and the popularity of this idea accelerated after its end with the hope that once-totalitarian states might one day even become 'like us'. Today, the West faces a harsh reality. While Western democracies assumed that they were shaping far-flung parts of the world in their own image, they failed to notice that, instead of conforming to the Western model, some regimes have become increasingly oppressive and even totalitarian at home, while seeking to corrupt, weaken or even transform the three systems to suit their own interests.

For example, Vladimir Putin's Russia has become increasingly repressive at home, while perceiving itself to be in a war with the West. It accuses the latter of waging hybrid warfare against Russia, namely through democracy-support programmes for civil society, the free media and democratic opposition, and through what the Kremlin perceives as Western-orchestrated 'colour revolutions' in Russia's neighbourhood (McDermott 2016). Externally, Russia has been prepared to undermine the universal security system (as witnessed by its annexation of Crimea and waging of an undeclared war in eastern Ukraine), and to weaken and corrupt the Western system. It has increasingly been playing the role of a spoiler, and an unpredictable and reactionary power that preys on adversaries' weaknesses (see below).

The Chinese Communist Party (CCP), on the other hand, is seeking to rewrite international norms (Richardson 2020). Furthermore, both the Kremlin and the CCP are exploiting the universal economic system and the Western system. The CCP achieves this in a variety of ways. For instance, the totalitarian regime in Beijing is using companies such as Huawei to build telecommunications networks globally that can give it a capability to disrupt communications and de facto spy on our citizens (Cerulus and Heikkila 2020). Furthermore, the Chinese economic system continues to be incompatible with WTO norms (Shea 2021), meaning that while it continues to benefit from the economic system, it does not offer the same level of openness to its own market. Finally, its companies continue to engage in widespread intellectual property theft, costing the US alone an estimated \$50bn annually (US, Office of the United States Trade Representative 2018), while using foreign investments and acquisitions to upgrade its domestic industries, ultimately, to degrade, reduce or replace Western competition in key sectors. If such actions are not addressed by Western countries, they will have an increasing impact on jobs and thus the very fabric of Western societies.

Meanwhile, Russian oligarchs and those friendly with the Kremlin launder dirty money through the City of London and other financial centres (Galeotti 2017). This exploitation has highlighted that, rather than the positive socialisation which Western pundits hoped would transfer the Western rules-based order to Russia, China and beyond, we have instead witnessed the corruption of the universal economic system and the Western system, and the undermining of the universal security system.

Unlike the CCP, the Kremlin does not have a predetermined strategy (Galeotti 2019, 15). Rather, according to Schaub Jr et al., the Russian form of hybrid warfare that has been waged against Western democracies in recent years seeks to undermine their resilience by ‘exploiting social, economic and political weaknesses’ in order to ‘produce instability that undermines social cohesion and exacerbates tensions . . . [and] reduce the ability of the target state to govern effectively or respond quickly and effectively in crises while avoiding clear and overt involvement’ (Schaub Jr et al. 2017, 33).

In some respects, Western democracies have been pushing back against these efforts from their adversaries. For example, the core US democracy-support institutes, including the International Republican Institute, have been leading responses to address disinformation and other hybrid tools by building up the capabilities of civil society and government institutions in Central and Eastern Europe (Merheim-Eyre 2019a; 2019c), while the Inter-Parliamentary Alliance on China has brought together parliamentarians from across the democratic world to address the CCP’s growing assertiveness. In a sign that the transatlantic community is also prepared to respond to the growing number of cyber-attacks from state and non-state actors, both the US and the EU have recently imposed targeted sanctions on the Russian officials identified as responsible for the operations. This was a particular milestone for the EU, whose member states remain divided on key issues of engagement with Russia, China and other authoritarian regimes. Furthermore, there is also the US-driven Clean Network initiative and the EU’s 5G Clean Toolbox, both of which seek to foster the development of safe 5G networks, while the US has been leading the way in protecting Western companies, for instance through the bi-partisan Protecting American Intellectual Property Act, which seeks to mandate sanctions on individuals and firms found to engage in, benefit from or enable intellectual property theft (US 2021).

While this may sound like a list of disparate measures, it rather highlights the scale of the challenges and vulnerabilities that Western democracies need to address. The openness of the Western system and globalisation, which for a long time was only seen in beneficial terms, have increasingly come to be manipulated by authoritarian regimes, with our societies, institutions, infrastructure and the economy increasingly being targeted.

But defending democracy goes beyond preventive measures. It requires a deeper political dialogue that is crucial to address many of the vulnerabilities facing Western democracies. Internally, for example, the Western system is being challenged by socio-economic tensions caused by globalisation, which are resulting in political discontent with the status quo (see Goodhart 2017). This, in turn, is being exacerbated by a form of progressivist ‘hyper-liberalism’, which claims universality and forces conformity with

its intellectual orthodoxy (Gray 2018), and populist forces which seek to challenge it (Mudde 2017).

Addressing such social fissures, and rebuilding social cohesion (especially while attempts to deepen divisions from both within and outside continue) will not be an easy task. Above all, it will require resolute leadership at a time when, from Berlin to Washington, DC, Western leaders are continuing to approach the defence of democracy timidly at best. Yet if the spirit of the Westminister Speech means anything, it is the ability of free societies to overcome their difficulties and to take freedom on the offensive. As Edward Lucas (2021) recently wrote:

But we can also choose to win. That is what Western leaders such as Margaret Thatcher, the two Helmut (Schmidt and Kohl), Ronald Reagan, and that wily Vatican brainbox knew. They took hard decisions and expressed their views with blazing moral clarity. The vast edifice of Soviet communism, based on fragile foundations of lies and fear, could not compete and crumpled.

## **Supporting freedom and democracy worldwide**

Going on the offensive to promote freedom and democracy creates many ontological questions about democracy support. As noted earlier, President Reagan's vision of democracy support was not a liberal internationalist call to arms, but a profoundly conservative one. Thus, while both conservatives and liberals/progressives can agree on the importance of supporting those wishing to be free, the latter tend to have a more rationalist view of human nature and a more optimistic view of societal 'progress' through modernisation. Conservatives, by nature, tend to have a sceptical or, at the very least, a more cautious perception of human nature with all its contradictions (Merheim-Eyre 2020).

For this reason, supporting freedom and democracy worldwide must also take into account the pace of change. President Reagan (1982) in his Westminister Speech noted that 'we must be staunch in our conviction that freedom is not the sole prerogative of a lucky few, but the inalienable and universal right of all human beings'. However, he also cautioned against 'forcing the pace of change' (Reagan 1982). Jeanne Kirkpatrick, who served both on Reagan's National Security Council and as the US ambassador to the UN, also made this point: 'Hurried efforts to force complex and unfamiliar political practices on societies lacking the requisite political culture, tradition, and social structures not only fail to produce desired outcomes; if they are undertaken at a time when the traditional regime is under attack, they actually facilitate the job of the insurgents' (Kirkpatrick 1979).

Thus, while the thirst for freedom is a natural instinct, building, and indeed sustaining, democracy is not easy. Kirkpatrick notes the long and bumpy process it took in Britain to build a parliamentary democracy, let alone the difficult and bloody process in France. We can observe these same difficulties today in Central and Eastern Europe (a region often held up as an example of successful democratic transition), where the desire for freedom in 1989 led to the end of the Soviet empire, but also where 40 years of totalitarian rule

and the destruction of civic associations by the Communists continues to impact democratic governance.

This is also directly related to the question of how the democracy-support agenda should look. As Jakub Grygiel pointed out, the question of promoting our ‘values’ is a problematic one because, though we may all be able to name those values, we disagree on the substance, such as on ‘questions of life, marriage and death’ (Grygiel 2019). Grygiel further notes that we should not ‘confuse our respect for life and love of liberty with “progressive values”, which are not universally appealing and whose infinite and elastic meaning defined by individual preferences weaken our reputation and undermine our national security’ (Grygiel 2019).

Supporting those living under authoritarian or totalitarian rule by providing access to free media; providing technical assistance, as was the case with Solidarity in the 1980s; giving moral support to the oppressed; or imposing costs on those engaging in or enabling human rights abuses through Magnitsky Act-style sanctions or other mechanisms, should and must continue to be our priority. However, a progressivist understanding of values and what the philosopher John Gray (2019) calls an expanding ‘illiberal empire of rights’ has, in recent years, made its way into the democracy-support programmes of the US, the EU and some of its member states. This is problematic not only because of our differing views on the substance of these values, but because questions about what constitutes family or when life begins or ends must fundamentally be part of a domestic democratic process and compromise among citizens. Pushing dogmas without sensitivity for the given society can lead to discontent, divisions and even the delegitimation of our efforts (however genuinely intended). President Reagan (1982) too, argued that supporting freedom and democracy is not about ‘cultural imperialism’, but about ‘providing the means for genuine self-determination and protection for diversity.’

The problem, as former President of the US National Endowment for Democracy (NED) Carl Gershman (2019) noted, is not only that the expansion of democracy-support programmes has led to increasing bureaucratisation, but that programmes are often driven more by the priorities of the donors rather than by those of the people whom they seek to support. Also, though top-down programmes to support the building or reform of public institutions is important, especially in formerly authoritarian or totalitarian countries, there is a fundamental need to strengthen bottom-up programmes, such as those supported by both the NED and the European Endowment for Democracy.

A bottom-up approach to democracy support is crucial for sustainability, not least because a vibrant civic and civil society not only holds the state institutions to account, but is also fundamental to resisting any attempts by the state to curb civil liberties—which is one of the main reasons why they are the first target of any authoritarian or totalitarian regime seeking to impose itself. In this respect, it is important that donors do not simply rely on the large professional non-governmental organisations whose reach is often limited to the bigger cities (and which are often confused with ‘civil society’), but also support smaller local initiatives beyond the major cities. Although bottom-up

programmes such as those of the European Endowment for Democracy and the NED tend to be more successful in this regard, larger donors such as the European Commission ought to step up re-granting. This would ensure the greater and more active participation of civic and civil society, which is crucial for building thriving democracies and ensuring that people exercise their freedoms.

## Conclusion

This article has sought to argue for a transatlantic agenda that returns to the spirit of President Ronald Reagan's 1982 Westminster Speech by developing an ambitious programme that defends democracy across the transatlantic area and supports people's desire for freedom globally, while avoiding the dogmatic approaches and ossification that have characterised democracy promotion over the past two decades.

To defend democracy, and to see it flourish worldwide, a transatlantic agenda is necessary because the transatlantic space remains the bedrock of the Free World, capable of bringing democratic states across the world together in a commonwealth. As such, common approaches, such as the recent coordination on sanctions against the CCP officials responsible for human rights abuses in Xinjiang (Lau 2021), are an important step in the transatlantic community's working together to stand with the oppressed against a cruel totalitarian regime.

The article has presented a long list of disparate measures, highlighting the scale of the vulnerabilities and challenges that Western democracies need to address, whether it be cleaning up our communications networks, supporting value chains, protecting businesses and people's livelihoods, fighting kleptocracy and disinformation, or addressing our social fissures.

Such tasks may sound daunting and, at a time when Western democracies seem to be facing a crisis of confidence, perhaps even illusory. Yet if anyone can overcome them it is, as Ronald Reagan (1982) believed, 'free people, worthy of freedom and determined not only to remain so but to help others gain their freedom as well.'

## References

- Centre for Historical Analysis and Conflict Research. (2016). *Is it time to wake up and smell the vodka?* London.
- Cerulus, L., & Heikkila, M. (2020). EU lawmakers brand Huawei, ZTE 'high risk' 5G vendors. *Politico*, 14 October. <https://www.politico.eu/article/meps-call-for-stop-to-public-funding-for-china-telecoms-huawei-zte/>. Accessed 6 September 2021.
- Chalmers, M. (2019). *Which rules? Why there is no single 'rules-based' international system*. Royal United Services Institute, Occasional Paper. London, April. [https://static.rusi.org/201905\\_op\\_which\\_rules\\_why\\_there\\_is\\_no\\_single\\_rules\\_based\\_international\\_system\\_web.pdf](https://static.rusi.org/201905_op_which_rules_why_there_is_no_single_rules_based_international_system_web.pdf). Accessed 17 September 2021.
- Flockhart, T. (2016). The coming multi-order world. *Contemporary Security Policy*, 37(1), 3–30.
- Galeotti, M. (2017). *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*. European Council on Foreign Relations. London.

- Galeotti, M. (2019). *We need to talk about Putin: How the West get him wrong*. London: Penguin Books.
- Gershman, C. (2019). The enduring power of Reagan's Westminister speech. Ronald Reagan Institute. [https://www.reaganfoundation.org/media/355165/gershman\\_westminster.pdf](https://www.reaganfoundation.org/media/355165/gershman_westminster.pdf). Accessed 20 August 2021.
- Goodhart, D. (2017). *The road to somewhere: The populist revolt and the future of politics*. London: C Hurst & Co.
- Gray, J. (2018). The problem of hyper-liberalism. *The Times Literary Review*, 30 March. <https://www.the-tls.co.uk/articles/john-gray-hyper-liberalism-liberty/>. Accessed 17 July 2021.
- Gray, J. (2019). Our Illiberal Empire of Rights. *UnHerd*, 26 June. <https://unherd.com/2019/06/our-illiberal-empire-of-rights/>. Accessed 24 August 2021.
- Grygiel, J. (2019). Democracy and authoritarianism: How should values matter in foreign policy: A response from Jakub Grygiel. *Reagan Foundation*. <https://www.reaganfoundation.org/reagan-institute/publications/democracy-and-authoritarianism-how-should-values-matter-in-foreign-policy-a-response-from-jakub-grygiel/>. Accessed 27 August 2021.
- Kirkpatrick, J. (1979). Dictatorships and double standards. *Commentary*, November. <https://www.commentary.org/articles/jeane-kirkpatrick/dictatorships-double-standards/>. Accessed 22 July 2021.
- Lau, S. (2021). UK, US, Canada follow EU sanctions on China officials. *Politico*, 22 March. <https://www.politico.eu/article/uk-us-canada-follow-eu-sanctions-on-china-officials/>. Accessed 22 August 2021.
- Lucas, E. (2021). Phoenix rising. *The Centre for European Policy Analysis*, 16 August. <https://cepa.org/phoenix-rising/>. Accessed 1 September 2021.
- McDermott, R. (2016). Does Russia have a Gerasimov Doctrine? *Parameters*, 46(1), 97–105.
- Merheim-Eyre, I. (2019a). Developing an EU-wide response to disinformation. *International Republican Institute*, 13 March. <https://www.democracyspeaks.org/blog/developing-eu-wide-response-disinformation>. Accessed 22 July 2021.
- Merheim-Eyre, I. (2019b). The West–Russia confrontation and limits to cooperative world order. In P. Kalra & E. van Gils (eds.), *Governance & resilience in wider Eurasia: Are cooperative orders possible?* COMPASS GCRF Conference Proceedings. Canterbury, UK, September. <https://www.kent.ac.uk/politics/rs-grcf-compass/COMPASS-Signature-Conference-Proceedings-2019-Updated-4-Oct-2019.pdf>. Accessed 17 September 2021.
- Merheim-Eyre, I. (2019c). US (and other powers) woo Central and Eastern Europe: A new centre of gravity? *RUSI Newsbrief*, 20 September. <https://rusi.org/publication/rusi-newsbrief/us-and-other-powers-woo-central-and-eastern-europe-new-centre-gravity>. Accessed 22 July 2021.
- Merheim-Eyre, I. (2020). Coronavirus, resilience, and the limits of rationalist universalism. *E-International Relations*, 21 April. <https://www.e-ir.info/2020/04/21/coronavirus-resilience-and-the-limits-of-rationalist-universalism/>. Accessed 20 August 2021.
- Mudde, C. (2017). Populism isn't dead: Here are 5 things you need to know about it. *The Guardian*, 7 July. <https://www.theguardian.com/commentisfree/2017/jul/07/populism-dead-european-victories-centrists>. Accessed 2 September 2021.
- Reagan, R. (1982). 'Address to Members of the British Parliament'. Speech made in Westminster, London, 8 June 1982. *Ronald Reagan Presidential Library and Museum*. <https://www.reaganlibrary.gov/archives/speech/address-members-british-parliament>. Accessed 21 August 2021.
- Richardson, S. (2020). China's influence on the global human rights system. *The Brookings Institution*, September. <https://www.brookings.edu/research/chinas-influence-on-the-global-human-rights-system/>. Accessed 22 July 2021.

