Strategic partnership for a secure and digital Europe

Forging a digitally advanced future with deepened transatlantic cooperation.

CENTER ZA EVROPSKO PRIHODNOST
CENTRE FOR EUROPEAN PERSPECTIVE
CEP

Atlantic Council

EUROPEUM
INSTITUT PRO EVROPSKOU POLITIKU
INSTITUTE FOR EUROPEAN POLICY

THE KOSCIUSZKO INSTITUTE

AI-REGULATION.COM

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

Strategic partnership for a secure and digital Europe

Forging a digitally advanced future with deepened transatlantic cooperation.

CENTER ZA EVROPSKO PRIHODNOST
CENTRE FOR EUROPEAN PERSPECTIVE
CEP

Contents

Title: Strategic partnership for a secure and digital Europe **Subtitle:** Forging a digitally advanced future with deepened transatlantic cooperation **Publisher:** CEP, Grajska cesta 1, 1234 Loka pri Mengšu **Responsible:** Katja Geršak **Editor-in-chief:** Katja Geršak **Editor:** Tine Šušteršič **Language editing:** Terry T. Jackson **Design and prepress:** Premedia, Andrej Juvan **Cover photo/photos:** Adobe Stock Photo **Print run:** 700

Ljubljana, November 2022

Introduction

The future economic development of the EU is impossible to imagine without digital transformation. As the EU strives toward its vision of a resilient, competitive, and secure digital future, the interconnected world dictates that the solutions will be most effective when reached and implemented with other international partners.

The Centre for European Perspective (CEP) has recognised this and has launched two publications highlighting the benefits of digitalisation for Central and Eastern Europe *(The Transformative Power of Digital)* and bringing regional perspectives to the fore *(Paving the Digital Path in Central and Eastern Europe)*. We strongly believe in a digitally robust EU and in creating an environment where innovation can thrive and data flow freely.

However, on Thursday, February 24, we awoke to a new European reality: one in which armed conflict is again happening, and the future seems more insecure than in previous decades. More than ever, the EU needs unity and a clear path ahead in forging together in economic and security areas. In the changed geopolitical reality, a like-minded and values-based partnership should become a priority and a strong and stable transatlantic bond and partnership are indispensable. As the EU strives toward its vision of a resilient, competitive, and secure digital future, a strategic partnership with the US should most comprehensively ensure the realisation of such a future. By combining the EU's and US's resources and commitment to human rights and democracy, we may effectively grow together and protect our economy and society from those that wish to harm us.

This publication aims to contribute to the discussion on the EU's digital future and how to best achieve it. We are thankful for contributions from prominent individuals, think tanks, and other organisations for their insightful contributions, and we find their perspectives invaluable.

In the first chapter, Théodore Christakis provides an in-depth explanation of what strategic partnership is and what it entails, as well as underscoring the need for cooperation to promote common values based on democracy, human rights, and a rules-based international system. He also highlights six mechanisms for cooperation with possible tangible results. Susan Ness takes stock of the progress of one of these mechanisms: the Trade and Technology Council (TTC). While there have been few tangible results thus far, ministerial meetings have presented trust-building opportunities, a prerequisite for a positive future outlook. Fredrik Erixon argues that transatlantic economic cooperation is unwell but that the US and the EU are in a prime position to create a new globalisation based on rules and norms that are free and fair and harness emerging trade in services, digital trade and ideas. While we often reiterate the values of democracy, the rule of law, and human rights, which the EU and the US share, Ewelina Kasprzyk, Maciej Góra, and Michał Krawczyk alert us to often overlooked values in the digital space: security, privacy, fairness, and accountability. While Western countries approach these values differently, they nevertheless still hold a united front against states that tend to use technology to exercise power in an authoritarian way. One such technology (AI), writes Gregor Strojin, is already proving to be one of the most transformative technologies in history. While the quest to set global standards for AI remains underway, the Council of Europe-led efforts with broad participation from countries like the US, Canada, and Japan shows the awareness of common goals and values. Danielle Piatkiewicz draws our attention to the need to (re)align digital policies to stop the growing regulatory divide between the EU and the US. Geostrategic region, such as Central and Eastern Europe, can, through the Three Seas Initiative, become an important vector for greater transatlantic cooperation. Finally, Susan Ness and Chris Riley present the case for modularity as an approach to multinational and stakeholder engagement in digital regulation. They argue that even small gains in alignment, measured against the massive geopolitical tensions, can deliver practical benefits in the near term and bring about a sense of unity in these troublesome times.

Katja Geršak,
Executive director of the Centre for European Perspective

A Strategic Transatlantic Partnership?

Opportunities and Hurdles for EU-US Regulatory Cooperation in the Digital Sphere

By Theodore Christakis, Professor, Chair AI-Regulation.Com, Université Grenoble Alpes, Senior Fellow, Cross Border Data Forum

In an article published in November 2021 dedicated to the important concept of 'European Digital Sovereignty', I defended the idea that the European Union (EU), beyond its regulatory action in the digital sphere, should also consider working closely on some issues with certain democracies that share several of Europe's human rights values. Paul Timmers had previously expressed this idea by talking about 'strategic partnerships' and by emphasising that Europe's quest for 'strategic autonomy' should be coupled with an awareness of 'strategic interdependence', which would:

> *…include strategic partnerships with like-minded countries, as well as efforts to push for a global consensus on issues of 'global common good,' including keeping an open internet and information exchange across the world.*

According to Timmers, strategic partnerships address the sovereignty gap by collaborating with like-minded, trusted partners in key areas. The starting point is identifying the who and what: who is 'like-minded', and what are the key areas? As he explained:

> *"Like-mindedness" is based on shared values, whether these pertain to the individual (such as respect for privacy and autonomy) or to the economy (liberal market economy) or to society and democracy (independent judiciary, freedom of expression, free elections) or to international relations (respect for the system of sovereign states and multilateralism).*[1]

This idea of 'shared values' became much stronger after the invasion of Ukraine by Russia in February 2022. In an article published shortly afterwards, Alex Joel wrote:

> *As we witness Russia's invasion of Ukraine and the world's response, I am reminded once again that what unites democracies is so much stronger than what divides us. Our common beliefs, values, and commitments shine clearly across the miles and oceans that lie between us. Yet it can be so easy to lose sight of those commonalities and become distracted by what seem now to be minor differences.*

The objective of the present paper will be to assess whether the strong alliance between the EU and the US in terms of their reaction to Russian aggression in Ukraine could, indeed, lead to a broader 'strategic partnership' that promotes certain key values in cyberspace and the digital sphere through regulatory cooperation. The first part of the article will briefly discuss some of the opportunities and hurdles involved in a strategic transatlantic partnership in the digital sphere (I). The second part of the article will attempt to identify the different mechanisms that could be used to promote regulatory cooperation in the tech sphere (II).

I. Transatlantic 'Like-mindedness'?

There is no doubt that 'like-mindedness' is a somewhat relative concept that depends on the issues and values at stake.[2] Serious disagreements about whether to regulate and how to regulate certain specific areas of the digital sphere persist between the EU and some of its closest allies, starting with the US. Such disagreements can also be linked to the broader spectrum of EU-US trade relations and interests. Bilateral trade and investment ties between the two sides are long-standing, strong, and extensive, but frictions often emerge between the partners due to the high level of bilateral commercial activity and different policy approaches to certain specific issues, including those that concern the digital sphere.

During the Trump Administration, EU-US trade ties were fraught. President Biden, however, emphasised from the outset his support for the EU and 'his commitment to repair and revitalise the U.S.-EU partnership.' In 2021, the two nations came together to address a series of issues that had provoked a great deal of friction, such as the WTO Boeing-Airbus subsidies dispute, digital service taxes, and US steel and aluminium tariffs and launched new modes of cooperation, notably the US-EU Trade and Technology Council (TTC) to which I will refer in the second part of this article.

Despite these efforts, contentious trade issues remain between the EU and the US. For instance, the US has long criticised what it considers to be EU regulatory barriers to agricultural trade. Conversely, the EU is currently upset about the US's so-called Inflation Reduction Act, which gives tax credits and financial incentives to US consumers so that they may buy greener cars that are 'made in the US'. European trade officials are angry about what they see as yet another example of American economic protectionism, which could force EU automakers to double down on their American production while harming investment and jobs within the EU.

In contrast, US officials claim that 'Brussels was on shaky ground with its accusations of protectionism given how the bloc was promoting its own "digital sovereignty" concept, which includes prioritising European alternatives to primarily American technologies'.[3] Interestingly, it is precisely the field of the digital economy that the US considers the EU to be increasingly adopting measures that mostly target US companies. Nigel Cory, of the US Information Technology and Innovation Foundation, echoed these concerns by arguing, for instance, against certain EU Member States' or even ENISA's attempts to introduce 'sovereignty requirements' and an 'immunity from non-EU laws' condition in their cloud cybersecurity certifications, by arguing that the 'EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty'.

Another area where great friction between the EU and the US exists concerns transatlantic data flows. The Court of Justice of the European Union (CJEU) issued its Schrems II judgment in July 2020, invalidating the EU/U.S. Privacy Shield and creating uncertainty about the use of Standard Contractual Clauses for transfers of personal data to third countries (see analysis here, here, here, here and here). In light of the legal uncertainty and the increasing tensions concerning transatlantic data transfers resulting from the intensification of enforcement actions by European data protection authorities (DPAs) since Schrems II (such as this and this), there was both a strong reason to reach a new EU/US agreement and also a stated willingness on both sides to do so.

In March 2022, the Presidents of the US and the European Commission jointly announced a political agreement for a new 'Transatlantic Data Privacy Framework' (TADPF) to 'foster trans-Atlantic data flows and address the concerns raised by the CJEU in the Schrems II decision of July 2020'. However, it was only six months later that the legal instruments that were intended to implement this political agreement were publicly announced. To be more specific, on October 7th, 2022, President Biden issued an 'Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities' ('EO'), and the Department of Justice supplemented this with a new regulation. As explained by the White House, 'Transatlantic data flows are critical to enabling the $7.1 trillion EU-U.S. economic relationship'. The TADPF intended to 'restore an important legal basis for transatlantic data flows' by addressing the two concerns that the CJEU raised in Schrems II, namely, on the one hand, the existence of binding safeguards that limit access to data by US intelligence authorities to what is 'necessary and proportionate' to protect national security and, on the other hand, the establishment of an independent and impartial redress mechanism, to investigate and resolve complaints that concern access to European data by US national security authorities. Max Schrems announced that he would very probably legally challenge the new arrangement. The European Commission believes that the CJEU 'will not strike down the agreement again' and intends to publish its draft adequacy decision

at the end of November. It remains to be seen whether the new arrangement will be validated by the CJEU or whether this major area of friction will remain. Indeed, the US Chamber of Commerce has warned that 'without secure data flows, meaningful progress on many other critical elements' of the EU/US cooperation agenda 'is not possible'.

Despite all these areas of friction, the EU and the US could still try to strengthen cooperation in several significant areas where convergence exists in order to promote common values based on democracy, human rights and a rules-based international system. Indeed, while waiting to converge on other issues, the EU and the US could work together on issues such as cybersecurity and resilience (including those that relate to the Internet of Things); the fight against cybercrime; the fight against illegal online content and disinformation; protection against foreign cyber interference; the protection of freedom of speech and access to information; setting global democratic standards and safeguards for access, by law enforcement and intelligence agencies, to data held by the private sector – a topic for which an extremely important process is currently underway at the OECD, as we will see; a human-centred approach to artificial intelligence; and, most importantly, an open, free and global internet, at a time when more and more firewalls are being erected, and even the architecture of the internet is being challenged by some authoritarian countries in certain standardisation bodies.

Another issue where the EU and the US seem to be in agreement concerns the need for a multi-stakeholder approach. The concept of strategic partnerships should not exclude the private sector. Tech companies should remain the principal target of global regulation so that several issues can be dealt with adequately, such as privacy and data protection; market dominance; power concentration; Zuboff's 'surveillance capitalism'; hate speech; or Commissioner Thierry Breton's accusation that they are sometimes 'too big to care'[14]. However, tech and other companies can also become, in some cases, precious allies in the promotion of values. Tech companies have, willingly or unwillingly, played a major role in the dissemination of certain European rules and values as a result of implementing, for instance, by means of the very way in which they engineer their products, the GDPR's principles of 'privacy by design' and 'privacy by default'. **Initiatives such as the Paris Call on Trust and Security in Cyberspace show how advantageous it is to have a multi-stakeholder approach to the promotion of cybersecurity and resilience.** Global companies could also play a crucial role, together with NGOs and civil society, in pressing governments to put in place effective tools, protections and safeguards when it comes to access by governmental authorities to data held by the private sector.

II. Mechanisms for Strategic Transatlantic Cooperation

Identifying key areas of convergence for EU/US cooperation in setting the rules for the digital world is one thing; trying to determine exactly how this regulatory cooperation would look is another. In this part of my article, I will attempt to briefly present at least six of the vehicles that EU/US regulatory cooperation could use in order to promote common values.

1) Bilateral Cooperation: the example of the TTC

One important vehicle of bilateral regulatory cooperation could be the Trade and Technology Council (TTC). The creation of the TTC was announced in June 2021, marking a significant step towards the reinforcement of the EU/US partnership after the 'coldness' of the Trump years. As its website announces, the different cooperation projects within the TTC are 'based on our shared democratic values, including respect for human rights, that encourage compatible standards and regulations'.

At the inaugural TTC ministerial meeting in September 2021, the US and the EU established ten working groups on various topics, including 'Technology Standards'; 'Information and Communications Technology and Services Security and Competitiveness'; 'Data Governance and Technology Platforms'; 'Misuse of Technology Threatening Security and Human Rights'; 'Export Controls'; 'Investment Screening'; and 'Promoting Small and Medium-Sized Enterprises' Access to and Use of Digital Tools' – to name just those most closely related to cyber/data issues.

More details on the work of the TTC and its working groups are provided in Susan Ness' article in the present publication. It suffices to recall here that, in the Joint Statement released after the second TTC meeting, which took place in May 2022, in Saclay-Paris, a few months after Russia invaded Ukraine, the EU and the US characterised their partnership as a 'cornerstone of shared strength, prosperity, and commitment to freedom, democracy, and respect for human rights.' They stressed that **'as recent events have proven, strong transatlantic bonds and cooperation on issues related to trade, technology, and security are more important than ever.'**

The 3rd TTC meeting will take place in Washington, DC, on December 5th, 2022. The negotiators are feeling the pressure to put aside divergences and to start 'showing results', which include announcing common action against foreign interference, greater cooperation on artificial intelligence standards/rules and other outcomes. As Susan Ness concludes in her article, 'deepening US-EU cooperation is a marathon, not a sprint'. It 'remains to be seen whether the two partners can deliver' on the lofty goals they fixed.

2) Common action in international organisations: the example of the ITU and the UN

A second vehicle for EU/US regulatory cooperation in the digital sphere is to undertake common action in order to protect shared values in international organisations. Two major recent examples could be cited in this respect.

The first is the alliance between the EU and the US in the International Telecommunications Union. This organisation, created in 1865, is the United Nations' specialised agency for information and communication technologies (ICTs). It plays a major role today in setting international standards for ICTs and has become, as Politico noted, 'ground zero in a battle for how internet networks work — everything from next-generation mobile networks to potential worldwide rules for autonomous cars'.[5] **The EU and the US have realised both the importance of the ITU and the effort of some authoritarian states, such as Russia and China, to use international standardisation organisations as a means of promoting their model of the digital world.** In a sign of successful transatlantic cooperation, the EU recently strongly supported Doreen Bogdan-Martin, the US candidate for the position of Secretary General of the ITU, who ran against a Russian candidate. The US, in return, supported Tomas Lamanauskas, the European candidate, for the post of the organisation's Deputy Secretary General. As a result, both of them won with a comfortable majority.

Another example of cooperation in international organisations is the common action of the EU and the US to promote certain human rights values in the context of the ongoing negotiations over a UN Cybercrime Convention.

On 28 February 2022, following a Russian initiative, the first session of the UN Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes began with the intention of adopting such a Convention until 2024.

The EU and the US have various important concerns in relation to these negotiations.

The first concern is about the relationship with the Budapest Convention. Russia has always refused to join the Budapest Convention against cybercrime, accusing it of having established a principle that 'might damage the sovereignty and security of member countries and their citizens' rights'. Russia's hostility to the Budapest Convention has therefore raised Western countries' fears that the initiative brought by Russia could be intended to compete with the Budapest Convention. This is why the US, the EU, and other Western countries have underlined, in many statements to the UN, their full support of the Budapest Convention.

The second concern for the EU and the US is that some UN Member States could attempt to use the UN Convention in order to call into question certain well-established principles, especially in the field of human rights. This concern has been all the greater since Russia submitted a draft convention to the United Nations that introduced no less than 23 criminal offences, some of which could be challenging in terms of human rights and freedom of expression. **The EU and the US argued that 'substantive criminal law provisions must be clearly and narrowly defined, and be fully compatible with international human rights standards'** (EU 1st Session) and that 'we should be careful not to treat traditional crimes as a 'cybercrime' merely because a computer was involved in their planning or execution' (US 1st Session). Therefore, they agreed to restrict the number of offences to cyber-dependent crimes and to a limited number of cyber-enabled crimes (US 1st Session; EU 1st Session).[6] The fourth session of negotiations will take place in Vienna at the beginning of 2023, and the EU and the US, despite their divergences on some issues, seem intent on joining forces in the defence of human rights.

3) Promoting soft law on important matters: the example of the OECD

A third vehicle of transatlantic cooperation could be the proclamation of soft law principles within certain important international institutions such as the OECD.

The recent successful conclusion of the OECD international talks on a global taxation system for tech giants is a good illustration of how some international organisations, especially the OECD, could represent the appropriate fora for addressing the complexities of certain digital regulatory projects and finding satisfactory multilateral solutions.

Another example of successful action within the OECD was the adoption, in May 2019, of the Recommendation on Artificial Intelligence (AI) – the first intergovernmental standard on AI. The recommendation aims to 'foster innovation and trust in AI by promoting the responsible stewardship of trustworthy AI while ensuring respect for human rights and democratic values'. Complementing existing OECD standards in areas such as privacy, digital security risk management, and responsible business conduct, the recommendation focuses on AI-specific issues and includes a series of principles concerning the responsible stewardship of trustworthy AI and calls on AI actors to promote and implement them. The OECD also hosts the newly launched Global Partnership on Artificial Intelligence (GPAI) in order to promote certain commonly shared values more easily and globally, such as the use of AI in a human-rights-friendly and ethical way.

The third field where the OECD is undertaking ground-breaking work, with the strong involvement of the US and the EU, is that which concerns government access to data held by the private sector. In December 2020, OECD countries quietly embarked on an unprecedented exercise to formulate common principles governing their access, for national security and law enforcement purposes, to personal data held by the private sector. The project is based on the premise that these democratic governments, despite divergences in their legal systems, share many commonalities in this area and that articulating these commonalities can help restore trust in data flows between countries but also highlight how they differ from authoritarian regimes that engage in indiscriminate access to individuals' data. After some difficulties in 2021, work on this project continued in an intensive manner, and Politico reported on October 20th, 2022, that 'there are wisps of white smoke on a deal'.[7]

4) Building multilateral ad hoc alliances: the example of using a task force to counter ransomware

Even outside the fora of existing international organisations, the US and the EU can build informal ad hoc alliances in order to act on certain important cyber/data issues. The latest example is the International Counter Ransomware Task Force (ICRTF), announced on November 2, 2022, following a meeting at the White House of the Counter Ransomware Initiative, which was established last year to strengthen global cooperation on countering ransomware attacks. The US and the EU, along with a group of 36 nations, have therefore decided to form this task force to counter ransomware attacks as part of a broader international effort to crack down on cybercriminals. The ICRTF, which will be led initially by Australia, will coordinate efforts to disrupt and counter ransomware payments, along with promoting information sharing between task force members. The ICRTF also intends to consider a model for ongoing collaboration with key private sector partners.

5) Strategic bicameralism

A fifth vehicle of regulatory cooperation could be based on a broader version of what two authors have called 'strategic bicameralism'.