- Rubio, M. (2021). *Rubio outlines path forward for China bill*. 11 May. <https://www.rubio.senate.gov/public/index.cfm/2021/5/rubio-outlines-path-forward-for-china-bill>. Accessed 25 August 2021.
- Schaub, G., Jr, Murphy, M., & Hoffman, F. (2017). Hybrid maritime warfare: Building Baltic resilience. *RUSI Journal*, 162(1), 32–40.
- Shea, D. (2021). To meet the China challenge, the US and Europe must look beyond the WTO. *The Hill*, 21 February. <https://thehill.com/opinion/international/539732-to-meet-the-china-challenge-the-us-and-europe-must-look-beyond-the-wto>. Accessed 1 September 2021.
- Thatcher, M. (1993). *The Downing Street years*. London: HarperCollins.
- US. (2021). Protecting American Intellectual Property Act of 2021. *Congress.gov*, 21 April, S.1294. <https://www.congress.gov/bill/117th-congress/senate-bill/1294/titles?r=9&s=1>. Accessed 17 September 2021.
- US, Office of the United States Trade Representative. (2018). *Findings of the investigations into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under Section 301 of the Trade Act of 1974*. <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>. Accessed 24 July 2021.

### Author biography



**Igor Merheim-Eyre, PhD**, is a Research Fellow at the Global Europe Centre (University of Kent) and works in a policy advisory role in the European Parliament. His main areas of focus include transatlantic relations and wider European security.



# Authoritarian consolidation in Belarus: What role for the EU?

European View  
2021, Vol. 20(2) 201–210  
© The Author(s) 2021  
DOI: 10.1177/17816858211061839  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Giselle Bosse**

## Abstract

The aim of this article is to review the EU's relations with Belarus over recent decades; to examine the patterns, opportunities and limitations of the EU's policies vis-à-vis the authoritarian regime; and to evaluate the effectiveness of the EU's responses to the brutal crackdown on civil society and political opposition following the flawed presidential elections in August 2020. It is argued that, despite its careful balancing act between principled approach and pragmatic engagement, the EU's perception of the Belarusian regime has been overly optimistic and often influenced by the appeal of short-term geopolitical and economic gains. How should the EU deal with a consolidating and increasingly ruthless dictatorship at the heart of Europe? By way of conclusion, the article maps a number of 'lessons learned' and suggestions for future EU policy towards Belarus.

## Keywords

Belarus, EU, Sanctions, Human rights, Readmission agreement, Eastern Partnership

## Introduction

A totalitarian power is mainly busy in keeping itself alive.  
(Svetlana Alexievich, quoted in *Donadio* 2016)

Belarus has experienced months of protests and civic action against the state, sparked by blatant election fraud and severe violence by government forces. The brazen breach of democratic norms in a country positioned between the EU and the Russian Federation has outraged the West. As a result, in recent months the years of Belarusian reconciliation with the West following the annexation of Crimea in 2014 have been reversed.

---

### Corresponding author:

G. Bosse, Maastricht University, P.O. Box 616, 6200 MD Maastricht, The Netherlands.  
Email: [g.bosse@maastrichtuniversity.nl](mailto:g.bosse@maastrichtuniversity.nl)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

The aim of this article is to review the EU's relations with Belarus over recent decades; to examine the patterns, opportunities and limitations of the EU's policies vis-à-vis the authoritarian regime; and to evaluate the effectiveness of the EU's responses to the brutal crackdown on civil society and political opposition following the flawed presidential elections in August 2020. It is argued that, despite its careful balancing act between principled approach and pragmatic engagement, the EU's perception of the Belarusian regime has been overly optimistic and often influenced by the appeal of short-term geopolitical and economic gains. This has resulted in restrictive measures being lifted too soon and too much credit being given to the regime's spurious reassurances that it would improve the country's human rights record. Lukashenka's objective has always been to remain in power, leveraging rapprochement with the EU to obtain economic concessions from Russia, while only paying lip service to improving human rights and democracy in order to maintain authoritarian rule domestically.

### **EU–Belarus relations: the disengagement–rapprochement cycle**

The EU's ties with the Republic of Belarus have always been limited. In 1996–7, bilateral ties came to a halt owing to major setbacks in Belarus's democratic growth and protection of human rights. It was not until 2008 that the first attempt at normalising relations between the EU and Belarus was made. Following the release of political prisoners, the EU lifted sanctions on nearly all Belarusian authorities, and the country was allowed to join the Eastern Partnership programme. At the time, leading human rights experts found little evidence of improvements in human rights and democracy, which prompted several commentators to claim that the EU's engagement with Belarus was not motivated by human rights concerns (see, e.g. Bosse 2012). Rather, the motivation was the desire for closer ties with Belarus to 'reward' Lukashenka for his unwillingness to recognise the breakaway Georgian provinces of Abkhazia and South Ossetia during the 2008 Russo-Georgian war (Vieira 2014). With the harsh crackdown on opposition protesters during the presidential elections in December 2010, this brief period of normalisation came to an end. Following the start of the Ukraine crisis in 2014, efforts to normalise EU–Belarus ties were resumed. Minsk's largely impartial stance towards Ukraine, as well as its support for the country's territorial integrity, acted as the catalyst. By early 2015, the majority of the EU member states had agreed that the sanctions on Belarus should be removed after all of Belarus's remaining political prisoners had been freed and rehabilitated. Soon after, at the end of October 2015, the Council suspended nearly all restrictive measures against Belarus, before removing them entirely in February 2016. However, just as during the previous rapprochement in 2008, there was little concrete evidence that the human rights situation in Belarus had improved (Bosse and Vieira 2018). It then worsened significantly when opposition protests were crushed in the aftermath of the 2016 parliamentary elections and again when protests erupted in February and March of 2017 in response to the so-called parasite law (Presidential Decree no. 3).

Yet despite the deterioration of the human rights situation in the country, the EU continued its rapprochement with Belarus. More specialised bilateral dialogues, such as the

EU–Belarus Coordination Group, were launched in 2016 and continued, despite human rights activists urging the European External Action Service to postpone meetings (*Eastern Partnership Civil Society Forum* 2017). Since 2015 the EU and Belarus had also been engaged in the implementation of an informal roadmap of ‘measures to deepen the EU’s policy of critical engagement with Belarus’ (Political and Security Committee 2015), including the conclusion of a Mobility Partnership and negotiations on a Visa Facilitation and Readmission Agreement. These developments have been viewed very sceptically by Belarusian civil society and human rights organisations (Bosse 2017, 293–4). Mobility Partnerships prioritise cooperation on border control and illegal migration, and the Readmission Agreements that have been concluded with authoritarian countries have been very controversial, especially in view of the human rights violations committed by border guards and the police (Amnesty International 2017).

### **Presidential elections in August 2020 and the brutal crackdown on protesters**

Hundreds of thousands of people have taken to the streets in Belarus to protest Alexander Lukashenka’s dictatorship since the presidential elections in August 2020. In response, the Belarusian regime has launched the most violent crackdown on human rights in the country’s post-independence history. Opposition candidates and their associates have been detained or forcibly exiled, Belarusian security forces have used excessive and indiscriminate force against protesters, thousands of peaceful protesters have been arrested, and authorities have systematically used torture and other ill-treatment against those detained. At least three peaceful protestors have died as a result of the use of force by the police (*Amnesty International* 2021a). Dozens of human rights groups and other civil society organisations have been closed arbitrarily, and many of their employees have been imprisoned as suspects in fabricated criminal cases or pushed into exile.

Two days after the flawed presidential elections in Belarus on 9 August, the EU’s High Representative for Foreign Affairs and Security Policy declared that the election had been ‘neither free nor fair’, deploring the ‘disproportionate and unacceptable violence’ (Council of the EU 2020a, 1). Throughout the month of August, however, the EU struggled to agree on sanctions against Belarus. Negotiations were blocked by Cyprus, which threatened to veto sanctions against Belarus to pressure the EU into imposing sanctions on Turkey over its gas drilling activities in the eastern Mediterranean. It took until 2 October for the EU to impose the first restrictive measures against Belarus, in the form of travel bans and asset freezes for individuals identified as responsible for the repression and intimidation of peaceful protesters, opposition members and journalists (Council of the EU 2020b, 2). On 12 October, the Council scaled down bilateral cooperation, financial assistance was recalibrated away from the Belarusian authorities, and the European Investment Bank and European Bank for Reconstruction and Development reviewed their operations in Belarus (Council of the EU 2020b, 4). Following the forced landing of a Ryanair flight in Minsk on 23 May 2021, and the detention by the Belarusian authorities of journalist Raman Pratasevich and his partner Sofia Sapega, the Council introduced targeted economic sanctions in June, including, *inter alia*, restrictions on

trade in petroleum products and potassium chloride (potash), restrictions on access to EU capital markets, and a stop on all European Investment Bank disbursements and payments (Council of the EU 2021).

## **Effect of the EU's restrictive measures and sanctions: a mixed picture**

Over recent decades, the effects of the EU's restrictive measures on Belarus have been ambiguous. On the one hand, the measures have made little difference to the authoritarian regime of Lukashenka, which has shown itself resilient to visa restrictions and the freezing of assets directed at top political officials and economic elites. Yet a qualitative difference can be observed in the manner in which the EU has imposed sanctions over the years. While many of the 'first generation' of restrictive measures against Belarusian business people and their companies have been annulled by the General Court of the EU (Lester and O'Kane 2021), the most recent restrictive measures have been designed more carefully in order to withstand potential legal challenges in court. The direct effects of the restrictive measures on the economic and financial activities of Belarusian companies linked to or close to the Lukashenka regime have been mixed as well. Several of the sectors targeted, such as armaments companies, are mainly oriented towards the Russian market, and also export to Asian and African markets, and therefore have not been particularly affected. However, some companies, including the Serbian Dana Holding, which fed into private presidential funds, are said to have started to withdraw from Belarus; several business people about to be targeted by sanctions have transferred their stakes in companies to relatives or close collaborators; and some of the sanctioned companies have reported problems with the supply of components from Western business partners (Kłysiński 2021).

With regard to the effects of the targeted economic sanctions, the picture is also mixed. The EU's ban on potash imports from and transiting through Belarus will have a rather limited impact on the exports of Belaruskali (the Belarusian potash company), because its main export product—potash with 60% potassium content—is not on the EU's list of sanctioned items (*Reuters* 2021b). As a result, only 20% of the potash exported via Lithuania is affected by the sanctions, and it is likely that Belarus will compensate for these losses by exporting the sanctioned product via ports in Russia and Ukraine to buyers outside the EU. According to diplomats, the EU took the deliberate decision to limit the impact of economic sanctions in response to worries expressed by the EU's agricultural lobby and to 'keep space for further pressure on Belarus' (*Reuters* 2021b). Overall, the impact of the EU's sanctions will remain limited considering that Belaruskali ships the bulk of its products to China, India and Brazil, with exports to the EU amounting to just 8% of Belarus's \$2.4 billion potash export revenue last year (Nardelli et al. 2021).

Restrictions on the export of petroleum products, and in particular the ban on new contracts for the import or transfer of Belarusian petroleum products, including fuels from third countries exported from Belarus, are likely to have the most significant impact. In 2020 Belarus exported \$1.8 billion worth of petroleum products into the EU

and the UK, representing 50% of Belarus's total exports of petroleum products (Dobrinisky 2021). In response, action has already been taken by the Lukashenka regime to circumvent the sanctions against its oil industry, including changing the shareholder structure of the targeted companies and founding new companies to replace earlier ones (Kubiak 2021).

In terms of financial sanctions, Belarus had already been effectively cut off from foreign financial markets following the oppressive measures enacted in the aftermath of the 2020 presidential elections. However, while the financial sanctions ban EU entities from creating new Belarusian state debt, they do not target the state-owned Bank of Belarus, thus allowing EU investors to continue to buy bonds from the bank and EU banks to lend it money (*Reuters* 2021a). Moreover, the Belarusian regime can continue to rely on strong financial support from Russia, including a new \$1 billion credit line agreed last year.

## **EU support for civil society and its effects**

Support for civil society in Belarus has always featured prominently in the EU's discourse. In practice, a large portion of the EU's bilateral funding went to government institutions as direct budgetary support. The involvement of civil society in financial assistance programmes, such as the European Neighbourhood and Partnership Instrument and its successor, the European Neighbourhood Instrument (ENI), was very limited. In accordance with EU auditing rules, only registered entities and organisations could participate in projects, greatly limiting the access to funds of independent civil society organisations in Belarus as these were often denied formal registration. The main direct sources of funding for Belarusian civil society were the European Instrument for Democracy and Human Rights and the European Endowment for Democracy. Between 2012 and 2016 the former made commitments to beneficiaries based in Belarus that amounted to just over €660,000, and additional funds were also available to Belarusian human rights activists through the latter (Bosse and Vieira 2018, 28–9). Thus the importance of EU financial support for civil society in Belarus has by and large been symbolic. Yet at the same time the EU has helped to open up new opportunities for networking and joint projects (e.g. through the Eastern Partnership Civil Society Forum) and EU officials have also pushed the regime to be more open to dialogue with civil society. Following the brutal crackdown on civil society since the summer of 2020, however, most independent civil society organisations have been closed down, and activists and experts have been either detained or forced into exile (*Amnesty International* 2021b). In December 2020, the Commission adopted a €24 million assistance package, EU4Belarus, to complement the emergency support (€3.7 million) that the EU had previously mobilised for the victims of oppression and the independent media (European Commission 2020). It remains unclear how the EU will disburse funds to 'local civil society organisations and human rights activists' and promote 'civic empowerment in the country' (European Commission 2020) in the current, highly repressive climate in Belarus. The support is therefore most likely to benefit individuals who have been forced into exile.

## What role for the EU? Lessons learned and prospects

Over the past two decades, the EU's policies vis-à-vis Belarus have largely been reactive, engaging with the Lukashenka regime when human rights violations had seemingly decreased, and resorting to varying levels of restrictive measures when the regime had (again) brutally cracked down on peaceful protests, often around the time of fraudulent parliamentary and presidential elections. A broader, long-term strategy for the EU's policy towards Belarus has never existed, except that support for independent civil society has always featured prominently in the EU's official rhetoric. A critical limitation of EU policy vis-à-vis Belarus is its lack of geopolitical and economic leverage over the regime, as Russia 'remains the only game in town in Belarus' (Preiherman 2021). However, it is unclear whether building up more serious economic and political relations with the authoritarian regime, allowing it to 'diversify its foreign economic relations and to lessen economic dependence on Russia' (Preiherman 2021), would have had the desired effect of making Minsk more dependent on the EU. As was clearly observable in the aftermath of the August 2020 presidential elections, Lukashenka makes no compromises when securing his rule domestically, regardless of how much bloodshed it takes. And falling back on Russia would always have been an option available to Lukashenka. But the EU could have avoided certain mistakes, which have been based partly on the appeal of short-term geopolitical and economic gains and partly on illusions or misconceptions about the nature of the Lukashenka regime.