Jeffery Attik and Xavier Groussot introduced this term to primarily describe:

> *A process wherein the form of legislation is first adopted by the EU (by analogy to initiating chamber of a bicameral legislature) and then 'proposed' to the US (the responding chamber) for rejection or reconciliation.*

The priority (legislative initiative) given to the EU in this 'bicameral' paradigm is without doubt due to the fact that Europeans are often those who initiate regulatory action in a series of fields in a largely unoccupied regulatory space. In her remarkable book The Brussels Effect, Anu Bradford[8] describes how the EU today 'promulgates regulations that influence which products are built and how business is conducted, not just in Europe but everywhere in the world'.

The influence of the EU in global digital regulation extends well beyond the important field of data protection as, in recent years, the EU has been at the forefront of almost all global regulatory endeavours aimed at checking the powers of digital giants. From privacy to data protection, from competition issues, to taming 'gatekeepers' and platform dominance, to protecting copyright and publishers' rights, from fighting hate speech and online disinformation to taking the lead on AI regulation, the EU has been a spectacular leader in digital regulation.

It goes without saying that if the US adopts some of the standards and rules initially proposed by the European Union, this could greatly enhance the 'Brussels effect' and help remedy several of its limitations (for instance, see here, pp. 24 ff).

Indeed, if the United States enacts legislation similar to those rules proposed for Europe, this could greatly enhance the global spread of such rules. As an example, the recent adoption of the 'Digital Services Act' by the EU, which 'sets out an unprecedented new standard for the accountability

of online platforms regarding illegal and harmful content', has led several politicians in the US to piggyback on these proposals to force the social media platforms to do more on the other side of the Atlantic. It remains to be seen whether the new EU rules in this field will influence similar regulatory developments in the US, something that might be complicated for various reasons, including the feeling that some of the EU regulatory proposals may unfairly target large US technology firms.

In Attik and Groussot's 'trans-Atlantic bicameralism' paradigm, it is the EU that takes the initiative. They note that 'the privilege of a legislative organ to initiate law-making is frequently more powerful than the subsequent right of the complementary organ to reform, endorse and ratify', but they also suggest that a positive response from the 'second' chamber (the US) could be very helpful in terms of enabling the progressive elimination of conflicts and a 'process of reconciliation'. One could argue that 'trans-Atlantic bicameralism' could also act in the opposite way, with the United States taking the lead in certain regulatory fields such as cybersecurity or protection of critical infrastructure and the

EU following suit. It remains to be seen whether 'strategic bicameralism' will work in practice, in which specific fields and in what ways. This remains nonetheless an attractive idea, showing that regulatory cooperation can also occur through parallel domestic regulatory action.

6) New Treaties: the example of law enforcement cooperation

The final vehicle that could enable an EU/US strategic partnership is the conclusion of bilateral treaties. An example that could be given here is law enforcement cooperation.

Since the 9/11 terrorist attacks, the EU and the US have negotiated at least eight binding international agreements, which include agreements on law enforcement access to data (for a presentation, see here). On September 25, 2019, the EU and the US officially started negotiations on the conclusion of yet another very important transatlantic agreement on cross-border access to e-evidence with regard to judicial cooperation in criminal matters.

As explained elsewhere, the ongoing EU-US negotiations present many challenges. However, this is a typical example of a field where transatlantic cooperation could be extremely useful, permitting the enhancement of judicial cooperation in criminal matters, the protection of human rights, the fostering of legal certainty and the avoidance of conflicts between the legal orders of different countries.

* * *

In conclusion, a wide range of mechanisms can be used to promote transatlantic regulatory cooperation in the digital sphere. The war in Ukraine has shown, once again, how important it is for the EU and the US to take the lead in promoting certain shared values, which are based on human rights, democratic accountability, and respect for the rule of law. However, several important hurdles and disagreements stand in the way of fruitful transatlantic regulatory cooperation. It remains to be seen whether the two sides will be able to find common, satisfactory solutions to these disagreements and divergent views in order to be able to fully liberate the potential of a strategic transatlantic partnership in the digital sphere.

Endnotes

1 Paul Timmers, "Challenged By 'Digital Sovereignty'", Journal of Internet Law, Vol.13, n°6, December 2019, at 15.
2 See also Paul Timmers, ibid.
3 See Barbara Moens, Mark Scott, "Von der Leyen tries to demine transatlantic trade dispute", Politico,· October 26, 2022.
4 Thierry Breton : « L'UE doit organiser l'univers numérique pour les 20 prochaines années », Le Point, September 27, 2020.
5 M. Scott, C. Goujard, "Digital great game: The West's standoff against China and Russia", Politico, September 8, 2022.
6 Many thanks to Professor Karine Bannelier for her help in drafting this passage.
7 The author serves as external consultant for the OECD Secretariat on this project. The opinions expressed here are the author's only and do not reflect the position of the OECD Secretariat or any OECD country.
8 Anu Bradford, The Brussels Effect, Oxford University Press, 2020.

Is the Glass Half Empty or Half Full?

Assessing the impact of the EU-US Trade and Technology Council in aligning Transatlantic democracies

By Susan Ness, non-resident Senior Fellow of the Europe Center of the Atlantic Council, Distinguished fellow at the Annenberg Public Policy Center of the University of Pennsylvania

Both the United States and the European Union are values-centric democracies that cherish the rule of law, voting rights, and fundamental freedoms. They enjoy thriving market-based economies and, together, compose the planet's largest economic bloc. And yet, for decades, trade and tech policy alignment has eluded these powerful partners. Will the most recent transatlantic iteration – the EU-US Trade and Technology Council (TTC) – break the mould? At the halfway mark in the Biden Administration, it's time to take stock of the progress so far. Whether there has been progress is a matter of perspective: is the transatlantic-alignment glass half empty or half full?

Resetting the tattered EU-US relationship.

The TTC is one of a series of initiatives launched by the EU and the U.S. in 2021 to reset a turbulent relationship and rebuild mutual trust after the prior US Administration.[9] Its stated purpose is to "coordinate approaches to key global technology, economic, and trade issues; and to deepen transatlantic trade and economic relations, basing policies on shared democratic values."[10]

This transatlantic interagency process was wisely designed to avoid the pitfalls of earlier negotiations – most notably the ill-fated Transatlantic Trade and Investment Partnership (TTIP), which the US and EU trade negotiators launched in 2013 but was shelved in 2017 at the start of the Trump Administration[11]; and the Transatlantic Economic Council (TEC),[12] a joint framework for advancing transatlantic economic cooperation that was launched in 2007 and, except during the Trump Administration, met annually but produced few tangible results.

By removing the most nettlesome issues from the remit of the TTC, the framers hoped to avoid the tripwires of past negotiations. Thus, off the table were contentious trade disputes, debates over pending legislation, such as the E.U.'s Digital Services Act and Digital Markets Act (to respect the regulatory autonomy of each party), and negotiations on transatlantic data transfers (addressed in a separate forum).[13]

Unlike the TTIP, the TTC was not structured as a trade negotiation, in which nothing is agreed upon until everything is agreed upon. Trade negotiations entail formal, adversarial, high-stakes discussions with a list of intractable disputes to resolve. In contrast, **under the TTC, the parties announce successes as they occur, thereby building trust and a positive outlook for future meetings.** And the TTC has spawned informal outreach between the two governments, providing a natural framework to tackle new issues as they arise.

To turbo-charge the forum, the TTC is co-chaired by three members of the Biden Cabinet: Commerce Secretary Gina Raimondo, Secretary of State Antony Blinken, and US Trade Representative Katherine Tai; on the European Commission side: Executive Vice Presidents Margrethe Vestager and Valdis Dombrovskis. The TTC meets twice a year at the ministerial level, conferring visible high-level political attention on the effort, which is accompanied by high-level pressure on staff to deliver results by the meeting deadlines. **These ministerial meetings also have presented invaluable trust-building opportunities on the margins for the co-chairs to engage in private conversations on other critical matters facing the transatlantic relationship.**

The TTC is structured around ten working groups focused on a wide-ranging agenda, each co-led by senior officials from each side of the Atlantic. Each working group is charged with an ambitious set of issues. Significant issues may be spun off into adjacent dialogues so that the working groups remain on course.

WORKING GROUPS

1. Technology Standards
2. Climate and Clean Tech
3. Secure Supply Chains
4. ICT and Services Security and Competitiveness
5. Data Governance and Technology Platforms
6. Misuse of Technology Threatening Security and Human Rights
7. Export Controls
8. Investment Screening
9. Promoting SMEs Access to and Use of Digital Tools
10. Global Trade Challenges

The TTC has made progress – even if tangible results are limited.

Clearly, the partners have spent a great deal of effort identifying areas of potential cooperation on a wide range of issues, engaging in conversations to define projects, and consulting frequently with their counterparts on areas of mutual concern, including greater coordination in plurilateral settings, such as the OECD. It's difficult to quantify the enduring impact of human relationships and trust that are nurtured through an established layered infrastructure like the TTC, but it's real. Some observers credit the TTC for expediting US and EU agreements on sanctions and export controls after Russia invaded Ukraine due to relationships previously formed through the TTC. Others argue that the outcome would have been achieved without the TTC.

In either event, **the war in Ukraine underscored on both sides of the Atlantic the urgency of achieving greater alignment on technology to demonstrate transatlantic unity and to promote democratic values as a bulwark against the malicious use of cyberspace by despotic regimes.**

EU-US collaboration was rewarded in early October by the overwhelming vote in the ITU[14] to elect American Doreen Bogdan-Martin as Secretary General of the ITU against a Russian candidate, as well as the election of Lithuanian Tomas Lamanauskas as the Deputy Secretary-General. While that campaign was orchestrated largely outside of the TTC, it was strengthened by the relationships forged through the TTC.

Critics see the glass as half empty.

There is consternation on both sides of the Atlantic that mere talk has been delivered in the 16 months since the TTC was launched. Also, some stakeholders and officials in member states feel left out of the process. **While EU and US working group technicians separately have held briefings and have taken testimony from stakeholders, it's clear that more could be done jointly to take advantage of the expertise outside of government.**

Also, there appears to be a disconnect between the bold ideas for transatlantic collaboration reflected in the statements of the co-chairs and the more cautious updates from the technocrats assigned to execute these lofty goals. The updates on progress evidence small steps and bureaucratic reticence.

The December ministerial meeting will affect whether the TTC glass is viewed as half-empty or half-full.