First, the EU has twice lifted sanctions against the regime despite little evidence that the human rights situation had improved in Belarus. On both occasions, the EU exchanged the achievement of geopolitical goals (Belarus's non-recognition of Abkhazia and South Ossetia in 2008 and its impartial stance on Ukraine in 2014) for the release of political prisoners. This allowed the Lukashenka regime not only to overplay its geopolitical significance to the EU (Bosse et al. 2021, 20–3) but also to turn political prisoners into a valuable bargaining chip in negotiations with the Union. In the future, the EU should prioritise progress in human rights and democracy in Belarus over short-term (and partly misconceived) geopolitical gains.

Second, the EU has always allowed lobbying efforts to water down the reach of its restrictive measures. Certain business people and sectors have been spared sanctions because lobbies within the EU have managed to influence member state decisions. The recent example of the EU agricultural lobby preventing meaningful sanctions against Belarus's potash exports is an illustrative case at hand. Moreover, EU companies such as Telekom Austria and Raiffeisenbank continue to operate lucrative branches in Belarus. The former was actively involved in providing mobile phone data from opposition activists to the Belarusian security services and blocking access to Internet webpages, while the latter blocked the bank accounts of hundreds of people involved in the protests (*Der Spiegel* 2021). Neither EU company is on the sanctions list, even though both are clearly violating the UN Guiding Principles on Business and Human Rights. In the future, the EU should be more consistent in the application of restrictive

measures, and resist lobbying efforts which undermine the EU's credibility and the effectiveness of sanctions.

Third, EU financial assistance should be distributed more evenly and be made more accessible to benefit local civil society organisations. Since 2007 by far the greatest part of EU funds has been disbursed to Belarusian public bodies. The cumbersome application processes for European Neighbourhood and Partnership Instrument and ENI funding were inaccessible for independent civil society organisations, especially those that lacked official registration in Belarus. The new Neighbourhood, Development and International Cooperation Instrument (NDICI) will include thematic programmes for 'Human Rights and Democracy' and 'Civil Society Organisations', and will operate independent of the consent of the governments and public authorities of the third countries concerned (European Parliament and Council 2021). It remains to be seen how the geographic and thematic programmes will work in tandem to support human rights and democracy, and what funds will be allocated to the eastern neighbourhood, especially given the global scope of the NDICI and the reduction of its budget by the Council from an initial €118.2 billion to €79.5 billion (European Commission 2021).

Fourth, the EU should avoid financing the repressive security apparatus of the Lukashenka regime and give up the illusion that the authoritarian regime will comply with international human rights standards. Over recent decades, the EU has invested heavily in border-management projects in Belarus, allocating more than €80 million since 2001 for border assistance, including high-tech communication equipment for Belarusian border guards. The provision of this equipment led to a major public scandal in 2013, in which the EU was accused of directly supporting the last dictatorship in Europe (*Telegraph* 2013). In July 2016 the European Commission announced in its Annual Action Programme for Belarus that it would provide €7 million from the ENI for the construction and/or renovation of several temporary migrant accommodation centres. The project started in October 2018. Soon after, investigative research group Danwatch exposed the 'inhumane treatment of migrants by the Belarusian border authorities', including 'pushbacks of Chechen refugees to Russia and extremely violent treatment of perceived irregular migrants by armed border guards' (Akkerman 2021, 28). In the future, and especially with regard to the new Readmission Agreement concluded with Belarus, the EU should be more careful in its selection of beneficiaries and very closely monitor the use of its assistance funds in Belarus. The EU should be under no illusions; the regime of Lukashenka is adamant about further consolidating authoritarianism in order to stay in power.

## References

- Akkerman, M. (2021). *Outsourcing oppression: How Europe externalises migrant detention beyond its shores*. Transnational Institute and Stop Wapenhandel. Amsterdam, April. <https://www.tni.org/files/publication-downloads/outourcingoppression-report-tni.pdf>. Accessed 24 September 2021.
- Amnesty International. (2017). *The human rights risks of external migration policies*. London. <http://www.refworld.org/pdfid/593fecfe4.pdf>. Accessed 24 September 2021.

- Amnesty International. (2021a). Belarus: No justice in sight for scores of human rights violations survivors one year on from disputed election. 9 August. <https://www.amnesty.org/en/latest/news/2021/08/belarus-no-justice-in-sight-for-scores-of-human-rights-violations-survivors-one-year-on-from-disputed-election/>. Accessed 24 September 2021.
- Amnesty International. (2021b). Belarus: Sweeping closure of dozens of NGOs as the crackdown on civil society continues. 23 July. <https://www.amnesty.org/en/latest/press-release/2021/07/belarus-sweeping-closure-of-dozens-of-ngos-as-the-crackdown-on-civil-society-continues/>. Accessed 24 September 2021.
- Bosse, G. (2012). A partnership with dictatorship: Explaining the paradigm shift in European Union policy towards Belarus. *Journal of Common Market Studies*, 50(3), 367–84.
- Bosse, G. (2017). EU–Belarus relations in the context of the European Neighbourhood Policy. In T. Schumacher, A. Marchetti & T. Demmelhuber (eds.), *Handbook of the European Neighbourhood Policy* (pp. 290–301). London: Routledge.
- Bosse, G., & Vieira, A. V. (2018). *Human rights in Belarus: The EU's role since 2016*. European Parliament, Directorate-General for External Policies. Brussels. [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO\\_STU\(2018\)603870](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU(2018)603870). Accessed 24 November 2021.
- Bosse, G., Höpner, M., & Vieira, A. (2021). Persuading the giant? Explaining Eastern Partnership states' (unexpected) negotiation success in relations with the European Union. *International Negotiation*, 1, 1–33.
- Council of the EU. (2020a). Belarus: Declaration by the High Representative on behalf of the European Union on the presidential elections. *Press Release*. 11 August. <https://www.consilium.europa.eu/en/press/press-releases/2020/08/11/belarus-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-presidential-elections/>. Accessed 24 September 2021.
- Council of the EU. (2020b). Council conclusions on Belarus. 11661/20, 12 October. <https://www.consilium.europa.eu/media/46076/council-conclusions-on-belarus.pdf>. Accessed 24 September 2021.
- Council of the EU. (2020c). Council Implementing Regulation 2020/1387 implementing Article 8a(1) of Regulation (EC) no. 765/2006 concerning restrictive measures in respect of Belarus. OJ L319 (2 October), 1. <https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=OJ:L:2020:319I:FULL&from=EN>. Accessed 24 September 2021.
- Council of the EU. (2021). Council Regulation (EU) 2021/1030 amending Regulation (EC) no. 765/2006 concerning restrictive measures in respect of Belarus. OJ L224 (24 June), 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3A0J.LI.2021.224.01.0001.01.ENG&toc=OJ%3AL%3A2021%3A224I%3ATOC>. Accessed 24 September 2021.
- Der Spiegel*. (2021). Im Dienste des Diktators. 20 August. <https://www.spiegel.de/wirtschaft/belarus-wie-westliche-firmen-alexander-lukaschenkos-regime-zu-diensten-sind-a-7e8ab687-0002-0001-0000-000178874265>. Accessed 24 September 2021.
- Dobrinsky, R. (2021). New EU sanctions against Belarus: What will be their economic effect? *Vienna Institute for International Economic Studies*, 28 June. <https://wiiw.ac.at/new-eu-sanctions-against-belarus-what-will-be-their-economic-effect-n-513.html>. Accessed 24 September 2021.
- Donadio, R. (2016). Svetlana Alexievich, Nobel Laureate of Russian misery, has an English-language milestone. *New York Times*, 20 May. <https://www.nytimes.com/2016/05/21/books/svetlana-alexievich-a-nobel-laureate-of-russian-misery-has-her-english-debut.html>. Accessed 24 September 2021.
- Eastern Partnership Civil Society Forum. (2017). Statement of the Coordinating Committee of the EaP CSF Belarusian National Platform on the events of 25–26 March 2017 in Minsk and

- other Belarusian cities. 27 March. [https://eap-csf.eu/wp-content/uploads/BNP-Statement-repressions-14.03.2017-eng\\_final.docx.pdf](https://eap-csf.eu/wp-content/uploads/BNP-Statement-repressions-14.03.2017-eng_final.docx.pdf). Accessed 24 September 2021.
- European Commission. (2020). *EU strengthens its direct support to the people of Belarus*. 11 December. [https://ec.europa.eu/neighbourhood-enlargement/news/eu-strengthens-its-direct-support-people-belarus-2020-12-11\\_en](https://ec.europa.eu/neighbourhood-enlargement/news/eu-strengthens-its-direct-support-people-belarus-2020-12-11_en). Accessed 24 September 2021.
- European Commission. (2021). European Commission welcomes the endorsement of the new €79.5 billion NDICI–Global Europe instrument to support EU’s external action. Press Release. Brussels, 19 March. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_21\\_1267](https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1267). Accessed 24 September 2021.
- European Parliament and Council. (2021). Regulation (EU) 2021/947 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, amending and repealing Decision no. 466/2014/EU and repealing Regulation (EU) 2017/1601 and Council Regulation (EC, Euratom) no. 480/2009. OJ L209 (9 June), 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0947>. Accessed 24 September 2021.
- Kłysiński, K. (2021). Pressure being stepped up cautiously: The EU’s and US’s sanctions against Belarus. *OSW Commentary*, 19 February. [https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-02-19/pressure-being-stepped-cautiously-eus-and-uss-sanctions#\\_ftnref12](https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-02-19/pressure-being-stepped-cautiously-eus-and-uss-sanctions#_ftnref12). Accessed 24 September 2021.
- Kubiak, M. (2021). Belarus secures Russian oil and gas supplies for 2021. *Eurasia Daily Monitor*, 7 January. <https://jamestown.org/program/belarus-secures-russian-oil-and-gas-supplies-for-2021>. Accessed 24 September 2021.
- Lester, M., & O’Kane, M. (2021). *Court judgements: Belarus; Sanctions: Law, practice and guidance*. <https://www.europeansanctions.com/judgment/country/belarus/>. Accessed 24 September 2021.
- Nardelli, A., Kudrytski, A., & Fedorinova, Y. (2021). EU hits Belarus with sanctions on potash, petroleum goods. *Bloomberg*, 24 June. <https://www.bloomberg.com/news/articles/2021-06-24/eu-hits-belarus-with-sanctions-targeting-potash-petroleum-goods>. Accessed 24 September 2021.
- Political and Security Committee. (2015). *Relations with Belarus: List of possible additional concrete measures to deepen the EU’s policy of critical engagement with Belarus*. 28 January. <https://www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentNumber=5612%2F15&DocumentLanguage=en>. Accessed 14 October 2021.
- Preiherman, Y. (2021). The Belarus test for the ‘geopolitical’ EU: A view from Minsk. *Heinrich Böll Stiftung*, 25 February. <https://www.boell.de/en/2021/02/25/belarus-test-geopolitical-eu-view-minsk>. Accessed 24 September 2021.
- Reuters. (2021a). Belarus leader has little to fear from EU sanctions – analysts. 1 July. <https://www.reuters.com/world/europe/belarus-leader-has-little-fear-eu-sanctions-analysts-2021-07-01/>. Accessed 24 September 2021.
- Reuters. (2021b). Most Belarus potash exports not affected by EU sanctions – analysts. 25 June. <https://www.reuters.com/world/europe/most-belarus-potash-exports-not-affected-by-eu-sanctions-analysts-2021-06-25/>. Accessed 24 September 2021.
- Telegraph. (2013). EU passes British aid to Belarus dictator. 19 October. <https://www.telegraph.co.uk/news/worldnews/europe/10391006/EU-passes-British-aid-to-Belarus-dictator.html>. Accessed 24 September 2021.
- Vieira, A. (2014). The politico-military alliance of Russia and Belarus: Re-examining the role of NATO and the EU in light of the intra-Alliance security dilemma. *Europe-Asia Studies*, 66(4), 557–77.

**Author biography**

**Giselle Bosse, PhD**, is Associate Professor in EU External Relations, Jean Monnet Chair in EU International Relations, and Vice Dean at the Faculty of Arts and Social Sciences, Maastricht University. She is also co-director of the Centre for European Research in Maastricht, visiting professor at the College of Europe (Bruges) and a research associate at the Wilfried Martens Centre for European Studies (Brussels).



# Battle of the hearts: China's aim to become a soft (super)power and Europe's response

European View  
2021, Vol. 20(2) 211–219  
© The Author(s) 2021  
DOI: 10.1177/17816858211055553  
journals.sagepub.com/home/euv



**Janne Leino**

## Abstract

While China has made remarkable advances in its economic, technological and military development over the past decades, its perceived influence and reputation are declining in some parts of the world. This poses a problem for Chinese decision-makers as the country's self-proclaimed goal to become a leading global power relies on its build-up of soft power, that is, the ability to influence others by persuasion rather than coercion. The article examines why China, despite the increasingly nationalist tendencies at home, will continue its international push to become a soft (super)power, and discusses how the EU should react.

## Keywords

China, EU, Soft power, Influence, Trade, Global Gateway

## Introduction

On 1 July 2021 Chinese President Xi Jinping made a speech during the celebrations for the one hundredth birthday of the Chinese Communist Party (CCP). During the carefully orchestrated ceremony, President Xi announced that 'through tenacious struggle, the Party and the Chinese people showed the world that the Chinese people were capable of not only dismantling the old world, but also building a new one' (*Xinhua* 2021). Indeed, since the reform and opening up policies of Chairman Deng Xiaoping, China has challenged the leading role of the US and Western countries in military and economic power, as well as by shaping global institutions. China now has the biggest army and navy in the world (US, Department of Defense 2020) and is on track to become the largest economy

---

## Corresponding author:

J. Leino, Konrad-Adenauer-Stiftung e. V., Multinational Development Policy Dialogue Brussels, 11 Avenue de l'Yser, Brussels, B-1040, Belgium.  
Email: [janne.leino@kas.de](mailto:janne.leino@kas.de)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

globally during the next decade. Moreover, China has been able to leverage its growing economic weight both within the UN system, in terms of securing top positions in several UN agencies and institutions, and by establishing new international institutions that support the country in its global policies and initiatives, one such example being the new Asian Infrastructure Investment Bank.

Many scholars see the increase in China's military, economic and international institutional power as a challenge to the current world order. In 2019 the EU emphasised this narrative by classifying China as a 'systemic rival', while also including the terms 'economic competitor' and 'cooperation partner' in its strategic outlook on the country (European Commission 2019). However, if China seeks to end the Pax Americana and become the hegemon of the twenty-first century, it needs more than mere military force, economic output and influence in international institutions. It will have to develop into a soft superpower. This was acknowledged in 2014 by Chinese President Xi Jinping, when he stated that China should 'give a good Chinese narrative, and better communicate China's message to the world' (Biswas and Tortajada 2018).

For European actors it is crucial to understand why and how China aims to build its soft power, and what kind of options it has to achieve this aim. This article argues that Europe should adapt its approach to China by clearly defining its red lines and speaking with one voice. Simultaneously, EU decision-makers should learn from modern history and refrain from generally branding 'Made in China' as something negative, as this might be counterproductive for countering Chinese influence.

## **China's desire to build up its soft power**

As tensions between the US and China have been rising, China has been using increasingly nationalistic tones both at home and abroad. Recently, hawkish Chinese officials have become known as 'wolf warriors' on social media channels such as Twitter—which are, ironically, banned from operating within China. Alongside limiting its citizens' access to social media channels, China has gone further, banning teaching materials and textbooks which are considered to promote Western ideals or views of history (*Reuters* 2018). Instead pupils now learn 'Xi Jinping thought', thus ensuring that 'red genes' are passed down through the generations (*Bloomberg* 2021).