The US and the EU are under pressure to announce tangible results during the third ministerial meeting to be held on December 5 and 6 in the Washington, DC region. TTC watchers are looking for common ground to be reached on artificial intelligence (AI), a key emerging technology. Both partners are focused on building trustworthy AI based on democratic values and protecting human rights. The EU's Artificial Intelligence Act[15] is chugging along on its legislative track, while the White House recently launched its Blueprint for an AI Bill of Rights[16]. A draft joint roadmap on AI evaluation and measurement tools for trustworthy AI and risk management will likely be announced at the December meeting.

In late summer, the US CHIPS and Science Act[17] was signed into law, while the European Chips Act[18], which would strengthen the European semiconductor industry, is slated to be adopted in the first half of 2023. Both the EU and the US seek to head off a subsidy race to the bottom, so the meeting might include agreement on exchanging information about subsidies.

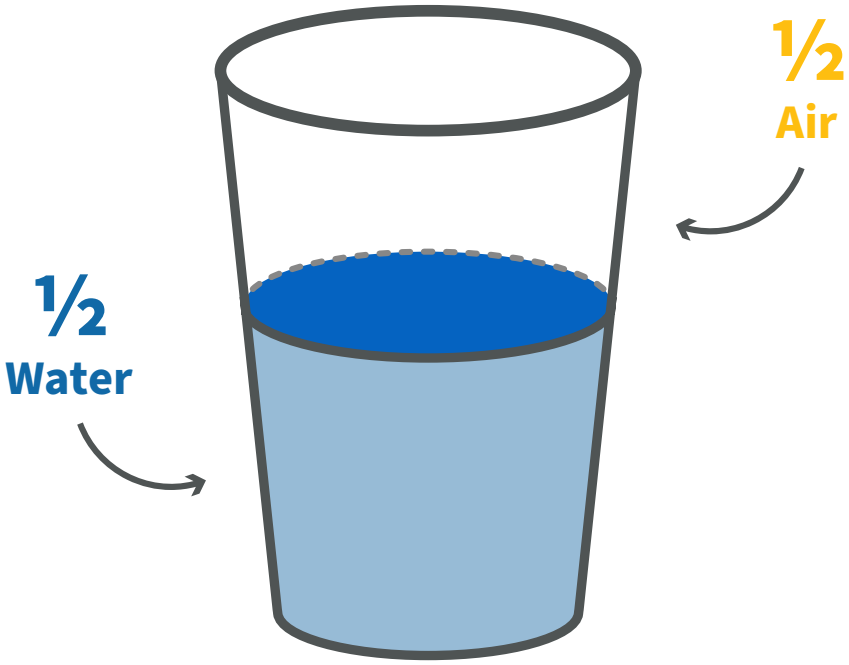
The parties have set up a task force to collaborate on public finance for ICT projects in developing world countries, and one such project may be defined at the December conclave. The goal is to counter China's growing influence from its Belt and Road Initiative investments in Africa, Asia, and South America and steer these countries toward Western standards and norms.

Deepening US-EU cooperation is a marathon, not a sprint. But tangible results will be needed to demonstrate the worth of the TTC if it's to be supported beyond the current European Commission and US Administration.

So, is the glass half empty or half full?

It's both… and neither. The political will to strengthen the ties between the EU and the US on technology and trade clearly exists. It remains to be seen whether both partners can deliver on these lofty goals.

But just as a glass is never truly empty (air fills any remaining room in the glass), the collection of ideas, discussions, activities, and incremental successes that the TTC has generated to date deepens the partnership with spill over benefits. In a world where tyrants seize and manipulate the cyber ecosystem to ruthlessly expand their power, the case for deepening EU-US collaboration to fortify a democratic values-centric alternative could not be more compelling.



Endnotes

9 See discussion in Dan Hamilton, Getting to Yes: Making the U.S.-EU Trade and Technology Council Effective, transatlantic.org/wp-content/uploads/2022/03/TTC-summary-brief-final-March-6-2022.pdf. The other transatlantic initiatives included coordinating global vaccine access, tackling climate change, rewriting global tax laws, creating a truce in the 17-year Boeing-Airbus subsidy dispute, eliminating targeted tariffs, creating a Joint Technology Competition Policy Dialogue, and forging a united response to the Russian war in Ukraine.

10 https://crsreports.congress.gov/product/pdf/R/R47095

11 https://www.theguardian.com/commentisfree/2016/nov/14/ttip-defeated-activists-donald-trump

12 https://en.wikipedia.org/wiki/Transatlantic_Economic_Council The current co-chairs of the TEC are the US Deputy National Security Advisor Daleep Singh and the EU Commissioner for Trade Valdis Dombrovskis.

13 See Tyson Barker, "TTC Lift-off: The Euro-Atlantic Tech Alliance Takes Shape," Internationale Politik Quarterly, September 30, 2021, https://ip-quarterly.com/en/ttc-lift-euro-atlantic-tech-alliance-takes-shape.

14 The UN's International Telecommunications Union vote was 139 out of 172 votes cast. https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx

15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

16 Blueprint for an AI Bill of Rights

17 https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

18 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733596/EPRS_BRI(2022)733596_EN.pdf

Does Transatlantic Economic Leadership Have a Future?

Transatlantic economic integration must harness emerging trade in services, digital services and ideas.

By Fredrik Erixon, Director of the European Centre for International Political Economy (ECIPE)

Transatlantic economic relations aren't in good health. Nor is the global economy a safe place that could provide stability at a time of tectonic geopolitical developments. A global economic recession is emerging following Russia's invasion of Ukraine and the ensuing spike in energy and food prices. Inflation is soaring, and few central banks can continue to maintain economic output and asset values by fuelling capital markets with more liquidity. After decades of fiscal irresponsibility – and record high budget deficits during the Covid-19 pandemic – most governments in the West are cash-strapped, and new borrowing comes at far higher interest rates. Could the outlook for the economy really get any worse?

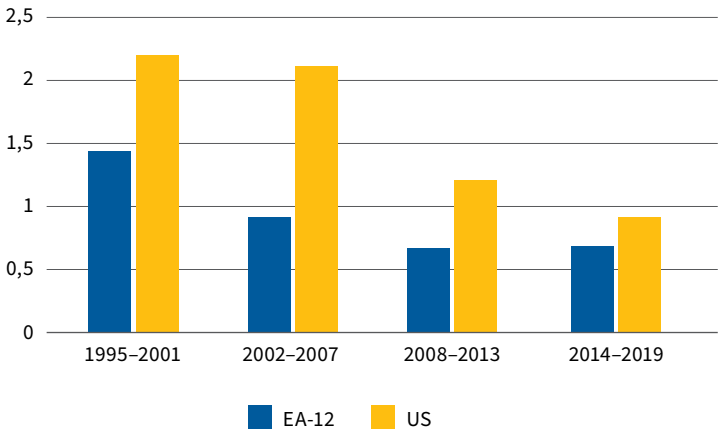
Unfortunately, the answer is – yes. Structural and institutional developments in the economy are adding to the cyclical pessimism. Productivity growth in the West (and elsewhere) has been poor for a long time, and labour productivity growth is down at such low levels that it is difficult to detect any underlying economic "oomph" (see Figure 1). Growth in merchandise trade, which had grown twice as fast as global growth in the heydays of globalization, has largely flatlined since the early 2010s.

Many of the economic institutions that Europe and the United States created after the Second World War to promote freer trade and market economy rules have lost their mojo. It's a long while since the G7 had anything conclusive to say about world economic policy. The G20 is missing in action. And what happened to the Bretton Woods institutions? The International Monetary Fund and the World Bank have become little more than modern conference centres at prime locations in Washington, DC. The World Trade Organization, whose meetings used to draw the ire of millions of demonstrators, seems to have passed out of being. Its meetings now feel like a gathering for the Vinyl Appreciation Society. Yes, strong WTO rules are better than the alternative – just as vinyl records give a far better sound than CDs and streaming music – but the world has moved on.

Yes, it could still get worse. **We are at a uniquely fragile moment for the post-war order and need wise and responsible leadership – yet such leadership is in short supply.** Like the devil in Dante's Commedia, Europe is frozen and seems stuck in ice – unable to move. Unlike his predecessor, President Biden is a decent man who doesn't feel a constant urge to insult other countries, but he seems to share Donald Trump's views on economic nationalism. Meanwhile, China has ramped up political and social control – sharpening its authoritarianism even more – and President Xi used the party congress in October 2022 to make the country's top leadership more of an echo chamber. India's Prime Minister, Narendra Modi, is stoking a domestic culture war – one that he thinks will benefit his brand of Hindu nationalism. Brazil's Jair Bolsonaro confirmed his reputation as the less competent version of Donald Trump. And Britain? It left Club Europe to make its way in the world as an agile, innovative, and free-trading economic power. It wanted no longer to be "shackled to the corpse" of the European economy – or so we were told. Now its politics are messier than Italy's, and its new-found economic dirigisme rivals France's penchant for state control. As the country's recent financial turmoil testified, it's a country at risk of becoming a public debt statement tied to a state.

I am being provocative, but just a bit. **Transatlantic economic cooperation, just like the world economy, is unwell.** The strong and joint reaction against Russia's invasion of Ukraine shows there is still life and energy in the old relationship between America and Europe, but the threats from an aggressive Russia and increasingly powerful China require far stronger responses. In the first place, both sides need to stop drafting policies (e.g., Europe's new digital regulations and America's Inflation Reduction Act) that harm the other. Then they should come up with bold initiatives that could boost Transatlantic exchange and pull many other economies closer to them.

Figure 1: Growth in GDP per hour worked



Source: Eurostat and Federal Reserve Bank of the United States

Economic policy should have a central role in new Transatlantic leadership. First, a strong economy is necessary for America and Europe to build power for the new Cold War – and prevent the growing systemic conflicts with China, Russia, and other malevolent regimes from heating up. If the transatlantic region is low-growth and resists the forces of structural economic change, it will be far more difficult to generate the necessary resources for building up military strength. Moreover, such an economy won't be attractive to many of the regions in the world that we want to pull more resolutely into the Western hemisphere.

The Trade and Technology Council (TTC) is the new kid on the block. Since the autumn of 2021, the EU and the US have been advancing a new form of transatlantic economic partnership that aims policies at the nexus of trade and technology. It's already proven to be useful. Sanctions packages against Russia have been coordinated in this new forum, and it has prompted some development that may lead to a new accord between the two partners that would lead to the free flow of data.