While these examples of hawkish diplomacy and a tighter grip on the education sector might suggest that China is turning inwards instead of outwards, this will not be the case in the long run. From China's perspective, there are several reasons to further increase its soft power and influence abroad.

First, soft power is the ability to obtain preferred outcomes by attraction rather than coercion or payment (Nye 2017). This is every country's aim in international relations. Moreover, in a digitalised world with long value and supply chains, it is often the image of a country, or of a company perceived to represent a country, that attracts promising talent and investment, or sells products. Thus, looking at soft power from a geopolitical

perspective, the battle to win hearts and minds will be just as important as developing the newest technology or the most modern fighter jets. If China succeeds in becoming a soft superpower, inspiring and influencing leaders and citizens around the world, it will be able to set the agenda and decide on standards in the new world order.

Second, like many European countries, China is facing the challenge of an ageing population and a declining labour force. To diffuse these developments, it will need to remain open. According to China's official census data from 2020, population growth is rapidly declining, while the number of people over 65 is increasing (China, National Bureau of Statistics 2021). This continuing demographic shift to a declining labour force, combined with a low fertility rate and a rapidly ageing society, is expected to weigh on the country's economic progress. Moreover, while the Chinese population is living longer, the average retirement age has not followed suit. The average retirement ages, 60 for men and 55 for women, will burden the national pension system (Lee and Wang 2021). Alongside the economic factors, these developments are putting pressure on society and families. It is unlikely that the recent policy changes and the abolition of the one-child policy will reverse the trend of an ageing population.

It is more likely that China will have to rely on a foreign workforce to boost its economic growth and its international innovation capacity, at least in the long run. Currently the number of foreigners living in China is still miniscule, despite the overall increase in population. According to the 2020 national census, there were 845,697 foreigners living in China, up about 250,000 from a decade ago, out of a total population of 1.4 billion (Li 2021). As a comparison, in 2020 more than one million foreigners were living in Belgium (*Statista* 2021), a country with around 11 million inhabitants.

Third, China relies on international markets. The Chinese economy is currently not self-sufficient nor will it be so in the near future, despite the new 'dual circulation' economic model, which has its root in the fourteenth five-year plan (2021–25). An example from the agricultural industry: China is the world's largest importer of agricultural products. In 2020 it imported \$133.1 billion worth of agricultural products (US, Department of Agriculture 2020). Even though President Xi (2015) has declared that 'the rice bowls of the Chinese people must be held by themselves', this goal will not be easily achieved. China possesses around 10% of the world's total arable land, but in per capita terms the acreage available for crops was less than half of the global average as of 2006 (Wang 2020). Moreover, China also needs export markets for its products and the international finance market for its own development. The Chinese export industry is one of the nation's economic pillars. In 2020 China exported products worth more than \$2,591 billion, almost twice as much as the US (\$1,432 billion) or Germany (\$1,380 billion) (*Statista* 2020).

Fourth, China openly recognises the need to work together with the international community on issues perceived as mutually beneficial. Most importantly these include the battle against climate change and biodiversity loss. The reasons behind China's international engagement are similar to those in Europe. On the one hand, the Chinese

population has become aware of the global problems related to climate change, and this awareness is pushing the climate agenda within the country. In a sign that the climate topic had reached national politics, in 2015 the country's censors decided to pull a critical Chinese environmental documentary from the Internet after it had been viewed 150 million times in just three days. On the other hand, the global market for climate- or sustainability-related technology will likely become a major source of innovation and offer export possibilities for domestic companies.

Lastly, in terms of size and economic geopolitics, China might not remain the most populous country or biggest economic market in the long run. India's population is expected to surpass China's by the end of this decade. In 2015 and 2016 India's annual GDP growth rate also exceeded that of China. However, measured by most development indicators, such as the UN Development Programme's Human Development Index, China is likely to remain ahead of its regional rival in the near future. Recent tensions between the two countries have shown that both are taking their neighbour more seriously in economic, political and military terms. As India is increasingly engaging in partnerships perceived as hostile by Beijing, such as the Quadrilateral Security Dialogue or Quad, tensions are likely to remain strong.

## **China's perceived influence is declining in parts of the world**

Layne (2018, 91) argues that soft power, which is needed for political influence, is built on ideological, ideational and cultural appeal. In these domains in particular, China's perceived influence has taken a hit in recent years. This tendency is especially clear in advanced economies: while in 2002 most citizens in Australia, the UK, the Netherlands, South Korea and Japan had favourable views of China, by 2020 the public's view had become unfavourable in all of these countries. Even in Germany, which has historically been an advocate for dialogue with Beijing, 71% of the respondents had an unfavourable view of China in 2020 (Silver et al. 2020). At the same time, China is also losing its influence in some developing countries. In a recent Afrobarometer study conducted in 16 countries, China was trailing the US as Africans' preferred development model (Appiah-Nyamekye Sanny and Selormey 2020). Moreover, the study revealed a possible link between soft power and economic opportunities: while a majority (55%) of those surveyed in the 16 African nations said that China's economic activities in their country had had an influence on the local economy, this number had dropped sharply from 71% five years ago. The possible link between China's soft power (ideological, ideational and cultural appeal) and the effect on its economic activities, especially in developing countries, should thus be a subject of further study.

The reasons for the declining positive perceptions of China are multifaceted. They include what have widely been considered negative developments linked to Hong Kong, Taiwan and Xinjiang. But this decline also stems from China's handling of the outbreak of the novel coronavirus (COVID-19) pandemic.

Analysing these trends from a Chinese perspective, two new challenges seem especially acute. First, it was easier for China to promote its own agenda during former US President Donald Trump's administration, as he claimed to put 'America first' and openly withdrew from parts of the international arena. This approach left the door open for increased Chinese economic and political influence, as even traditional US allies had to reassess the US's commitment. President Joe Biden has announced that the US will re-enter the international arena and build democratic alliances, and has also used a hawkish tone when speaking of China. Second, while China's outbound foreign direct investments increased yearly between 2005 and 2016, since 2017 they have been decreasing (MERICS 2021). As the current pandemic enters its third year, a rapid increase in these investments seems unlikely. This trend might lead to disappointment among partnering Belt and Road (BRI) countries, which are expecting lucrative trade deals and investments from China. The closest examples of disenchantment with the BRI can be found in Central and Eastern Europe, where several governments have publicly raised their disappointment (Kapitonenko 2021). Lithuania has even taken things a step further by leaving the Chinese-led 17+1 cooperation format and has allowed Taiwan to open a 'representative office' on its soil, despite objections from Beijing.

In summary, these developments mean that China now has to operate in a more contested international arena alongside a (re-)engaged US and a more cautious EU, while it has fewer economic options at its disposal. In this situation, soft power based on perceptions and narratives becomes an even more important tool in its foreign-policy tool-box.

## **Finding a balance between nationalism and building international partnerships**

In light of China's push for further international engagement and the drop in influence abroad on the one hand, and the increasingly indoctrinated home audience on the other, China finds itself in a balancing act between two potential ways of moving forward. It can either soften its international outreach by toning down some of its rhetoric and focusing on building up alliances of its own, or it can (re-)focus on its domestic audience while continuing to fuel anti-Western sentiments in a select small group of countries where these sentiments prevail. Most probably it will choose a mix of both approaches.

After public opinion turned against China in the aftermath of the COVID-19 outbreak, China's leadership to some extent moderated its tone. 'We must focus on setting the tone right, be open and confident but also modest and humble, and strive to create a credible, lovable and respectable image of China,' Xi Jinping told cadre members in June 2021 (Lee Meyers and Bradsher 2021).

As one example of this, China has toned down its mask and vaccine diplomacy, which might be partly due to the lower effectiveness of the Chinese COVID-19 vaccines compared to those made in the US and Europe (McGregor 2021). Like the EU, China has

recently announced that it will build up its local vaccination production capacity, instead of simply selling or donating vaccines. Most notably it announced that it would build a large vaccine production plant in Indonesia, the biggest country in South-East Asia. China will also most likely increase its efforts to build good ties with emerging leaders around the world through educational exchanges and programmes that target political leaders and other social influencers. Examples of this can be found in the outreach programmes of the CCP in South-East Asia (see Reiss 2021), in the founding and upgrading of Chinese language and culture centres, and in the planned first campus of a Chinese university in Hungary.

While China is building its soft power, it might find it difficult to find a balance between a soft approach on the one hand, and maintaining and communicating absolute positions on the other. As these self-defined ‘red lines’ are deeply rooted in the increasingly nationalistic Chinese education system, Chinese decision-makers will be able to count on, and might even feel pressured by, popular support. Most notably these red lines include issues such as Taiwan, Tibet, Xinjiang, Hong Kong and the country’s position on the South China Sea, where China has overlapping territorial claims with several other nations. One example of the diplomatic balancing act Beijing faces occurred in August 2021, when the Chinese Ministry of Foreign Affairs asked Germany to clarify the intentions of a German naval vessel in the South China Sea before rejecting its previously planned port call in Shanghai. The EU’s intentions with regard to applying a coordinated maritime presence mechanism in the Asia-Pacific region will likely be met with similar caution.

## Conclusion

Knowing that China will aim to increase its influence and soft power, the EU has several options in terms of how to react. Learning from the past, the EU should not fall for the ‘Made in Germany’ trap. In 1887 the UK forced foreign products to be marked with their country of manufacture. This was done to protect local production by clearly marking products which did not originate in the UK. Subsequently, Germany was able to benefit from the ‘Made in Germany’ tag, as it became synonymous with quality. Drawing conclusions from this, it is important that EU decision-makers acknowledge the technological advances of Chinese companies as such when drafting relevant trade or value-chain legislation. Branding ‘Made in China’ as something purely negative will be counterproductive.

Instead, the EU and its member states should focus on further developing its greatest assets: its own soft power and, in cooperation with likeminded partners, the power to define common values-based standards.

For skilled people around the world, including many Chinese, Europe and the US remain attractive places to study, work or settle. In an extreme example, between 2012 and 2020 the annual number of asylum seekers from China rose from 15,362 to 107,864, according to the UN High Commissioner for Refugees (*Economist* 2021). During

President Xi's reign more than 600,000 Chinese nationals have sought asylum, most of them in the US.

Building one's own soft power based on liberal values does not mean giving up one's principles. The EU should get better at forming consensus, while clearly defining its own red lines. Internally, the EU and its member states should continue to define both the Union's standards and the mechanisms for dealing with possible breaches of them. Consider the following example from the field of education, a domain considered crucial for building soft power and fostering innovation. Like the foreign direct investment screening mechanism, the EU and its member states should take steps to ensure the continuance of academic freedom and the freedom of speech. This does not mean limiting the number of Chinese students, as President Trump did in May 2020, but that there should be checks and balances in place to ensure academic freedom is guaranteed. Recent reports about CCP cells in North American universities, whose members report on or intimidate staff members and students, should act as a warning.

In its external relations the EU should have a clear division of labour and transparent decision-making processes in place to enable it to speak swiftly and with a single voice. EU policies and instruments should also build up local capacities and offer real alternatives to developing countries. In July 2021 the European Council announced the new 'Globally Connected Europe' initiative, which builds on the 2018 Strategy for Connecting Europe and Asia and will be finalised by spring 2022. The initiative and the 'Global Gateway' connectivity strategy are widely seen as Europe's response to the Chinese-led BRI as they aim to (1) identify and implement high-impact and visible projects and actions, (2) present financing schemes to incentivise investments, (3) mobilise the private sector and (4) ensure the EU's visibility (Council of the EU 2021).

In order for this and other initiatives to be successful in building European soft power, there are many open questions that need to be addressed. These include the following:

- Who will be the leading European figure(s) to enable the EU to compete with China in terms of worldwide recognition?
- How will future projects, activities and their target groups be decided on within the EU? How can a swift and transparent decision-making process which includes different voices from the partner country be secured?
- How will the EU secure its visibility and intended impact, especially in projects that are funded by the private sector, and how will it ensure that these projects and actions are built on the values and principles that it claims to uphold?

If the EU wants to counter Chinese influence and expand its own soft power, then alongside economic and connectivity projects, it should also focus on people-to-people dialogues and capacity-building programmes which raise awareness of the Chinese and European development approaches among students, civil society, the media and young

decision-makers. The focus should be on long-term programmes which enable mutually beneficial development and aim to shape international norms and standards together with the partner country involved. Through an inclusive and proactive approach, flanked by a commonly agreed upon and output-oriented monitoring and evaluation scheme, the EU has the power to simultaneously increase its own soft power and counter Chinese influence.

## References

- Appiah-Nyamekye Sanny, J., & Selormey, E. (2020). *Africans regard China's influence as significant and positive, but slipping*. Afrobarometer Dispatch no. 407, 17 November 2020. [https://afrobarometer.org/sites/default/files/publications/Dispatches/ad407-chinas\\_perceived\\_influence\\_in\\_africa\\_decreases-afrobarometer\\_dispatch-14nov20.pdf](https://afrobarometer.org/sites/default/files/publications/Dispatches/ad407-chinas_perceived_influence_in_africa_decreases-afrobarometer_dispatch-14nov20.pdf). Accessed 1 September 2021.
- Biswas, A., & Tortajada, C. (2018). China's soft power is on the rise. *China Daily*, 23 February. <https://www.chinadaily.com.cn/a/201802/23/WS5a8f59a9a3106e7dcc13d7b8.html>. Accessed 1 September 2021.
- Bloomberg. (2021). China teaches school children 'do as President Xi tells you'. 4 February. <https://www.bloomberg.com/news/articles/2021-02-04/china-teaches-school-children-do-as-president-xi-tells-you>. Accessed 1 September 2021.
- China, National Bureau of Statistics. (2021). *Main data of the seventh national population census*. 11 May. [http://www.stats.gov.cn/english/PressRelease/202105/t20210510\\_1817185.html](http://www.stats.gov.cn/english/PressRelease/202105/t20210510_1817185.html). Accessed 20 August 2021.
- Council of the EU. (2021). *A globally connected Europe – Council conclusions*. 12 July. <https://data.consilium.europa.eu/doc/document/ST-10629-2021-INIT/en/pdf>. Accessed 1 September 2021.
- Economist. (2021). Under Xi Jinping, the number of Chinese asylum-seekers has shot up. 28 July. <https://www.economist.com/graphic-detail/2021/07/28/under-xi-jinping-the-number-of-chinese-asylum-seekers-has-shot-up>. Accessed 1 September 2021.
- European Commission. (2019). *EU–China – A strategic outlook*. 12 March. <https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook.pdf>. Accessed 1 September 2021.
- Kapitonenko, N. (2021). China's soft power debacle in Eastern Europe. *IPS-Journal*, 5 May. <https://www.ips-journal.eu/topics/foreign-and-security-policy/chinas-soft-power-debacle-in-eastern-europe-5146>. Accessed 1 September 2021.
- Layne, C. (2018). The US–Chinese power shift and the end of the Pax Americana. *International Affairs*, 94(1), 89–111. [https://www.chathamhouse.org/sites/default/files/images/ia/INTA94\\_1\\_6\\_249\\_Layne.pdf](https://www.chathamhouse.org/sites/default/files/images/ia/INTA94_1_6_249_Layne.pdf). Accessed 1 September 2021.
- Lee, A., & Wang, O. (2021). China population: Beijing urged to act in face of 'brutal' facts of slower birth rate, declining workforce. *South China Morning Post*, 11 May. <https://www.scmp.com/economy/china-economy/article/3133088/china-population-beijing-urged-act-face-brutal-facts-slower>. Accessed 1 September 2021.
- Lee Meyers, S., & Bradsher, K. (2021). China's leader wants a 'lovable' country. That doesn't mean he's making nice. *New York Times*, 8 June. <https://www.nytimes.com/2021/06/08/world/asia/china-diplomacy.html>. Accessed 1 September 2021.
- Li, L. (2021). China embraces increasing foreign residents. *China Daily*, 12 May. <http://global.chinadaily.com.cn/a/202105/12/WS609b14c5a31024ad0babd49f.html>. Accessed 3 September 2021.

- McGregor, G. (2021). How do China's COVID vaccines fare against the Delta variant? *Fortune.com*, 31 August. <https://fortune.com/2021/08/31/china-covid-vaccine-sinovac-sinopharm-delta-variant-effective/>. Accessed 3 September 2021.
- MERICs. (2021). *Chinese FDI in Europe: 2020 update*. <https://merics.org/en/report/chinese-fdi-europe-2020-update>. Accessed 1 September 2021.
- Nye, J. (2017). Soft power: The origins and political progress of a concept. *Nature.com*, 21 February. <https://www.nature.com/articles/palcomms20178>. Accessed 14 September 2021.
- Reiss, A. (2021). All that glitters is not gold: The Chinese Communist Party's influence on the political elite in Southeast Asia. *Konrad Adenauer Stiftung*, 30 June. <https://www.kas.de/en/web/auslandsinformationen/artikel/detail/-/content/es-ist-nicht-alles-gold-was-glaenzt-1>. Accessed 1 September 2021.
- Reuters. (2018). China expunges unapproved, foreign content from school textbooks. 20 September. <https://www.reuters.com/article/us-china-education-idUSKCN1M00D9>. Accessed 1 September 2021.
- Silver, L., Devlin, K., & Huang, C. (2020). *Unfavorable views of China reach historic highs in many countries*. Pew Research. <https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/>. Accessed 1 September 2021.
- Statista. (2020). Die 20 größten Exportländer weltweit im Jahr 2020. <https://de.statista.com/statistik/daten/studie/37013/umfrage/ranking-der-top-20-exportlaender-weltweit/>. Accessed 1 September 2021.
- Statista. (2021). Foreign population of Belgium in 2020, by origin. <https://www.statista.com/statistics/517235/foreign-population-of-belgium-by-origin/>. Accessed 14 September 2021.
- US, Department of Agriculture. (2020). *China: Evolving demand in the world's largest agricultural import market*. <https://www.fas.usda.gov/data/china-evolving-demand-world-s-largest-agricultural-import-market>. Accessed 1 September 2021.
- US, Department of Defense. (2020). *Military and security developments involving the People's Republic of China 2020. Annual report to Congress*. <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>. Accessed 1 September 2021.
- Wang, O. (2020). China food security: How's it going and why's it important? *South China Morning Post*, 29 November. <https://www.scmp.com/economy/china-economy/article/3111623/china-food-security-hows-it-going-and-whys-it-important>. Accessed 1 September 2021.
- Xi, J. (2015). 'The rice bowls of the Chinese people must be held by themselves: Ensuring food security and social stability'. Speech given at the Central Rural Work Conference, 23–4 December 2013. *China Story*. [https://www.chinastory.cn/ywdbk/english/v1/detail/20190719/101270000042741563517384580290837\\_1.html](https://www.chinastory.cn/ywdbk/english/v1/detail/20190719/101270000042741563517384580290837_1.html). Accessed 4 October 2021.
- Xi, J. (2021). Speech at a ceremony marking the centenary of the Communist Party of China, 1 July. *Xinhua*. [http://www.xinhuanet.com/english/special/2021-07/01/c\\_1310038244.htm](http://www.xinhuanet.com/english/special/2021-07/01/c_1310038244.htm). Accessed 1 September 2021.

## Author biography



**Janne Leino** leads the Konrad Adenauer Stiftung's Multinational Development Policy Dialogue's programmes on foreign and security policy in Brussels. Previously, he was the chief representative of the Hanns Seidel Foundation's office in Hangzhou, China and a guest researcher at the Zhejiang International Studies University. Before moving to China, he worked for the Ministry for Foreign Affairs of Finland.

# EU dialogue with Russian society: A reality check

European View  
2021, Vol. 20(2) 220–225  
© The Author(s) 2021  
DOI: 10.1177/17816858211050130  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Robert Pszczel**

## Abstract

Engagement with Russian civil society is the least contested part of the EU's current and expected future approach to Russia. There is broad agreement on the need to conduct a dialogue with Russian citizens and to facilitate people-to-people contacts, as well as to support civil society as such. However, this general goal is not fully matched by a clear understanding of what the basic features and sentiments of Russian society are today. This article seeks to sketch an unvarnished picture of Russian society, knowledge of which is essential for the effective design and successful conduct of any engagement activities (their formats, channels of communication and content). The key problems include the lack of enthusiasm among ordinary Russians for the European project, and their growing confusion—fuelled by authoritarian control and disinformation—about European institutions and norms.

## Keywords

EU, Russia, Civil society, Engagement, Public opinion, Europe

## Introduction

The European political world is still reverberating with echoes of the recent spat induced by the last-minute initiative of French President Emmanuel Macron and German Chancellor Angela Merkel to convince other EU member states ahead of the 24–5 June European Council meeting to restart high-level meetings with Russia (Fleming et al. 2021). Egos have been bruised, and accusations of a lack of European solidarity and disregard for the opinions of Central and Eastern European countries, as well as counter-claims about a lack of realism, are flying high and low. This debate will no doubt go on, but the immediate task should be to fill with substance those elements of the EU's Russia policy which either have been agreed or have officially been put on the table.

## Corresponding author:

Robert Pszczel, Fundacja im. Kazimierza Pułaskiego, ul. Oleandrów 6, 00-629 Warsaw, Poland.  
Email: [office@pulaski.pl](mailto:office@pulaski.pl)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

The most concrete and promising elements are included in the new policy prescription presented by High Representative of the Union for Foreign Affairs and Security Policy Josep Borrell on 16 June. Developed together with the European Commission, this Joint Communication on EU–Russia relations is built around three main pillars: (1) pushing back, (2) constraining and (3) engaging (European Commission 2021). The 24–5 June European Council meeting took into account this report in its discussion on EU–Russia relations (European Council 2021, 6).

This paper focuses on the third pillar of the Joint Communication from the point of view of the intended addressee, that is, Russia, or more specifically, the Russian people. Such engagement includes two parts: the relationship with the Russian authorities (this topic will be left to one side as it is worthy of a separate analysis) and the relationship with the broader Russian civil society. In a recent blog post, for example, High Representative Borrell (2021) emphasised:

Crucially, we [the EU] must continue to engage with Russian civil society and citizens. Our quarrel is with the policy choices of the Russian government, not the Russian people. So, we should strengthen people-to-people contacts, which could include more visa facilitation for young people, academics, or other cross-border exchanges. We must continue to support Russian civil society and human rights defenders and be more flexible and creative in the way we do so.

The giant of the Renaissance, Leonardo da Vinci, is famously credited with the advice that ‘Nothing can be loved or hated unless it is first understood.’ It certainly makes sense for the EU to follow this credo in its relationship with Russia by taking a closer look at Russian society. This article argues that, currently, Russian society does not closely resemble its European counterparts. Its dominant frames of reference are geared more to the past than to the future. Moreover, the authoritarian model of governance in the country complicates efforts to hold an authentic dialogue with truly independent representatives of civil society. This calls for a modest and tailored approach, while keeping more ambitious goals of engagement for the future.

## **Europeanness in Russia**

Instinctively, many observers hope that the Kremlin’s disdain for European norms, values and traditions (e.g. the rule of law, human dignity, individual rights and freedom of speech) is not reflected in Russian society. Protests are apparently inevitable (Lemon 2020). Under conditions of real freedom, it is assumed that Russians would choose the European vision and opt for shared values. Much attention is given (for good reason) to those Russians who are fighting to transform Russia into a normal European country, who seem to epitomise such a vision. The EU’s own Agreement for Partnership and Cooperation with Russia, concluded in 1997, speaks of ‘the historical links existing between the Communities, its Member States and Russia and the common values that they share’ (Official Journal of the European Communities 1997, 1).

The problem is that at present the evidence offered by the Levada Center, a non-political Russian polling and sociological research organisation, suggests something

different. In 2021 only 29% of Russians considered Russia a European country (down from 52% in 2008), and even fewer feel themselves to be European (27%; down from 35% in 2008) (*Levada Center* 2021a). What is perhaps most depressing is the fact that such sentiments are even stronger among the youngest group of Russian adults (aged 18–24)—a bare 23% in that age group regard Russia as a European country, while a whopping 74% do not see themselves as European (*Levada Center* 2021a).

Another poll conducted by the Levada Centre, this time asking Russians to name their preferred prominent personalities in the world, does not inspire optimism either. Not for the first time, former Soviet dictator Joseph Stalin tops the list (39%), followed by his predecessor Vladimir Lenin, then Russian poet Alexander Pushkin and Tsar Peter the Great (*Levada Center* 2021b). Russian President Vladimir Putin is high in the rankings too (even if slipping), and the only non-Russians include Albert Einstein with 9%, followed by Napoleon Bonaparte and Adolf Hitler (each with 5%) (*Levada Center* 2021b). By choosing such role models (in particular those responsible for millions of deaths), Russian society seems quite far away in its sentiments from the European mainstream. It is no wonder that 70% of respondents support the idea of reviving Gulag-like prison labour in Russia (*The Moscow Times* 2021).

This bleak picture is reinforced by the Russians' stated preference for events that generate pride (*Levada Center* 2020). The Soviet Union's victory over Nazi Germany in the Second World War comes first, followed by Russia's annexation of Ukraine's Crimea region in 2014 and the Soviet/Russian conquest of space.

## Implications of the data

All these indicators point to a society that is stuck in the past. The shadow of the empire hangs over ordinary Russians (i.e. admiration of Stalin, and almost religious pride in the Second World War victory and the annexation of Crimea). The lack of confidence in Europe can be linked to this as well—the world has moved on but Russia has not moved with it. Of course, the Kremlin has reinforced and nurtured such sentiments through its anti-democratic and anti-European policies, never missing an opportunity to belittle European unity and the value of its institutions. Most recently in an opinion editorial, Russian Foreign Minister Sergey Lavrov compared Europeans to a choir mindlessly following the lead vocalist, that is, the US (Lavrov 2021). In addition, in his zeal to denigrate Europe, Lavrov even falsely claimed that European schools teach that Jesus was bisexual (Lavrov 2021).

This imperial nostalgia comes at a price. Russian historian Mikhael Khodarkovsky is probably right to argue that the lack of democracy in Russia is a hangover from the loss of its empire. And this creates a negative feedback loop—without dropping this imperial sentiment Russians are not likely to improve the state of democracy in their country. As Andrei Kolesnikov puts it: there can be no modernisation without de-Stalinisation (Kolesnikov 2021). But how can this happen when the state is de facto criminalising the search for objective history? A recent piece of legislation approved by Putin forbids making comparisons between Stalin's Soviet Union and Hitler's Germany (Parfitt 2021), as

if the 1939 Molotov–Ribbentrop Pact and its secret protocol, which divided Central and Eastern Europe into Nazi and Soviet spheres of influence, was never concluded.

Russian society is clearly suffering from a deficiency of democracy. Russia is progressively being turned into a dictator's dream, what some commentators have called a 'managed administrative utopia' (Meduza 2021). Russia's best and brightest are either abroad or in prison—and the silent majority is losing its appetite for protest. The State Duma elections in September 2021 were the least competitive in modern history, with only a token number of opposition candidates being allowed to stand. Access to information—the essential nourishment for free debate and scrutiny of rulers, and a key ingredient in opinion-forming—is becoming severely restricted (Tkachev 2021). A National Surveillance Programme is also being developed, modelled on the Chinese camera-state (Коммерсантъ 2021). And all this is happening in the open, with Kremlin-linked figures such as Vladislav Surkov (former deputy prime minister and adviser to Vladimir Putin) even trying to present an ideological justification for reduced liberties ('An overdose of freedom is lethal to a state') (Foy 2021).

Russian society is thus deprived of any real political choice, is suffering from political apathy and, thanks to the Kremlin's constant propaganda barrage, continues to distrust those who are branded as external and internal enemies. In short, it is politically disoriented and traumatised.

Moreover, the implied deal of the first decade of Putin's rule (i.e. accept 'managed democracy' in return for improved standards of living and modernisation) is no longer on the table. Corruption is rampant, and social and economic inequalities are reaching unacceptable levels: according to some estimates the 500 richest individuals in Russia own half of the nation's wealth (Prokofief 2021). The real monthly wage median in the country (after accounting for the Moscow discrepancy) is a paltry 25,000 roubles (or €290 at the early July exchange rate) (RTVI Новосту 2021). Ordinary people are preoccupied less with new holidays abroad than with the rising price of energy and poor infrastructure. It is no wonder that, during his latest Direct Line public conversation, Putin was asked to intervene personally on issues of leaking pipes and firemen's salaries. Climate change (long downplayed by the authorities) is leading to the literal collapse of buildings in Russia's north. The 'shadow economy' is not shrinking—people do not trust the authorities, and they cannot function properly in a legal framework that is ridden with chaos and corruption. Political obsessions with conspiracy theories are even blocking regional development, as in the Kaliningrad region (Goble 2021). Yes, the Russian people are a sturdy lot—but with everything that is going on around them they are trying to cling to what they have, rather than dreaming of a Russia that is catching up with EU countries in terms of affluence and quality of life.

As if all of the above was not enough, Russia is currently reeling from the worsening pandemic situation. The number of COVID-19 cases, particularly those of the Delta variant, is growing. The Kremlin's disinformation campaign against foreign vaccines has come back to bite Russia with a vengeance—many Russians, traditionally distrustful of the government, are even more reluctant to get a dose of the local Sputnik V vaccine (of which there are shortages anyway).

## Conclusion

So how do you develop ‘people-to-people contacts’ between the EU and Russia in such conditions? Some experts suggest ensuring ‘the survival of Russian civil society’ by preparing ‘to host Russian political emigrants’ in our countries and providing some form of support ‘for the repressed that remain in Russia’ (Domanska 2021). Selective visa liberalisation may be a sensible policy too. And on top of that, the EU and the rest of the Western community must do more to undermine the Kremlin’s hold over the Russian people’s access to information. But perhaps most importantly, the level of ambition should be modest and realistic—for now. Once Russian society is able to heal itself and Russia regains the respect of its neighbours, a real and in-depth conversation will become possible, and the topics of such dialogue could even include issues of integration (as argued by Sławomir Debski of the Polish Institute of Foreign Affairs) and convergence.

Right now, however, whatever the EU chooses to do, it must be aware that engaging with Russian society today means dealing with a traumatised, disoriented and generally distrustful nation. Russians’ ability and freedom to self-express and identify their own real interests are severely hampered by authoritarian pressure. Moreover, any channels or frameworks for communication might be tainted by Soviet-like interference from the state apparatus. One should also keep these conditions in mind when forced into conversations with representatives of the Russian regime, for they are the ones who are responsible for the current predicament of Russian society.