Nevertheless, the TTC is woefully inadequate for the challenges ahead. For deepened transatlantic relations to impact economic strength and be a powerful source of norms and rules in the global economy, it needs to promote much more transatlantic trade liberalization and level up the ambitions of regulatory cooperation by an order of magnitude or two. There is a good basis for this. The global economy is going through a technological shift that will have a huge impact on rates of productivity and growth – on economic competitiveness and power. **The US and Europe remain the central sources for this shift and can harness it to create a new globalization based on rules and norms that are free and fair and set by democratic market economies.**

In the real economy, this development is already emerging. Just look at the current trade landscape, which is increasingly guided by trade in services, digital services, and ideas. If anything, it seems that **cross-border economic exchange has increased its influence on the economy by relying far more on growth in ideas exchange – exchange involving R&D, innovation, technology and knowledge transfers, management imitation, and new patterns of digital commercial interaction.** And the pandemic has ushered in a new degree of intensity in ideas-based exchange. Take the pharmaceutical sector: various global networks of firms, universities, governments, and foundations were involved in developing Covid-19 vaccines and treatments. There are many more cross-border exchanges of ideas now. Some of these exchanges are monetized, while others aren't. Most of them will never be recorded as trade, but they are a central part of what constitutes modern globalization.

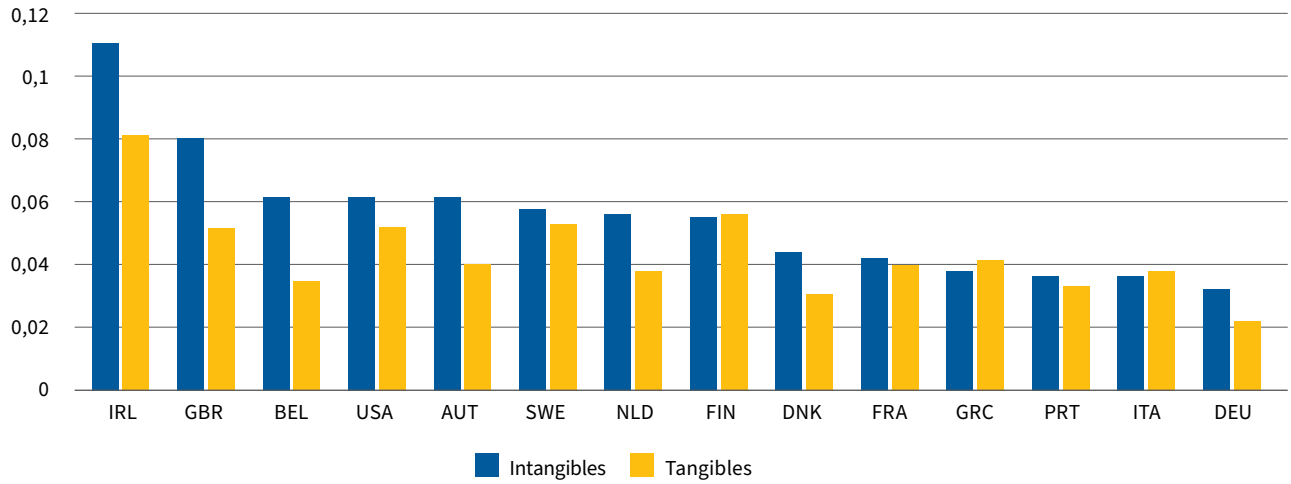
Trade flows have grown faster in ICT services and ideas than in goods since 2014. Obviously, trade in ICT services has been boosted by the whole wave of digitalization. The US Congressional Research Service has estimated that US exports to the EU of ICT and potentially ICT-enabled services amount to 190 billion US dollars, which is almost 15 percent of total trade between the two partners. Total US exports of ICT-enabled services were estimated at 439 billion US dollars, hitting almost 18 percent of total US exports.[19] What is less obvious is that trade in ideas also has started to grow faster. Flows of ideas are an ambiguous phenomenon. Most workers experience it constantly, but it is difficult to define it precisely. Moreover, given poor data availability, it is nigh on impossible to quantify.

To better understand trade in ideas, we have to start with the growth of the intangible economy and digitalization. Both these factors are leading to changing patterns of cross-border exchange and workplace interaction. Intangible assets include a variety of assets like the stock of patents, brands, R&D, software, and distribution networks – and all these factors are increasingly important to economic development. **These assets – and investment in them – define much of the productivity growth in modern economies, partly because they represent new knowledge, innovation capacities, and the ability to push the technological frontier.** And as Figure 2 shows, the growth rate for intangible assets is higher than the growth in tangible assets.

Intangibles are powered by digitalization because new technologies for interaction across borders have opened up for greater utilization of intangible assets. People can interact by e-mail or use professional platforms to have a constant flow of ideas between organizations or within an organization. Large companies especially work with cross-border teams for purposes of R&D, product development, market offerings, marketing strategies, and more. These new ways of working are commonplace, but most of the time, there are no records that track the economic and commercial significance of these interactions. It's just standard operating procedure.

What is clear, however, is that these interactions are increasingly generating value – both in America and Europe. These flows transfer as much knowledge and know-how as standard forms of trade when a formal exchange takes place. Trade economists

Figure 2: Average growth rate of tangible and intangible assets 1995-2015



Source: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ECO/WKP(2019)16&docLanguage=En

have always put a great value on the role that trade and investment play in "technology transfer." Trade can improve the static allocation of resources in an economy, but what is far more important is that **trade and investment allow firms and economies to access technology and knowledge that they otherwise couldn't.** They would be saddled with whatever offering that incumbent firms would have.

The broader picture is thus that cross-border interactions help workers and firms to imitate productive and successful economic behaviour from other countries and units. And imitation is a critical part of the ideas-based economy. It's a learning process in which all parts of a firm are exposed to other forms of production and market behaviour. Management and managing teams in all firms spend a great amount of their time channelling information that is necessary for positive imitation. Firms that operate on multiple markets are ever more dependent on coordination between markets. Modern factory-floor teams spend a growing part of their working time interacting with peers in other factories to learn from them or to share positive experiences with them. Consequently, **the ideas-based economy – and trade in ideas – are a phenomenon that affects all sectors.**

As innovation and product development become more central to the competitiveness of a firm, the ideas-based economy gets a boost. This is good news for the transatlantic economy. The economic power of innovation lies not only in the creation of the new idea itself but in its use and how it forces other organizations to learn from the innovating firm. Innovation these days tend to foster many more cross-border interactions than in the past. With fragmented production structures, more units than before have to learn from and adjust to new innovations. With presence in more markets, there has been a growth in the efforts that firms must make to ensure that new innovations can be marketed. And that is just developments inside a firm. Perhaps even more demanding is that firms need to keep track of the development in many different sectors – not just among their immediate competitors – and be prepared to take on board key innovations outside their market territory quickly. If they don't do so, the risk is that another competitor will.

The ambition for a revived agenda for transatlantic economic integration is to harness emerging trade in services, digital services, and ideas. It is this economy that will set the tone for economic progress and power in the 21st century. If America and Europe cannot find the ground for establishing the policies and rules that will guide new commerce, they will reduce their capacity to generate new prosperity and stand up against new aggressions by malevolent regimes.

Endnotes

19 https://fas.org/sgp/crs/misc/R44565.pdf

United (for the Most Part)

Values Shaping the West's Approach towards Technology

By Ewelina Kasprzyk, Programme Director, the Kościuszko Institute
Maciej Góra, Analyst & Project Coordinator, the Kościuszko Institute
Michał Krawczyk, Disinformation Analyst & Project Coordinator, the Kościuszko Institute

The virtual world is an increasingly more accurate reflection of the real world, with more and more of the elements and processes that make up human activity being transferred into it. We see a growing role of states, organisations, companies and, finally, international law in shaping cyberspace, which has become, among other things, another domain for the conduct of military operations and global competition. This makes cyberspace, much like the analogue world, a battleground for various ideologies, worldviews, and values to determine the nature of the virtual world and its rules.

Shared values and contradicting approaches

While much of the work and research in the previous decade has been dedicated to the themes of strengthening resilience and cybersecurity, the notions of values, especially political ones, have been overlooked. Values conflict in cyberspace is often reduced to simplistically presented tensions between privacy and security. But it should be stressed that the notion of values is extremely complicated and can be understood very differently. In the broad sense, value can be associated with what is good and desirable, setting principles or standards of behaviour and creating judgment of what is important in a given context. Values help evaluate different situations and acts in terms of goodness, but they do not directly guide actions. Different values can directly interact with each other – if we agree that cybersecurity is a value, we will act to increase it; at the same time, if privacy is a value, we will be obliged to respect some level of privacy while increasing security. As we can see, values in cyberspace, as in real life, have an inherently judgmental character and are the result of clashing positions and views, including differences between democratic and authoritarian approaches. Also, values in cyberspace are context-specific; a given value is not absolute. In one situation, there is a need to maximise privacy; in another, a limited amount of it will be enough to respect.

Ibo van de Poel, in his book *The Ethics of Cybersecurity,*[20] presented the four main shared values that should form a base for fair cyberspace. These are:

Security – understood as the safety of people, systems, and states from various types of threats. The answer for security value is presented by information security, which responds to problematic situations in which harm is done, including data breaches, cybercrime, cyberwarfare, etc.

Privacy – includes values such as moral autonomy, human dignity, identity, anonymity, and confidentiality. Privacy focuses on securing private data, enhancing informed consent, etc. The perspective on privacy can be different between the US and Europe; while the US approach focuses on its relation to liberty and put emphasis on the protection of citizens against state actors, the European approach is closely linked to human dignity, so privacy is also focusing on the relationship between people, individuals and companies.

Fairness – the assumption that we should strive for a state where problems and solutions are equally distributed in cyberspace. This moral cluster contains values such as justice, equality, accessibility, freedom from bias, non-discrimination, and protection of civil liberties. Cybersecurity threats and measures to combat them are not equally distributed. Fairness is a response to the problem and also to the fact that cybersecurity threats and measures

can undermine democracy and civil rights. People should be then treated fairly and equally in cyberspace; this is also closely connected with measures conducted by state and business actors.