## References

- Borrell, J. (2021). How to deal with Russia? EEAS blog, 28 June. [https://eeas.europa.eu/headquarters/headquarters-homepage\\_en/100901/How%20to%20deal%20with%20Russia](https://eeas.europa.eu/headquarters/headquarters-homepage_en/100901/How%20to%20deal%20with%20Russia). Accessed 13 July 2021.
- Domanska, M. (2021). How the EU can engage Russian civil society. *Carnegie Europe*, 29 June. <https://carnegieeurope.eu/strategieurope/84858>. Accessed 13 July 2021.
- European Commission. (2021). *Joint communication on EU–Russia relations: Push back, constrain and engage*. Communication, JOIN (2021) 20 final, 16 June. [https://ec.europa.eu/info/files/joint-communication-eu-russia-relations\\_en](https://ec.europa.eu/info/files/joint-communication-eu-russia-relations_en). Accessed 13 July 2021.
- European Council. (2021). European Council meeting (24 and 25 June 2021) – Conclusions. EUCO 7/21, 25 June. <https://www.consilium.europa.eu/media/50763/2425-06-21-euco-conclusions-en.pdf>. Accessed 14 July 2021.
- Fleming, S., Pop, V., Khan, M., Peel, M., & Foy, H. (2021). Berlin and Paris propose reset for EU relations with Moscow. *Financial Times*, 23 June. <https://www.ft.com/content/03528026-8fa1-4910-ab26-41cd26404439>. Accessed 13 July 2021.
- Foy, H. (2021). Vladislav Surkov: ‘An overdose of freedom is lethal to a state’. *Financial Times*, 18 June. <https://www.ft.com/content/1324acbb-f475-47ab-a914-4a96a9d14bac>. Accessed 13 July 2021.
- Goble, P. (2021). Kaliningrad elites selling out Russia for German money, Shulgin says. *Window on Eurasia*, 21 June. <http://windowoneurasia2.blogspot.com/2021/06/kaliningrad-elites-selling-out-russia.html>. Accessed 13 July 2021.
- Kolesnikov, A. (2021). Похороны Сталина – продолжение. Как память о войне и репрессиях превратилась в два разделяющих дискурса. *Carnegie Moscow*, 28 June. <https://carnegie.ru/commentary/84853>. Accessed 13 July 2021.

- Коммерсантъ*. (2021). Обзор с пристрастием. 16 June. <https://www.kommersant.Ru/doc/4857301>. Accessed 13 July 2021.
- Lavrov, S. (2021). The law, the rights and the rules. *Russia in Global Affairs*, 28 June. <https://eng.globalaffairs.ru/articles/the-law-the-rights-and-the-rules/>. Accessed 13 July 2021.
- Lemon, J. (2020). 45 percent of Russians support anti-Putin protests while just 17 percent oppose demonstrations: Poll. *Newsweek*, 28 July. <https://www.newsweek.com/45-percent-russians-support-anti-putin-protests-while-just-17-percent-oppose-demonstrations-poll-1521078>. Accessed 26 August 2021.
- Levada Center*. (2020). Gordost i identichnost. 19 October. <https://www.levada.Ru/2020/10/19/gordost-i-identichnost/>. Accessed 13 July 2021.
- Levada Center*. (2021a). Russia and Europe. Press release, 22 March. <https://www.Levada.ru/en/2021/03/22/russia-and-europe/>. Accessed 13 July 2021.
- Levada Center*. (2021b). Самые выдающиеся личности в истории. 21 June. <https://www.levada.Ru/2021/06/21/samye-vydayushiesya-lichnosti-v-istorii/>. Accessed 13 July 2021.
- Meduza*. (2021). Intolerable competition: What fuels the Russian authorities' perpetual legitimacy crisis. 25 June. <https://meduza.io/en/feature/2021/06/25/intolerable-competition>. Accessed 13 July 2021.
- Official Journal of the European Communities. (1997). *Agreement on partnership and cooperation*. OJ L327 (28 November), 3. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A21997A1128%2801%29>. Accessed 26 August 2021.
- Parfitt, T. (2021). Vladimir Putin bans comparisons between Soviets and Nazi Germany in Second World War. *The Times*, 1 July. <https://www.thetimes.co.uk/article/vladimir-putin-bans-comparisons-between-soviets-and-nazi-germany-in-second-world-war-wtdtw6g9n>. Accessed 13 July 2021.
- Prokofief, D. (2021). Федерация Трех толстяков. Новая газета. *Novaya Gazeta*, 16 June. <https://novayagazeta.ru/articles/2021/06/16/federatsiia-trekh-tolstiaikov>. Accessed 13 July 2021.
- RTVI Новости*. (2021). Наталья Зубаревич: когда государство пугается, оно начинает немножко доить // Вы держитесь! YouTube, 29 May. <https://www.youtube.com/watch?v=KbQEzU3XxPg>. Accessed 13 July 2021.
- The Moscow Times*. (2021). 7 in 10 Russians support reviving 'Gulag' prison labor—Poll. 1 June. <https://www.Themoscowtimes.com/2021/06/01/7-in-10-russians-support-reviving-gulag-prison-labor-poll-a74068>. Accessed 13 July 2021.
- Tkachev, I. (2021). The X-files: How the Russian state is creeping underground. *Riddle*, 1 June. <https://www.ridl.io/en/the-x-files-how-the-russian-state-is-creeping-underground/>. Accessed 13 July 2021.

## Author biography



**Robert Pszczel** is a Senior Fellow with the Pulaski Foundation, Warsaw. He is a former diplomat and NATO official; he served as Director of the NATO Information Office in Moscow in the period 2010–15.



# The democratic deficit of the EU: Breaking the spell of a false analogy

European View  
2021, Vol. 20(2) 226–233  
© The Author(s) 2021  
DOI: 10.1177/17816858211069701  
journals.sagepub.com/home/euv



**Svetoslav Malinov**

## Abstract

The article contains a critique of the concept of the democratic deficit of the EU. Its logical unsustainability is revealed by demonstrating that it is based on the ‘fallacy of false analogy’. Several of the numerous implications of this assertion are elaborated, with a special emphasis on the ‘no-demos thesis’. The article does not treat the idea of the democratic deficit of the EU merely as an analytical concept that is based on a false analogy and thus logically incorrect. For the concept has been persistently used in political debates as one of the most destructive tools against the EU. The concluding section contains a radical proposal for a counter-offensive in favour of European integration.

## Keywords

EU, Democratic deficit, Fallacy of false analogy, Brexit, Input–output legitimacy

## Introduction

Brexit has caused a major crisis for the EU; for the first time a member state has withdrawn from the Union. The widespread perception of the ‘democratic deficit of the EU’ (DDEU) was an implicit precondition for the persuasiveness of the major messages of the successful Brexit campaign in June 2016 (Beetz 2018, 339). Within that context, any grievance could easily be transformed into a rejection of the EU as a whole. At the heart of this lasting legitimacy crisis is the powerful image of the allegedly distant, uncontrollable and undemocratic Brussels. The concept of the DDEU was the stepping-stone for the various versions of the ‘taking back control’ slogan that was the most effective message of the Brexit campaign. If the degree to which the EU was deemed a legitimate

---

### Corresponding author:

S. Malinov, Sofia University, ‘St. Kliment Ohridski’, 15 „Tsar Osvoboditel” Bul, Sofia 1000, Bulgaria.  
Email: smalinov@mail.bg

**[AQ: 1]**

democratic decision-maker had been higher, then the majority would have voted to remain in the EU (Beetz 2018, 340).

The article contains a critique of the DDEU, interpreted as an umbrella concept that covers a wide range of accusations made against the EU that relate to it being not democratic, or insufficiently so. The logical unsustainability of the concept of the DDEU is revealed by demonstrating that it is based on the ‘fallacy of false analogy’. The article elaborates on several of the numerous implications of this assertion, which is connected with the interpretation of the EU as a *sui generis* polity. Special emphasis is placed on the ‘no-demos thesis’ as undermining any argument that the EU is undemocratic. The DDEU is not treated merely as an analytical concept that is based on a false analogy and thus logically incorrect; for it has been persistently used in political debates as one of the most destructive tools against the EU. The concluding section contains a practical proposal for a counter-offensive in favour of European integration.

## Defining the concept of a democratic deficit

There is no deficit in the number of publications on the DDEU.<sup>1</sup> Although hard to prove, it is easy to agree that ‘more ink has been spilt in recent years over the issue of the democratic deficit in the EU than just about any other problem’ (Schmidt 2005, 767). The remarkable diversity of the literature on the subject is characterised by deep disagreement. Although there are influential voices stating the opposite, the overwhelming majority of scholars shares the basic intuition that ‘something is rotten’ with the state of democracy in the EU. It is impossible to underestimate the influence of such a widespread perception, since the affirmation of democracy permeates all aspects of European integration. The Copenhagen criteria that define whether a country is eligible to join the EU require that a state has the institutions to preserve democratic governance and human rights. The Lisbon Treaty contains several passages (arts. 2, 10 and 21, among others) underlining the fundamental importance of democracy for the Union. Beyond the normative level, we can discern a pragmatic argumentation: an organisation such as the EU should be democratic in order to exist and survive. Only democratic legitimacy can guarantee efficiency and stability. As a union of democratic states, its citizens would simply not put up with the EU if it was not democratic.

Criticism of the democratic deficit has always accompanied the process of European integration. This criticism first arose with the marginalisation of the national parliaments as a result of the powers attributed to the European Parliament (EP) and to the European Commission, which was viewed as an executive body consisting of technocrats who lacked democratic legitimacy. More recently, this criticism has been focused on the leading role of the Commission and the determining powers assumed within it by the stronger member states. Even more recently still, the European Central Bank has come in for criticism, accused of widening its scope of action in a regime of virtual unaccountability (Amato et al. 2019, 164). Majone, one of the leading scholars on the DDEU, summarises this process by distinguishing two levels in the use of the term: first, the DDEU as ‘an incomplete development of the institutions, policies, and political processes that we take

for granted in a representative democracy' and, second, the DDEU as 'a set of problems that arise whenever important policymaking powers are delegated to politically independent bodies' (Majone 2005, 37). In the second sense he refers to the 'legitimacy problem of nonmajoritarian institutions', that is, institutions exercising important public functions without being directly accountable to the voters or to their elected representatives (Majone 2005, 38). Obviously, the European Central Bank and the European Commission are again the main culprits in this respect.

### The fallacy of false analogy

The concept of the DDEU is based on an analogy that likens the EU to a modern democratic state (MDS). This analogy is thought to be a powerful mechanism for the acquisition of new knowledge and conceptual change (Blanchette and Dunbar 2002, 672). Two subjects can be considered analogous if they share a common pattern of relationships among their constituent elements, even if the elements themselves differ across the two subjects. Typically, one analogue, termed the *source*, is older, familiar and better understood than the second, less familiar analogue, termed the *target*. In our case, the process of analogical reasoning starts with the MDS as the source and focuses on the EU as the target.

This difference in initial knowledge provides the basis for analogical transfer, using the source to produce inferences about the target (Holyoak 2012, 117). Analogical reasoning goes beyond the initial information, using systematic connections between the source and the target to formulate plausible inferences about the latter. The main stages involved in analogical reasoning are usually described as encoding, retrieval and mapping. Among those different stages, 'mapping is often considered to be the crux of analogical reasoning' (Blanchette and Dunbar 2002, 672). This is because mapping is 'the stage at which knowledge about the source is carried over to the target' (Blanchette and Dunbar 2002, 673). In the ideal case scenario, by mapping from a source to a target problems can be solved, and well understood cases can provide the basis for understanding processes in new domains.

However, what if the very process of mapping turns out to be the source of confusion and instead of solving real problems creates imaginary unsolvable ones (Tversky and Kahnemann 1983)? I believe this is the case in the analogical reasoning which positions the MDS as a source and the EU as a target. In his work *A System of Logic* (1843), the classic political philosopher J. S. Mill identifies this kind of confusion as the fallacy of false analogy. For Mill, an argument from analogy 'is an inference that what is true in a certain case is true in a case known to be somewhat similar, but not known to be exactly parallel, that is, to be similar in all the material circumstances' (Mill 1882, 968). An object (O1) has the property A; another object (O2) is not known to have that property, but resembles O1 in property B; thus the conclusion to which the analogy points is that O2 has property A also. Resemblance in one point is inferred from resemblance in another point, even though there is not only no evidence to connect the two circumstances by way of causation, but the evidence positively tends to disconnect them. This is 'the Fallacy of False Analogy', concludes Mill (1882, 970).

The main example that Mill chooses for illustration is heavily political; it is ‘that favourite argument in defence of absolute power’, drawn from the analogy of paternal government in a family, which is not and cannot be controlled by the children themselves (Mill 1882, 970). Paternal government, says the argument, works well; therefore, despotic government in a state will also work well. There is no doubt that irresponsibility, that is, a lack of control, is a common circumstance of both governments. However, it is wrong to suppose that the affection of the parent to the children, and the superiority of the parent in wisdom and experience are reproduced automatically in the relations between a political despot and his subjects. ‘When either of these circumstances fails even in the family and the influence of the irresponsibility is allowed to work uncorrected, the result is anything but good government’ (Mill 1882, 970). This, therefore, is a false analogy.

Although much more sophisticated and comprehensive, the DDEU argument is in essence a fallacy of false analogy *à la* Mill. An object (in our case the polity of the MDS) has democratic institutions and procedures providing democratic legitimacy; another object (the more complex polity of the EU) resembles the MDS in numerous respects: both have a territory, flag, hymn and currency; a central bank; executive, legislative and judiciary branches of government; rights and freedoms for citizens, and so on. Therefore, the EU is expected to have democratic institutions and procedures, providing democratic legitimacy.

## The use and abuse of the concept of the DDEU

The inevitable conclusion after the rejection of the analogy between the MDS and the EU is to affirm that the latter is a polity *sui generis*. Numerous scholars have developed arguments in this regard.<sup>2</sup> Although there is no consensus on what is at the core of the EU’s uniqueness, the no-demos thesis seems to be most easily accepted (Weiler 1995). According to it, the European polity lacks a (single) demos, and thus lacks a common public sphere, civic identity and public discourse. Democratic theory treats the existence of a demos as a given; its identity should be partially defined by the boundaries of the MDS itself (Maenent 1997, 92–5). The concept of democracy is meaningless without the claim that the government should be accountable and responsible to a given people, elected and controlled by it, obliged to serve its interests and so on. The DDEU concept requires the presence of a European demos in order to trigger the argument that the polity of the EU fails to represent it. No demos means there is no way to identify a democratic deficit whatever the polity. No European demos therefore means there is no way to prove the existence of the DDEU.

In addition to the no-demos thesis, the *sui generis* school has highlighted numerous differences between the MDS and the EU. Phillippe Schmitter offers an extensive list of the features of the MDS that the EU does *not* possess, starting with a ‘locus of clearly defined, supreme authority’ and ending with the ‘capacity for controlling the movement of goods, services, capital, and persons within its borders’ (Schmitter 2000, 160–1). These fundamental structural differences demonstrate how irrelevant the traditional

yardstick of modern democratic theory is. The new European polity is not based on a community with a common identity that would require a process of self-government by political equals; accountability and representation can be meaningful only if the identity problem is solved (Zürn 2000, 188). The EU is a polycentric multilevel power arrangement that is still in the process of formation. We do not know where the inevitable transformations will lead the EU and its institutions. There is a possibility that the Union may evolve in the direction of a federal state. The closer it gets to that, the more relevant the requirements of traditional democratic theory will be. However, this is just a distant possibility and a very unlikely one. The proponents of the concept of the DDEU extrapolate to the EU characteristics that still do not exist and will probably never come into existence in the future. As a result, they severely criticise the EU as undemocratic as if it is a sovereign state with a parliamentary democracy.

The DDEU argument creates false expectations nurturing false solutions. The principal expectation is the idea that deficits can be reduced, balanced and finally overcome; this presupposes the existence of a standard, a norm or an ideal. The urge to construct such a 'democratic optimum' seems to be irresistible (Decker 2002, 256) and, whether successful or not, is usually followed by ambitious proposals for institutional reforms. A stronger EP and a more transparent European Council are the reforms that have been proposed ad nauseam. Some have even proposed the creation of a pan-European public sphere as the first step to creating a 'euro-demos' (Habermas 2008, 131–8). From this perspective the problem seems to be solvable and transitory; hence the belief that sooner or later the inventiveness of scholars and the goodwill of politicians will result in the end of the DDEU. These false hopes are potentially destructive since the issue is more fundamental and may turn out to be more enduring.

Since its birth in ancient Greece, the idea of democracy has always been connected with a particular polity. The MDS is the latest of these polities and its representative model of mass democracy differs substantially from the limited and direct model of the *polis*. Democracy cannot be detached from the institutions and the socio-cultural and socioeconomic prerequisites that made it possible in a given historical context (Greven 2000). There is no 'pure' or 'essentialist' notion of democracy that can exist independent of its empiric manifestations. At present, political science cannot provide a theory of democracy that is not based on preconditions rooted in the modern nation state. It is fair to hypothesise that it may be impossible to achieve such a level of abstraction. What we know for sure is that a democratic model dissociated from the MDS does not exist and its construction is at best in the initial stages. There is no doubt that in the age of globalisation we desperately need a new theory of democracy for polities without a single demos, fixed territory or unchallenged sovereignty. However, there is no guarantee that such a brave and utterly novel undertaking can be accomplished.

It was Thomas Hobbes who wrote that if it were to be entangled with politics even the doctrine that the three angles of a triangle should be equal to the two angles of a square would have been suppressed (Hobbes 1998, 70). Stepping outside the academic

debates about the DDEU, we can observe a striking contrast between its logical weakness and theoretical vulnerability, on the one hand, and its popularity and widespread application, on the other. Is this asymmetry simply due to an inaccurate scientific argument fading away too slowly? No, it is about politics. If not recognised and dismantled as a fallacy of false analogy, the DDEU argument is transformed into a formidable political weapon. So, to update Hobbes, if there are political interests at stake then it is no surprise that the enemies of the EU adore approaching its numerous problems from the perspective of the democratic deficit. The users and abusers of the DDEU concept will never be concerned with its scientific status. No wonder they are victorious in political debates—there is simply no way to prove that the EU is as democratic as or more democratic than the MDS.

## Conclusion

Once accepted as admissible, the comparison between the MDS and the EU in terms of democracy will always end up affirming the existence of the DDEU. Instead of being exposed as a logical fallacy, it becomes a deadly political trap for the supporters of European integration. After surrendering to the assumption that the EU is not democratic enough in comparison with the MDS, they seek consolation in the argument that the DDEU is a temporary predicament that can be overcome through serious institutional reforms. This claim demands concrete proposals for reforms that are open to all kinds of criticism, along with the possibility of simply being rejected by national governments. There is always the hope of a trickle-down effect from the high scientific level to popular understanding that will bring to light the fundamental weaknesses of the concept of the DDEU. However, this may take decades; in the meantime the political advocates of the idea of the DDEU will continue their destructive work.

The proposal that was promised at the beginning of this article addresses the question of what is to be done to neutralise the harmful effects of this deplorable situation. It can be articulated most clearly using the terms of Fritz Scharpf (1997): *input* and *output* legitimacy. For him, democracy is a two-dimensional concept, relating to the inputs and the outputs of the political system at the same time. On the input side, democracy requires that political choices should be derived, directly or indirectly, from the authentic preferences of citizens; on the output side, it implies effective control and achievements. Thus, input-oriented authenticity and output-oriented effectiveness are equally essential elements of democratic self-determination (Scharpf 1997, 19–20). The fundamental weakness of the input structures of the EU is the alpha and omega of any DDEU debate. It has been demonstrated that we still do not possess a normative theory of input legitimacy for the *sui generis* polity of the EU—at best such a theory is in the initial stages of construction.

The essence of this practical proposal is that the advocates of the EU should avoid the minefield of input issues and decisively move in a different direction; their focus should be exclusively on improving and promoting output-oriented effectiveness as a precondition for asserting the output legitimacy of the EU. Input-oriented debates should be

avoided and deconstructed. They lead to battles, the result of which is predetermined by the false analogy between the MDS and the EU that is dominated by the concept of the DDEU. The best outcome that the pro-EU side can achieve is to lose with dignity. The constant stream of proposals for institutional reforms to overcome the DDEU should stop—there are no standards to evaluate them by and no precedents to refer to. If this is the case then we have to admit that in spite of the good intentions behind such proposals, there is a possibility that their realisation could make the EU even less legitimate. By ending this constant stream of proposals, enormous amounts of misdirected financial resources, intellectual efforts and political energy will be saved. It is time to break the spell of the DDEU argument and put an end to the conceptual tyranny of its numerous false dilemmas. The defence of the EU should be built on the much more reliable foundation of output legitimacy by recognising and promoting the unique public goods that only the Union can provide.

## Notes

1. As an introduction to the DDEU discussion, see Majone 1998; Føllesdal 2006; Moravcsik 2002; and Zweifel 2002.
2. For additional analyses of the EU as a polity *sui generis*, see Beetham and Lord 1998; Bellamy and Castiglione 1998; Decker 2002; Weiler 1995; and Zürn 2004.

## References

- Amato, G., Moavero-Milanesi, E., & Pasquino, G. (eds.) (2019). *The history of the European Union: Constructing utopia*. Portland, OR: Bloomsbury.
- Beetham, D., & Lord, C. (1998). *Legitimacy and the EU*. New York: Longman.
- Beetz, J. P. (2018). From practice to principle and back: Applying a new realist method to the European Union's democratic deficit. *Political Studies*, 66(2), 339–55.
- Bellamy, R., & Castiglione, D. (1998). The normative challenge of a European polity: Cosmopolitan and communitarian models compared, criticized and combined. In: A. Føllesdal & P. Koslowski (eds.), *Democracy in the European Union* (pp. 254–84). Berlin: Springer.
- Blanchette, I., & Dunbar, K. (2002). Representational change and analogy: How analogical inferences alter target representations. *Journal of Experimental Psychology*, 28(4), 672–85.
- Decker, F. (2002). Governance beyond the nationstate: Reflections on the democratic deficit of the European Union. *Journal of European Public Policy*, 9(2), 256–72.
- Føllesdal, A. (2006). The legitimacy deficits of the European Union. *Journal of Political Philosophy*, 14(4), 441–68.
- Greven, M. (2000). Can the European Union finally become a democracy? In: M. T. Greven & L. W. Pauly (eds.), *Democracy beyond the state? The European dilemma and the emerging global order* (pp. 35–62). Lanham, MD: Rowman and Littlefield.
- Habermas, J. (2008). *Europe: The faltering project*. Cambridge: Polity Press.
- Hobbes, T. (1988). *Leviathan*. Oxford: Oxford University Press.
- Holyoak, K. J. (2012). Analogy and relational reasoning. In: K. J. Holyoak & R. G. Morrison (eds.), *The Oxford handbook of thinking and reasoning* (pp. 234–59). Oxford: Oxford University Press.
- Majone, G. (1998). Europe's democratic deficit. *European Law Journal*, 4(1), 5–28.
- Majone, G. (2005). *Dilemmas of European integration: The ambiguities and pitfalls of integration by stealth*. Oxford: Oxford University Press.

- Manent, P. (1997). Democracy without nations? *Journal of Democracy*, 8(2), 92–102.
- Mill, J. S. (1882). *A system of logic ratiocinative and inductive, being a connected view of the principles of evidence, and the methods of scientific investigation*. New York: Harper & Brothers.
- Moravcsik, A. (2002). Reassessing legitimacy in the European Union. *Journal of Common Market Studies*, 40(4), 603–24.
- Scharpf, F. W. (1997). Economic integration, democracy and the welfare state. *Journal of European Public Policy*, 4(1), 18–36.
- Schmidt, V. A. (2005). Democracy in Europe: The impact of European integration. *Perspectives on Politics*, 3(4), 761–79.
- Schmitter, P. C. (2000). *How to democratize the European Union – And why bother?* Lanham, MD: Rowman and Littlefield.
- Tversky, A., & Kahneman, D. (1983). Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment. *Psychological Review*, 90(4), 293–315.
- Weiler, J. H. H. (1995). Does Europe need a constitution? Demos, telos and the German Maastricht decision. *European Law Journal*, 1(3), 219–58.
- Zürn, M. (2004). Global governance and legitimacy problems. *Government and Opposition*, 39(2), 260–87.
- Zweifel, T. D. (2002). Who is without sin cast the first stone: The EU's democratic deficit in comparison. *Journal of European Public Policy*, 9(5), 812–40.

### Author biography



**Svetoslav Malinov**, Ph.D., is Associate Professor and Head of the Department of Political Science at the Faculty of Philosophy, Sofia University St. Kliment Ohridski. He is also a former Member of the European Parliament with the European People's Party Group from Bulgaria.

# Another article on the Strategic Compass (kind of)

European View  
2021, Vol. 20(2) 234–236  
© The Author(s) 2021  
DOI: 10.1177/17816858211062490  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)  


**George Pepios**

An unconfirmed anecdote is doing the rounds following the informal European Council meeting in Slovenia at which leaders laid out their cards on EU defence cooperation. Whilst leaders were leaving what Dutch Prime Minister Mark Rutte called a ‘brainstorming debate’ (Herszenhorn and Bayer 2021) in the early hours of the morning, one member asked another if she had understood in which direction they (i.e. the Union) are going. Slightly bemused, her counterpart answered, ‘Who cares about the direction?’ To which the former replied, ‘The Compass does . . .’.

Indeed, the Strategic Compass has been asked to provide direction—more specifically to ‘narrow the gap between ambition and reality’ and ‘clarify the overall image of EU defence cooperation’ (Nováky 2020, 1). Savvy EU observers, security experts and flag-waving federalists were waiting for Mr Josep Borrell (the EU’s *almost* foreign minister) to present the first results of this two-year process just as the Israelites of old looked to Moses to lead them out of Egypt. Expectations were high! How could it not be so? The EU’s very own yes-man, President Charles Michel, has declared 2022 the ‘year of European Defence’ (Herszenhorn 2021).<sup>1</sup> The stars are aligning! The brave European seafarers are reaching Ithaca. But hold on a moment. . . What if the EU’s very own North Star turns out to be not so bright after all?

It is such a shame that we only talk about ‘bubbles’ when we discuss the economy and the financial world, as I cannot find a more appropriate word to describe the hype around the Strategic Compass. It brings to mind the same frenzy that engulfed another catchphrase in the ‘strategic’ family—a muted one, of course, as thankfully EU current affairs have not reached mass popularity status (yet). The difference is that this time around what is described as ‘strategic’ is a compass: a reliable, solid and tested navigation device that has been showing the way since time immemorial. (Well, since the Chinese Han

---

**Corresponding author:**

G. Pepios, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1st floor, B-1000 Brussels, Belgium.

Email: [gp@martenscentre.eu](mailto:gp@martenscentre.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

Dynasty around 206 BC. But please keep this to yourself, dear reader, because the fact that it was not made in Europe will not resonate very well with Berlaymont.) It has little in common with its perplexing, ambiguous and contested predecessor, *strategic autonomy*.

There is a very real threat (pun intended) that the Strategic Compass will end up being a real-life version of the compass the irreverent *Pirates of the Caribbean* protagonist Jack Sparrow held, which always pointed in the direction he wanted.<sup>2</sup> In that situation the perception of a threat becomes a self-fulfilling prophecy. But reaching that stage is another brain teaser altogether. The EU's very own Moses, Mr Borrell, caught wind of this when he famously told the leaders in that same meeting (at which everything and nothing seemed to happen), 'We need to know what we want' (Herszenhorn and Bayer 2021). There is nothing new or ground-breaking to report here, as the divergent strategic cultures in Europe keep being referenced as the only impediment to developing a common defence union (Zandee et al. 2020). One could even say that there is a certain bravery (or, for the cynics amongst us, a certain quixotism) attached to this statement, as it presupposes that 'we' (all the 27) have a common 'want' in the security and defence domain. This is precisely the source of the problem that the Compass has been tasked with circumventing: there is no consensus among the member states as to what constitutes a threat to the EU's security (Fiott 2020). How do you bring together those still lamenting the 'threat from the East'; the ones dreading 'the threat from within'; and finally, those concerned about the threat from above and beyond? That is the million-dollar question that the Compass has been tasked with answering.

To tighten this Gordian knot even more, in typical EU manner the Compass will almost certainly, 'for economic and political reasons' (Fiott 2020, 8), shy away from labelling specific countries as threats. For many member states, however, the threats they are facing have a name and a clear source: usually a dying democracy in the neighbourhood or a dictatorial adversary on the loose. It is certain that they will be seeking validation from their European brethren and a sense of recognition that goes beyond the longstanding policy of the 'sympathy rub' and a sterile statement that the EU is 'extremely/deeply/gravely concerned' (Is EU Concerned? 2021). Looking back at my school hiking years, which was the first and last time I held a compass in my hands, the magnetic needle did not tell me much: it was vague, abstract and unhelpful—and I would inevitably resort to the more accurate Google Maps application I had downloaded onto my phone. I guess we will have to wait and see whether the member states follow in the footsteps of my teenage self and end up doing their own thing, leaving the Compass forgotten in the background, persistently and continuously pointing north.

## Notes

1. N.B. The European Commission has also declared 2022 to be the 'year of European Youth'. Despite being a 24-year-old who gets a bit excited whenever the words 'European', 'Defence' and 'Union' are placed next to each other, I cannot but think that both of these titles are rather ambitious.
2. With thanks here to Álvaro de Cruz for brushing up my Disney knowledge!

## References

- Fiott, D. (2020). *Uncharted territory? Towards a common threat analysis and a Strategic Compass for EU security and defence*. EU Institute for Security Studies, Brief 16. [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2016%20Strategic%20Compass\\_0.pdf](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2016%20Strategic%20Compass_0.pdf). Accessed 26 October 2021.
- Herszenhorn, D. (2021). Charles Michel declares 2022 'year of European defense'. *Politico*, 2 October. <https://www.politico.eu/article/charles-michel-declares-2022-year-of-european-defense/>. Accessed 26 October 2021.
- Herszenhorn, D., & Bayer, L. (2021). For EU leaders, 'Strategic Compass' points in different directions. *Politico*, 6 October. <https://www.politico.eu/article/eu-leaders-strategic-compass-different-directions/>. Accessed 26 October 2021.
- Is EU Concerned? (@ISEUConcerned). (2021). *Twitter account*. <https://twitter.com/ISEUConcerned>. Accessed 26 October 2021.
- Nováky, N. (2020). *The Strategic Compass: Charting a new course for the EU's security and defence policy*. Wilfried Martens Centre for European Studies, Policy Brief. Brussels, 19 December. [https://www.martenscentre.eu/wp-content/uploads/2020/12/CES\\_POLICY-BRIEF\\_TheStrategicCompass-V1.pdf](https://www.martenscentre.eu/wp-content/uploads/2020/12/CES_POLICY-BRIEF_TheStrategicCompass-V1.pdf). Accessed 26 October 2021.
- Zandee, D., Deen, B., Kruijver, K., & Stoetman, A. (2020). *European strategic autonomy in security and defence: Now the going gets tough, it's time to get going*. Clingendael Report. [https://www.clingendael.org/sites/default/files/2020-12/Report\\_European\\_Strategic\\_Autonomy\\_December\\_2020.pdf](https://www.clingendael.org/sites/default/files/2020-12/Report_European_Strategic_Autonomy_December_2020.pdf). Accessed 27 October 2021.