Accountability – given that the actions taken by cyberspace actors, such as states or global companies, directly affect every user of cyberspace, accountability should be considered, incorporating values such as transparency, openness, and explain-ability. Accountability is a response to the lack of responsibility for activities in cyberspace. As cyberspace is a relatively new domain, law and legislation are lagging in terms of creating an environment to hold people, states, and businesses accountable for harmful acts online. We can see that, for example, in the case of social media platforms and their role in the disinformation problem. The Digital Services Act (DSA) and the Digital Markets Act (DMA) address this in the EU.

Still, the core values can be viewed very differently, and the relation between them can be set in numerous ways. The key here seems to be taking all these four core values into account, finding the right balance between them, and extending them to all users in the same way. It is in this element that the greatest differences can be seen between the approaches of democratic and authoritative countries and societies to regulate cyberspace on the basis of values. Authoritarian governments tend to enhance security at the expense of other values and surround only part of the population with protection, whereas the democratic approach focuses on creating similar rules for all. So, as can be seen, cyberspace is another domain of conflict taking place in the real world, separating the democratic approach from the authoritarian one.

To regulate or not to regulate?

Values are primarily used in the context of geopolitical competition, and the assumption that all Western countries share the same values is crucial in strengthening the so-called 'collective West's' position and increasing its influence throughout the world. It turns out, however, that the very thing that was supposed to differentiate 'us from them' is not always shared or understood the same way, even when it comes to questions of a more ethical nature.

The differences and similarities in the approach to ethics in technological development between the United States and the European Union are best illustrated by the different approaches to regulating artificial intelligence. Even though AI has been in development for several decades, it is still classified as an emerging and disruptive technology due to its huge potential to upset political, economic and social stability.

The need to regulate AI was observed by states several years ago, and more than 60 of them have issued their own AI policy documents.[21] The need for regulations in this area was stated in the Inaugural Joint Statement of the US-EU Trade and Technology Council, which underlined that 'AI technologies can help tackle many significant challenges that we face, and they can improve the quality of our lives' but also that they 'can threaten our shared values and fundamental freedoms if they are not developed and deployed responsibly or if they are misused' and affirmation of 'their [USA's and EU's] willingness and intention to develop and implement AI systems that are innovative and trustworthy and that respect universal human rights and shared democratic values'.[22]

The rapprochement between the United States and the European Union in the regulatory processes of artificial intelligence is a phenomenon that has been deepening in recent years and can be attributed to, among others, the fears of China taking the lead in the research and use of it.

The work of the High-Level Expert Group on AI and the White Paper on AI published in February 2020 resulted in the presentation of the Artificial Intelligence Act in April 2021 by the European Commission, the first such comprehensive legislation in the world regarding this technology. The AI Act classifies the uses of artificial intelligence into categories related to the potential risks of its use for individual and societal well-being – the greater the risks, the more controls and oversight are required. The AI Act is supposed to provide a framework that safeguards European values, with some of the uses of AI, like social credit systems, being outright banned from development and implementation in the EU. These checks, aimed at protecting the fundamental rights of Europeans, will be placed on all providers wishing to place their products and services in the EU's single market. While the issue of regulating AI due to its commitment to ethical values is praised by many, others argue that the European Union's approach will reduce investment in this market, slow economic growth, hinder research into the technology and cause a brain drain.

The United States, in line with its political traditions, has chosen a different approach. Both Democratic and Republican administrations have chosen not to regulate AI at the federal level, seeing it as counter-productive to limit a still rapidly developing technology and as a move that would contribute to falling further behind China in its development. **The laissez-faire approach to AI regulation, however, is criticised not only for its lack of protection for the end user and the possibility of bending ethical rules through technology providers but also as an element that gives an advantage to authoritarian states, such as China, in shaping global regulation in their favour.**

This is why, over the previous two years, we have seen Brussels and Washington moving closer together on AI regulation issues. In the US, in addition to state laws, the National AI Initiative Act has been passed at the federal level. Pending legislation is the Algorithmic Accountability Act of 2022, which the Biden administration unveiled in early October 2022; it is a non-binding act but strikes many of the notes played by the European Commission's AI Act. In addition, the US and the EU are cooperating in international organisations' AI initiatives, such as the OECD and the Global Partnership on Artificial Intelligence, and the EU-US Trade and Technology Council is heavily involved in the issue of coordinating approaches to this technology.

Holding up a united front

The world has always been polarised – and technology is just another domain that reflects the growing divide between democratic and authoritarian regimes, openness and control, privacy and surveillance, supporting freedoms and abusing power. This divide is oftentimes boiled down to values that guide and shape the development, employment and use of technology. Privacy, security, fairness, accountability – our approach to those values is what differentiates the so-called 'collective West' from states that tend to use technology to exercise their power in a rather authoritarian way. **The Western countries themselves also have their differences regarding technological development, which might be shocking given their declared unity against the adversarial use of technology commonly ascribed to states like Russia or China.**

Is the 'collective West' holding up a united front when it comes to values and technology? For the most part, yes – besides some oftentimes contradicting approaches towards development and regulations. Those visible discrepancies perhaps are not extreme enough to tarnish the collectiveness of Western countries; however, they do affect transatlantic cooperation a great deal.

As cyberspace is increasingly divided along ideological lines, mirroring what is happening geopolitically, the West should continue to promote its values through its policies and governance frameworks in order to minimise harms to democracy but also to curb the projection of authoritarianism through technologies. It is up to stakeholders – from public and private sectors to civil society – to sit down and figure out what core values should underpin their shared approach towards technology. This is one of the greatest challenges the transatlantic partners are facing right now.

Endnotes

20 I. van de Poel, The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology vol. 21, 2020.
21 https://oecd.ai/en/
22 U.S.-EU Trade and Technology Council Inaugural Joint Statement

The quest for global standards in AI

Cooperation between the EU and the US (in combination with other like-minded partners) is necessary to shape the future of AI

By Gregor Strojin, Vice Chair of the Committee on AI at the Council of Europe

Disruptive nature of AI

One of the recurring memes used over the past few years when discussing the need for the responsible development of artificial intelligence (AI) was the quote from the 1993 Jurassic Park character, Dr Ian Malcolm that the 'scientists were so preoccupied with whether they could, they did not stop to think if they should'. Although this film relies on genetic cloning as the underlying technology, various others provided examples of AI-related cataclysmic dangers and formed part of our perceptions of future human-robot relations. Such a dystopia, for the moment, firmly remains in the realm of science fiction. The risk of AI taking over the world and enslaving humanity is, nevertheless, allegorical. **Actual applications and experiences have shown that the most significant risk factor remains the human; how and why we use the technology.** The year 1993 was also when Tim Berners Lee released the source code of the World Wide Web into the public domain. Since then, the internet and connected digital technologies have exponentially and irreversibly transformed the world.

Both technologies differ in many ways. The internet is primarily a clearly defined set of protocols that have revolutionised communications and whose core has not changed much since. AI, on the other hand, is a creator of content. More importantly, it is a continuously and heterogeneously developing family of technologies making its definition a moving target. Although systematic research into AI started already in the 1950s, its development and implementation remained relatively slow. The internet has, without a doubt, facilitated the exponential expansion of AI over the previous decade. Vast amounts of data, available computing powers, and increasingly complex algorithmic approaches contributed to the proliferation of various AI technologies. Pattern recognition, classification, prediction, recommendation, and decision-making capabilities provide novel insights, approaches, and solutions to various problems. Unlocking such potentials allows for significant optimisation and remodelling of the existing methods in all areas of life, proving AI to be one of the most transformative technologies in history. It forms the basis for advances in autonomous vehicles, robotics, medicine, protein folding, nuclear fusion, natural language processing, image generation, and virtual reality, to name just a few, but also for deep fakes, dehumanisation of workplaces, surveillance technologies, and autonomous weapons.

While most AI applications are purely technical and used in various industrial settings, many directly impact individuals and, through this, society, gradually and on a mass scale. The previous decade provided evidence of the significant opportunities and changes that will continue to fuel AI's growth and attract investments. It also brought attention to the broader challenges and costs that need to be adequately addressed and are often overlooked while pursuing individual goals.

The risks associated with new technologies are ever-present yet seldom readily identifiable. Digital, highly integrable, and seemingly multi-purpose nature of AI is additionally characterised by obscurity. Even when the decision-making process of the AI is not hidden in a black box guarded by intellectual property rights, its reasoning is often too complex for humans to functionally understand or verify. Additionally, AI forms only a part (or parts) of the environments where prediction, recommendation, or even decision-making occurs, further obscuring causality and the general chain of responsibility.

Unsplash, Helena Lopes

From ethics to regulation

As such, AI represents the very definition of disruptive technology. Growing capabilities and perceived and actual risks catalysed the discussion on the need to create standards for ethical, responsible, accountable, trustworthy, safe, explainable, or human-centric AI. Eventually, they resulted in calls for regulation, which would provide legal clarity on rights and obligations. Many questions had to be addressed, ranging from quality, safety, and reliability issues of the marketed products to security, economic, political, and various social issues, foremost of which is AI's impact on fundamental rights: human rights, democracy, and the rule of law. The ethical and legal dimensions of AI attracted broader attention in the mid-2010s. By 2018, various initiatives grew to hundreds and provided a plethora of material. Much work on standard setting was done by experts participating in the work of technical standards organizations, such as ISO or IEEE, in policy development and support by organisations such as the OECD, UNESCO, or Council of Europe (CoE),

or within thematic but influential initiatives such as Global Partnership on AI (GPAI) which connected like-minded countries. Most cooperation, with the notable exception of UNESCO, was between Western countries. **However, their recommendations, guidelines and ethical charters remained voluntary and non-binding, thus lacking effectiveness which is particularly needed in critical cases.**

Numerous countries have since adopted national strategies on AI, which incorporated many of their findings and recommendations, primarily to facilitate their research and economy. However, few have committed to binding rules, often viewing them as inhibitors of both innovation and limiting the potential of the state. Recently, in October 2022, in the US, the White House released a Blueprint for an AI Bill of rights, which provides a framework of 'backstops against potential harms' for ensuring more accountable AI through a series of five principles and associated practices, but it remains non-binding. That said, various US regulatory agencies are looking into sectoral practices, and binding rules in the US will likely be introduced through vertical rather than horizontal instruments. In March 2022, China introduced binding Internet Information Service Algorithmic Recommendation Management Provisions, which focus on transparency, provision of services, and user rights protection, impose relatively high administrative and compliance burdens on the providers and operators, and establish a complex and widespread governance structure. The instrument focuses on algorithmic recommendation services with public opinion properties or social mobilisation capabilities. While its mechanisms and goals could prove a challenge to align with democratic or the rule of law principles, they will no doubt be observed closely by other regulators in the world to assess their effectiveness.

Due to interests at play, the governance of AI is a delicate subject that considers varying political, economic, and social factors. The scope and effectiveness of new standards will depend on the type of political values and mechanisms within a particular community and can be glimpsed by some basic questions. What kind of future and AI do we want? Centralised or decentralised? Open or closed? Transparent or obscure? State-controlled or libertarian? Authoritarian or democratic? Opportunistic or principled? One that tests the limits of what could be done, or one that questions what should be done?

Individual national approaches have obvious limits in a globalised world and risk regulatory divergence, which could limit the potential for interoperability and economy. Unlocking the potential of the technology requires multi-stakeholder engagement and as comprehensive inclusion. **There is a limit to the width and depth of the achievable consensus within the global community unless the depth and effectiveness of regulatory instruments are sacrificed.**

European approach

Europe traditionally serves as an example of how a coordinated international approach can successfully manage national aspirations. **The CoE was the first major organisation to address AI regulation from an intergovernmental perspective, basing its approach on its general mandate of protection and promotion of human rights, democracy, and the rule of law.** By this mechanism, several conventions regulating the impact of new technologies were developed in the past, setting global standards in pharmaceuticals, automated data processing, biotech, and cybersecurity, among others. The very nature of the collective European states' deference to the human rights standards enshrined in the European Convention on Human Rights makes them somewhat unique in the global context, as it provides a regular forum for intergovernmental cooperation and consequently enables a structured approach to aligning the design, development, and application of AI with its human rights standards on a relevant regional level. The Ad Hoc Committee on AI (CAHAI) was formed in 2019 to prepare a feasibility study and elements of appropriate legal instruments. It established that a new legal framework comprising a combination of legally binding and (not only) non-binding instruments of horizontal and vertical nature was required to address and mitigate the risks of both the technology and the inadequacy of the current rules. In 2022, negotiations on an appropriate instrument, provisionally titled AI Treaty (CoE AIT), started among 46 member states and with direct participation by six non-members (Canada, the Holy See, Israel, Japan, Mexico, USA) with the goal of finalising it by November 2023.

Almost simultaneously with the CoE, work commenced at the European Union (EU) level, but from a different direction. A proposal for a binding regulation titled AI Act (EU AIA) was put forward in line with the more comprehensive and market competitiveness-based Digital Agenda of the newly

formed European Commission (EC) in April 2021. **An effective approach to political issues should not target technology but rather its impact on society and the economy, including the rights and obligations of various stakeholders.** Both instruments understand this but to varying degrees. They are horizontal and with a risk-based and proportionate approach, but they differ in many elements. While the CoE AIT primarily addresses the Member States, the EU AIA targets the market. This perspective influences various provisions, ranging from the operationalisation of risk assessment and compliance measures to the enforcement and organization of governance. Currently (October 2022), the EU AIA proposal is discussed at two levels, at the Council of the EU with representatives of the 27 Member States and at the European Parliament, where over 3000 amendments were submitted to the original text. The date of the adoption of the final text is, therefore, still uncertain, but it could be by the end of 2023.

In July 2022, the EC proposed that the EU Member States provide it with a mandate to negotiate the CoE AIT on their behalf, as the subject matter falls within the remit of the EU's exclusive competencies. On the one hand, this could simplify negotiations for the CoE AIT as the 27 members will speak with one voice and represent the majority of votes in the CoE. It could also highly align the CoE AIT with the provisions of the EU AIA and create an international regulatory vehicle to which non-EU states can accede. **The combination of a CoE treaty (Convention on automated processing of personal data) and an EU regulation (GDPR) is, for example, one of the reasons that have enabled GDPR to become a global standard in personal data protection and also an essential motivation for non-CoE member states, including the US, to join the negotiating table actively.** On the other, such approach could divert the CoE AIT emphasis from human rights protection toward ensuring internal market consistency. Among some of the issues, EU AIA's maximum harmonisation regulation approach will prevent Member States from creating complementary rules that would differ from the EU AIA, for example, by strengthening the requirements for impact assessment, expanding the list of high-risk categories or by implementing additional rights or obligations.

Similarly, some of the envisaged elements of the CoE AIT might not be considered consistent with the provisions of the EU AIA. In line with the principle that 'nothing is agreed until everything is agreed', the finalised provisions of both instruments remain to be seen. Currently, as evident in various iterations of the compromise texts of the EU AIA, discussions remain open regarding fundamental issues, including definition, risk classification, and various exceptions to the rules. Through modifications at such points, the scope and effectiveness of the EU AIA could be altered during the final phases of the negotiations. Furthermore, due to the future negotiating role of the EC in the CoE AIT, the ongoing discussions regarding many of the EU AIA provisions might be reviewed in light of the new positioning.

Potential for global standards

Both European instruments will create global standards, but their actual global impact remains to be seen. Developing effective standards requires significant compromises on all sides; otherwise, they could be set at the lowest common denominator and remain ineffective. Indeed, many open issues do not need a binding approach, as they can be resolved on the level of technical standards or recommendations. The crucial issues, which require legislative intervention, relate to non-technical issues of political and social nature. As such, binding regulation which would fail to address fundamental rights issues adequately would be counter-productive, as it would stifle innovation without solving the pressing needs and could possibly entrench the existing practices.

Conversely, overambitious approaches might eventually result in a dead end, especially if the planned instruments are not adopted after lengthy development and negotiations. Negotiations with global partners within the CoE have only just started. However, broad participation by delegations from the US, Canada, Israel, Mexico, and Japan is a good indicator of the awareness of shared values and goals. The speed of AI's implementation does indicate that time is a factor, and that no regulation is regulation already. We should, however, strive for functionality of solutions and sustainability of our societies, rather than primacy in regulatory measures.

Securing a Digital Future

The Case for Strengthening Transatlantic and CEE Cooperation

By Danielle Piatkiewicz, Research Fellow, EUROPEUM Institute for European Policy

The ongoing war in Ukraine has revealed how today's battlefield takes place, more than ever, in the digital space. We have witnessed the Kremlin targeting Ukraine's critical infrastructure seeking to dismantle and disrupt internet and cell towers, and carrying out an onslaught of disinformation tactics aimed at changing the narrative of the war. Ukraine has been defending not only their physical borders but also its digital ones.

The war highlights the growing importance and dependence our societies have on digital technologies and how the digital space will be the new ground for strategic competition. In the next decade, emerging technologies have the potential to reshape our economies, transform militaries, influence democracies, and reshape the world. Simply put, the future is digital.

As geostrategic competitors like Russia and China continue to compete, rival, and govern the tech space, it remains vital for strategic partners to align to secure the digital space. **To set the global standard and regulate the digital space, the United States (US) and the European Union (EU) should continue to focus on developing a shared set of values and democratic principles to define the digital policy space.** This should include tackling the most pressing issues around digital technologies, from cyber hacking, artificial intelligence (AI), and internet regulation to data protection. However, diverging policies among the transatlantic allies have thus far prevented them from achieving a unified approach.

For countries within Central and Eastern Europe (CEE), the war in Ukraine has heightened security tensions within the region. Building up their defence capabilities on land, air, space, and the digital space remain vital in countering malign actors. Seen more than ever as a geostrategic location on Europe's eastern border, the US, EU, and North Atlantic Treaty Organization (NATO) will need to work in unison in order to protect the region from any future aggression from autocratic threats.

This brief will outline some of the main challenges and opportunities the transatlantic relationship has in achieving a joint-digital future. It also highlights aspects to which the CEE region can contribute towards this future.

(Re)Aligning digital policies

The challenges faced when dealing with digital technologies vary drastically. From dealing with cyber hacking to regulating the tech space, the US and EU have approached these challenges in various ways.

In recent years, the EU has made significant progress in both achieving strategic autonomy as well as 'digital sovereignty'[23] by strengthening its resiliency and competitiveness in order to secure its digital future. The European Union has set forth goals to strengthen its security and defence policy by 2030 through its recently released Strategic Compass. The aim is to develop the EU as a stronger and more agile international actor, able to respond to threats emanating from the strategic environment in which it operates, including investing in the digital domain better to protect the EU's security and defence interests.

The Strategic Compass focuses on countering these increased threats by developing specialised tools at its disposal (EU hybrid toolbox, Foreign Information and Manipulation Toolbox, among others). In

addition, the EU has set out both the Digital Markets Act (DMA), which aims to ensure a fair and competitive online economy, along with the Digital Services Act (DSA), which limits the spread of illegal content online; both acts will alter how users and companies utilise the internet.

On the other side of the Atlantic, the Biden administration calls for the deepening of relations with allies, specifically multilateral cooperation with the EU and NATO on a range of issues, including cybersecurity. As outlined in their recently released National Security Strategy, the US 'will strengthen democracy across the world, and multilateral institutions, as we look to the future to chart new and fair rules of the road for emerging technology, cybersecurity, and trade and economics'.[24]

The US under the Biden administration has struggled with balancing both 'reinvigorate U.S. global engagement on technology while simultaneously managing new regulatory proposals for American tech giants'.[25] However, this stance shifted in early October when President Biden unveiled a new AI Bill of Rights, which outlines five protections Americans should have in the AI age. It should serve as a blueprint and guide for a society that 'protects all people from these threats — and uses technologies in ways that reinforce our highest values'.[26] In particular, the Bill of Rights calls for closer cooperation among the government, technology companies, and citizens to hold AI accountable.