## Author biography



**George Pepios** is the European View Research and Editor Intern at the Wilfried Martens Centre for European Studies.



# Back to Geneva: Reinterpreting Asylum in the EU

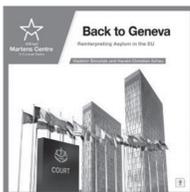
European View  
2021, Vol. 20(2) 237–238  
© The Author(s) 2021  
DOI: 10.1177/17816858211061792  
journals.sagepub.com/home/euv



**Vladimír Šimonák**  
and **Harald Christian Scheu**

The Geneva Convention, adopted 70 years ago, was created as a tool for war refugees from Europe. Only with time did the Convention lift its geographical restrictions and established a universal nature of refugee protection. Today, some blame the Geneva Convention for causing the European asylum system to be unduly permissive with regard to access to asylum and other aspects of international protection. Based on an analysis of relevant case law and international comparisons, the paper asserts that the Geneva Convention itself cannot be linked to certain overly generous interpretations and that such an outcome was not intended by the framers of the Convention. Rather, supplementary judicial and legislative interpretations, which have accumulated over decades, have caused Europe's asylum system to become permissive in certain aspects, compared to those of other major democratic jurisdictions. The paper offers several alternative views on how one may assess the differences in interpretations of the Geneva Convention between the EU, on the one hand, and Australia, the US and Canada, on the other. An examination of these differing perspectives allows us to advance operational efficiency of the EU's asylum system by moving it closer to the original intention of the Geneva Convention.

## Author biographies



**Vladimír Šimonák** is currently head of the Crisis Management Unit at the Slovak Ministry of Foreign Affairs. Between 2008 and July 2021 he was with the Slovak Ministry of the Interior. In 2011 he assumed responsibility for the last-mentioned ministry's European policies and was posted to Brussels in 2015. A graduate of law and international relations, he has developed expertise in the European politics of migration and asylum.

## Corresponding author:

V. Šimonák, Ministry of Foreign and European Affairs of the Slovak Republic, Hlboká cesta 2, 833 36 Bratislava 37, Slovak Republic.  
Email: vladimir.simonak@mzv.sk



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

---

**Harald Christian Scheu** is a lecturer in European law and public international law at the Faculty of Law of Charles University in Prague and the Police Academy of the Czech Republic in Prague. He conducts research in the fields of international migration law and international human rights law. Since 2013 he has been a member of the Council of the Government of the Czech Republic for Human Rights, and since 2014, a member of the Czech Government's Legislative Council.



# Qualified Majority Voting in EU Foreign Policy: Make It So

European View  
2021, Vol. 20(2) 239  
© The Author(s) 2021  
DOI: 10.1177/17816858211061837  
journals.sagepub.com/home/euv

## Niklas Nováky

This paper makes a case for extending qualified majority voting (QMV) to the EU’s Common Foreign and Security Policy (CFSP), the Union’s main framework for collective external action. Although many EU capitals are unwilling to move away from unanimity in decision-making on CFSP, the paper argues that the benefits of introducing some QMV to this intergovernmental domain outweigh the costs. QMV would boost the resilience of the EU’s foreign-policy system to third-country influence, facilitate the emergence of a common strategic culture among the member states and mitigate the risk that the tone of common European foreign policy is set in various mini-lateral forums outside the EU. The Lisbon Treaty contains a built-in safety mechanism that is designed to ensure that no member state could be dictated to on issues vital to its national interests if QMV were to be used in CFSP. Initially, QMV should be extended only to the adoption of EU statements on international human rights questions. Although a modest step, this would help build trust and confidence among the member states, both towards each other and in the use of QMV in CFSP. If the experience was positive, this could create momentum for expanding QMV to additional CFSP areas later on.

## Author biography



**Niklas Nováky, PhD**, is a Senior Research Officer at the Wilfried Martens Centre for European Studies. He focuses on foreign, security and defence policy. He is also the Assistant Editor-in-Chief of the *European View*, the Martens Centre’s biannual policy journal. He is author of the book *European Union Military Operations: A Collective Action Perspective* (Routledge 2018). Dr Nováky has also published peer-reviewed articles on different aspects of EU defence cooperation in some of the most respected academic journals in the field.

## Corresponding author:

N. Nováky, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1<sup>st</sup> floor, Brussels, B-1000, Belgium.  
Email: nn@martenscentre.eu



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

# A Brussels-Based Dictatorship or a Paradise of Subsidiarity? National Prerogatives and EU Migration Policy

European View  
2021, Vol. 20(2) 240–241  
© The Author(s) 2021  
DOI: 10.1177/17816858211062320  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



## Vít Novotný

The issues of subsidiarity and member state autonomy in asylum and migration policy-making have been present in the background of the political and legal conflicts among the EU member states. This paper demonstrates that treaty provisions on subsidiarity have been ineffective as safeguards of member state autonomy on immigration and asylum. Nevertheless, the treaties do endow the members with expansive autonomy in this policy area. The paper argues that this autonomy manifests itself in two different regimes that govern decision-making: intergovernmentalism and supranational consociationalism. Outside the scope of the treaties, inter-governmentalism has been effective in preventing irregular migration movements from outside the EU territory. Within the framework of the Lisbon Treaty, member states developed supranational consociationalism, an ultra-consensual decision-making regime that was first introduced in deeply divided societies. Applying this method in the EU context, the national elites have bypassed majority voting on asylum in the Council and resorted to consensus on ‘sensitive’ matters, where it is the governments affected that decide whether a given issue is sensitive. This paper argues that the current combination of intergovernmentalism and consociational arrangements should be maintained as it upholds political peace between the members. Nevertheless, given the ongoing problems with the rule of law in the area of immigration and asylum, the European Commission should limit member states’ non-compliance with the existing legislation.

---

### Corresponding author:

V. Novotný, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1<sup>st</sup> floor, B-1000 Brussels, Belgium.

Email: [vn@martenscentre.eu](mailto:vn@martenscentre.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

### Author biography



**Vít Novotný** is a Senior Research Officer at the Wilfried Martens Centre for European Studies. He specialises in migration, asylum and border management. He has postgraduate degrees in politics, public administration, European studies and clinical pharmacy.



# Reforming the European Stability Mechanism: Too Much but Never Enough

European View  
2021, Vol. 20(2) 242–243  
© The Author(s) 2021  
DOI: 10.1177/17816858211063978  
journals.sagepub.com/home/euv



**Anna Peychev**

On 27 January 2021 the member governments of the European Stability Mechanism (ESM) signed the Agreement Amending the ESM Treaty, instituting long-awaited reforms to the EU's crisis management and financial-aid mechanism. This paper finds that the ESM Reform Treaty not only fails to address the outstanding issues in the original ESM framework, but exacerbates the status quo by further empowering the Mechanism outside the legal framework of the EU treaties. The ESM's 'peacetime powers' represent a consequential novelty in this regard. These 'powers' are in fact the ESM's own analytical capabilities, which have been extended beyond its financial-aid function and are now applicable within the bounds of the European Semester for economic governance. Perhaps worst of all, the ESM remains an extremely limited instrument, legally designed to imagine the single scenario of a sovereign debt crisis which requires disciplinary conditionality in exchange for financial aid. Future reforms are not just advisable, they are a functional necessity. It will become increasingly difficult for the ESM to exercise its new powers or provide suitable crisis management without the efficiency and legitimacy which these adjustments could confer. A compromise solution could see the ESM become its own independent technocratic institution, equally removed from the political influence of governments and the reach of the Commission. Introducing flexibility in its strict conditionality could be a matter of reinterpreting the meaning of 'sound budgetary policy' from the Court of Justice of the European Union's ruling in Pringle. Lastly, in matters of justiciability and the protection of fundamental rights, nothing prevents ESM governments from committing the activities of the Mechanism to the European Charter on Fundamental Rights or the authority of the European courts, should they wish to do so.

---

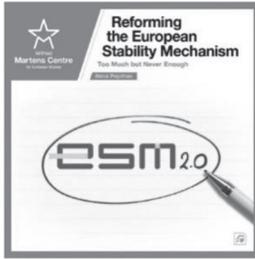
**Corresponding author:**

A. Peychev, Brussels School of International Studies, Canterbury, Kent CT2 7NZ, UK.  
Email: [ap@martenscentre.eu](mailto:ap@martenscentre.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

## Author biography



**Anna Peychev** is a visiting fellow at the Martens Centre. She is an expert on Economic and Monetary Union governance, specifically the European Semester and the European Central Bank. Dr Peychev obtained her doctorate from Kent Law School, University of Kent, with her research analysing the legislative aftermath of the EU sovereign debt crisis. She has previously earned an LLM in international law at the Brussels School of International Studies and a Bachelor's degree in international relations from the University of Calgary, Canada.



# Getting Back to Basics: Four Centre Right Steps to Economic Recovery

European View  
2021, Vol. 20(2) 244–245  
© The Author(s) 2021  
DOI: 10.1177/17816858211062328  
journals.sagepub.com/home/euv



**Eoin Drea**

Europe and the centre right simply can't afford to get this recovery wrong. The challenge is to develop a policy approach which balances the unprecedented economic circumstances arising from the pandemic with the societal demand for more inclusive growth. Only in blending these challenges into a "Middle Way" can the centre right hope to lead the economy recovery. This Policy Brief proposes four steps. (1) The unlocking of consumer spending and business investment to drive an initial economic expansion aided by tapering pandemic supports. Growth must become the immediate tool for tackling (and capping) pandemic related debt. (2) A back to basics set of priorities facilitating employment creation, affordable housing and the provision of essential public services. A 'back to basics' approach is necessary as it is the only way to deliver the payoffs needed to maintain support across a broad swathe of the middle classes. (3) A renewed commitment to reducing public debt and controlling inflation. Prolonged high inflation erodes purchasing power, particularly for those on fixed incomes or with savings. The optimal strategy for debt reduction is to keep debt levels steady initially, but then focus on slowly reducing it over time. Repairing public finances remains a marathon, not a sprint. (4) The centre right must play the long-term game because institutional reform (at both EU and national level) is about generational change, not soundbites. The European Recovery Fund is a long-term investment tool for achieving structural change, not a short-term mechanism for fiscal expansion. Europe's fiscal rules also require a more easily understood framework. The ownership of these redesigned rules should rest with member states through a more decentralised Eurozone.

---

**Corresponding author:**

E. Drea, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1<sup>st</sup> floor, B-1000 Brussels, Belgium.

Email: [ed@martenscentre.eu](mailto:ed@martenscentre.eu)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

### Author biography



**Eoin Drea, PhD**, is a Senior Research Officer at the Wilfried Martens Centre for European Studies. He is a specialist in economic and social policy. He is currently focusing on issues relating to Ireland, UK-EU relations, the Euro and the social-economic realities facing working- and middle-class families. He is a regular media contributor and his opinion pieces have appeared in *The Guardian*, *Politico*, *Euronews* and *The Irish Times* among others.



# Me, Myself and I: Could Tax Individualisation Create Jobs and Reduce Inequality?

European View  
2021, Vol. 20(2) 246–247  
© The Author(s) 2021  
DOI: 10.1177/17816858211063304  
[journals.sagepub.com/home/euv](https://journals.sagepub.com/home/euv)



**Ronald Bachmann, Philipp Jäger  
and Robin Jessen**

Throughout Europe the Covid-19 pandemic has led to lower economic growth and higher unemployment. This has resulted in a surge in public debt and an increase in gender inequalities in the labour markets of many advanced countries. This situation has stimulated interest in policies that can simultaneously boost employment, increase tax revenues and reduce labour market inequalities. This report investigates whether a move from family-based (i.e. joint) taxation to individual taxation would increase the labour supply of the lower-earning spouse (often the woman). It has often been argued that joint taxation decreases the employment of women because it increases the tax rate for the second earner. This report focuses on the situation in Germany because work disincentives for women are particularly strong in the country's tax system. However, it is likely that the conclusions will apply to other EU countries with joint income taxation, for example, France, Poland and Portugal. According to our simulations, moving to individual taxation would substantially increase the labour supply in Germany and therefore also spur economic growth. Moving to individual taxation and returning the higher tax revenues to married couples (to ensure that there are no additional budgetary costs) would increase the labour supply by more than a half million full-time equivalents. This reform would lead to a measurable increase in GDP, that is, an increase of up to 1.5%. Such a tax reform might be a way to reduce debt levels and stimulate the economy in the face of the current massive rise in public debt and decline in GDP. It could also help reverse labour market gender inequalities, which have been exacerbated by the pandemic. However, since the simulated reforms produce results that are not distributed

---

## Corresponding author:

R. Bachmann, RWI – Leibniz Institute for Economic Research, Hohenzollernstraße 1-3, D - 45128 Essen, Germany.

Email: [Ronald.Bachmann@rwi-essen.de](mailto:Ronald.Bachmann@rwi-essen.de)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

equally, ultimately a political value judgement is needed to decide whether the sizeable efficiency gains would outweigh the losses for those who would lose from the reform. Politically, the negative impact on more financially vulnerable groups may need to be addressed through further targeted tax reforms.

### Author biographies



**Ronald Bachmann** is head of the Department of Labour Markets, Education and Population at the RWI – Leibniz Institute for Economic Research and adjunct professor at the Düsseldorf Institute for Competition Economics (DICE) at Heinrich-Heine-Universität Düsseldorf.

**Philipp Jäger** is a researcher at the Department of Macroeconomics and Public Finance at the RWI.

**Robin Jessen** is a researcher at the Department of Macroeconomics and Public Finance at the RWI.

# Artificial Intelligence and Governance: Going Beyond Ethics

European View  
2021, Vol. 20(2) 248–249  
© The Author(s) 2021  
DOI: 10.1177/17816858211061791  
journals.sagepub.com/home/euv  


**Michał Boni**

Artificial Intelligence (AI) is changing our world. This new phenomenon carries many threats, but also offers many opportunities. We need to find a suitable framework to support trustworthy AI. A key challenge remains: can we, as humans, retain control over the technology or will the technology take control of humanity? In responding to this challenge, the following question needs to be considered: What kinds of tools are needed, not only to keep control of AI development, but foremost to multiply the possible opportunities it offers? The current pandemic has shown how useful and important AI can be in helping us to fight COVID-19. Moreover, it has clearly demonstrated that we cannot afford *not* to utilise it, nor do we have time to lose with regard to its development. Hence, it is our responsibility to urgently establish an adequate framework for the development of AI systems based on a revision of the existing law and followed by possible new legislative proposals with a clear focus on future-proof tools. We have to generate a suitable governance model that not only has its foundation in law, but that also ensures democratic oversight through the open and collaborative participation of all partners and the validation of AI solutions by science and society. We should build trustworthy AI based on a human-centric and principled approach. The practical implementation of ethical rules in the design of AI and the evaluation of the everyday functioning of AI systems are essential. It will not be possible to develop AI and claim all its economic and social benefits without a clear model for data use that fully respects fundamental rights and the principles of cybersecurity. It will not be possible to build trustworthy AI without transparent rules for the relationships between its users and AI designers, developers and deployers. It will not be possible to accurately implement various AI functionalities without undertaking risk assessments and introducing mechanisms to manage those

---

**Corresponding author:**

M. Boni, Wilfried Martens Centre for European Studies, 20 Rue du Commerce, 1<sup>st</sup> floor, B-1000 Brussels, Belgium.

Email: [miboni54@gmail.com](mailto:miboni54@gmail.com)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

risks. To achieve all of the above, we need compromises at various levels: between European institutions and stakeholders, between European institutions and member states, and between political groups, which are currently more focused on their differences than similarities.

### Author biography



**Dr Michał Boni, Ph.D.**, is a senior research associate at the Wilfried Martens Centre for European Studies and an assistant professor at the Warsaw University for Social Sciences and Humanities. He is a former Member of the European Parliament from Poland and a former Polish Minister of Administration and Digitisation.