Some critics say the 'plan lacks teeth' and the US needs even tougher regulation around AI.[27] The EU, on the other hand, is moving towards a 'much more

restrictive regulatory approach than the US. While a compromise on a privacy shield for cross-border data flow has been reached, disagreement remains over the details of cloud governance, including an EU cybersecurity certification proposal.[28]

While these are just some examples of how the US and EU are taking divergent paths in facing digital challenges, progress was established in 2021 with the launch of the Trade and Technology Council (TTC), which aims to shape the rules that will govern the advance of technology. European Commission President Ursula von der Leyen stated after inviting the US to join the EU in writing this global standard: 'Together, we could create a digital economy rulebook that is valid worldwide. It goes from data protection and privacy to the security of critical infrastructure. A body of rules based on our values: human rights and pluralism, inclusion, and protection of privacy'.[29]

The TTC 'marked a transatlantic cooperation reboot'[30] in fostering cooperation to key global trade, economic, and technology issues and to deepening transatlantic trade and economic relations based on shared democratic values. As it celebrates the first anniversary of its founding, the TTC has been credited with coordinating efforts in response to Russia's invasion and outlining substantive plans to coordinate US-EU development in emerging technologies, most notably in AI. The next TTC meeting will take place in December and will likely include a joint declaration on human rights and address concerns around AI, semiconductors, and global connectivity, among other issues.

How can the CEE shape its digital future?

While the TTC has ambitious aims to align the transatlantic agenda, it will require political will, unity, and investment from both sides to achieve a joint digital future. To achieve this, geostrategic regions such as the CEE must also be involved in shaping their respective digital futures.

The war has reaffirmed many security concerns among CEE countries, who have (rightfully) flagged Russia's growing aggression towards the region for decades. As a result, the war has bolstered US security commitment and increased allied and NATO support in the region, including in the digital space.

The EU's Strategic Compass outlines support for not only Ukraine but also the broader Eastern neighbourhood. This includes boosting EU cooperation in countering hostile interference by Russia. We have seen the extensive use of military instruments and hybrid tactics aimed at compromising their stability and their democratic processes, which have direct implications for the EU's security.

As the EU develops its strategic aims to develop its security and defence capabilities as outlined in the Strategic Compass, the CEE region can play a pivotal role in building up short- and long-term defence against Russia – especially in the digital domain. For example, we have seen EU Member States step up their digital support for Ukraine. Given the experience in countering Russian hybrid threats, countries like Poland, Slovenia, Latvia, and Estonia, among several others, have joined Ukraine

to fight cybercrime, counter disinformation tactics, and provide digital infrastructure. The CEE region has decades of experience in combating these cyber-threats and has a vested interest in securing the region from any further infiltration from malign actors.

However, deviating security and political objectives within the CEE region, especially regarding areas around democracy, economic growth, and investments in the energy infrastructure and digital sectors, stand to challenge the political alignment the EU is attempting to achieve.

Over the years, the Visegrad 4 members (Slovakia, Czech Republic, Hungary, and Poland) have departed on many aspects, from migration to issues around energy. The war in Ukraine has amplified these divergences and has taken its toll on the CEE security environment. For example, Hungary has experienced diverging views on severing full ties with Russia, and mounting rule of law issues around Hungary and Poland have created further tensions within the EU. These tensions have only been temporarily hushed as Poland, for example, remains the main hub for channelling military and humanitarian aid to Ukraine and the primary destination for refugees fleeing from the conflict. If left unaddressed for much longer, future clashes between the EU and specific countries in the CEE region could escalate.

Steps for CEE to take

While the TTC aims to align US-EU digital policies, the Three Seas Initiative (3SI) remains a useful tool for the CEE region to improve connections among twelve EU Member States located between the Baltic, Adriatic, and Black Seas. Created in 2019, this politically inspired, commercially driven platform remains a vital component mechanism to boost the economic growth and resilience of the region by developing transport, energy, and digital infrastructure.[31] Shortly after the war, signatories made a joint statement calling for the further development of infrastructure connections and digital services among the 3SI countries. This included investments in cybersecurity and the use of trusted solutions. Both aim to increase their security, but also to make better use of their potential to 'promote our region as a trusted partner and supplier of proven solutions in the field of cybersecurity and telecommunications'.[32]

While the temptation to create new avenues of co-operation, the 3SI is an existing tool that already aligns the US-EU and the CEE region and should be further harnessed to develop interconnectedness between the regions.

Next steps

Looking ahead at how to shape a joint digital future in which all US-EU and CEE interests are included – will be impossible. But, finding compromises and utilising both existing and new infrastructure will be key in bolstering and securing the digital space. The TTC and 3SI are examples of how this cooperation could develop further.

The CEE region will also need to do some soul-searching, especially regarding their mounting and often polarising political stances towards issues such as migration, energy, and the rule of law. **Finding alignment with the US and EU on these issues will be critical in shaping the current and future orientation of their security environment, especially in the digital space.**

While the conflict in Ukraine has no end date in sight, the CEE region remains vulnerable to malign actors such as Russia. The CEE region has an important role in helping defend the EU and the US's interest in defending the democratic values that bind the allies. The CEE region has the opportunity to not only help rebuild but to be an active contributor to Ukraine's post-war reconstruction – one that can ensure future guarantees that the region can defend itself from future threats.

Endnotes

23 Komaitis, Konstantinos and Justin Sherman, "US and EU tech strategy aren't as aligned as you think", Brookings, May 11, 2021. https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/

24 Biden-Harris Administration, National Security Strategy, The White House, October 2022. Page 48.

25 Komaitis, Konstantinos and Justin Sherman, "US and EU tech strategy aren't as aligned as you think", Brookings, May 11, 2021. https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/

26 Biden-Harris Administration, Blueprint for an AI Bill of Rights, The White House, 2022. https://www.whitehouse.gov/ostp/ai-bill-of-rights/

27 Ibid.

28 Barfield. Claude, "The US-EU Trade and Technology Council is still in search of a role", The Washington Examiner, October 21, 2022. https://www.washingtonexaminer.com/restoring-america/courage-strength-optimism/us-eu-trade-technology-council-still-in-search-of-role

29 Komaitis, Konstantinos and Justin Sherman, "US and EU tech strategy aren't as aligned as you think", Brookings, May 11, 2021. https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/

30 Bonefeld-Dahl, Cecilia, cited in TechEurope "Becoming Tech Allies: 24 Targets for the EU-UU Trade & Technology Council By 2024", Digital Europe, February 22, 2022.

31 Three Seas Initiative, https://3seas.eu/about/objectives

32 Three Seas Initiative, Joint Declaration of the Seventh Summit Three Seas Initiative, https://3seas.eu/about/joint-declaration-of-the-seventh-three-seas-initiative-summit

How to avoid splinternet?

Modularity is a key tool for a better digital future

By Susan Ness, non-resident Senior Fellow of the Europe Center of the Atlantic Council, Distinguished fellow at the Annenberg Public Policy Center of the University of Pennsylvania
Chris Riley, Global internet policy and technology researcher and a distinguished research fellow at the Annenberg Public Policy Center of the University of Pennsylvania.

Imagine a world where each national government determined what online information its citizens could access and send legally. Far-fetched? Not really. The internet is global, but the laws that govern it are local.

Internet users worldwide are pummeled by the same disinformation and online harms, amplified by the same global platforms and services. Responding to public outcry, a growing number of regional and national governments are drafting their own signature digital laws to attack the same global problems.

Making matters worse, authoritarian governments, among them China and Russia, have walled off access to the open internet, blocking and punishing websites that offer factual information about their political opponents, and weaponizing disinformation at home and abroad. Defending their "sovereign version of the Internet" they cynically claim they are cleansing cyberspace of disinformation and terrorism – just like western governments.

As a consequence, the Global Internet is fast becoming the "splinternet," where the globally-connected open Internet "splinters" into disjointed networks, and governments or large companies control the information users can see. The future of a free and open global internet may well hinge on democracies forging greater digital alignment to serve as a clear alternative to the internet of despotic regimes. It will not come easily.

Modularity is an intriguing approach to multinational and stakeholder engagement on digital regulation.

Western democracies understandably seek to improve platform responsibility and accountability consistent with human rights and freedom of expression. But despite increasingly similar values-based governance ideas, transatlantic collaboration on a comprehensive digital regulatory regime is not in the cards, given the disparities in the U.S. and European legal systems, norms, and priorities, along with starkly different time frames for action.

While full alignment is impossible, there is a way right now for like-minded democracies to collaborate on narrowly crafted processes, while respecting their different regulatory frameworks, legal systems, and societal norms. It's called "modularity."

Modularity is a fresh form of co-regulatory governance, in which modules—discrete processes, protocols, and codes—are developed through multistakeholder procedures involving civil society, industry, academia and participating governments. The governments in turn recognize these common "modules" as satisfying the requirements under their respective regulatory regimes without the need for a new international treaty.

Examples of potential modules include systems for vetting researchers and approving their access to platform data under enforceable safety and privacy conditions; vetting procedures, minimum standards and oversight of independent auditors seeking to conduct risk assessments and algorithm impact audits; minimum disclosures and archiving rules for political advertising; and common protocols for crisis situations.

These may seem like small gains in alignment, measured against the massive geopolitical tensions pushing division. But it is a start that can deliver practical benefit in the near term, through operational alignment on important technical issues. And it helps build the muscle of collaboration and unity at this much needed time.

Picture modularity as a five-step process using, for illustration, a module designed to vet researchers for access to platform data:

First, problem identification: One or more governments identify an open challenge, such as vetting researchers under a digital platform data access mandate.

Second, module formation: A group of multistakeholder experts (which may or may not include officials from multiple governments) collaborates to develop a module that sets out standards and processes for vetting researchers and their research proposals, and is designed for use across multiple jurisdictions.

Third, validation: Individual governments evaluate and approve the module by declaring that its output satisfies a specific provision, if any, of their digital platform legislation. In this example, the module output would be a determination that the researcher and her research project are cleared to receive platform data and that the project will follow strict privacy and security protocols.

Fourth, execution: The modular system applies its protocols to individual cases, in this instance, by vetting research projects that applied for clearance, and overseeing that the research project follows the required privacy and security protocols.

Fifth, enforcement and analysis: Each government enforces its national policies and procedures, including penalizing a platform that fails to provide suitable access to researchers as required under that national law. It also periodically reviews the module to ensure that it remains fit-for-purpose.

Agreements would allow the module overseers to update the module processes and rules, based on actual experience. The update would apply immediately across jurisdictions without having to wait to secure regulatory approval in each country. In that way, the modular system would be responsive to a rapidly evolving marketplace. Sunset provisions would be built in to ensure that the modules are regularly assessed for effectiveness.

The good news is that over the past few years, academics, and civil society have partnered to develop a variety of standards, protocols, and best practices that could serve as a solid foundation for such modules. In some instances, governments have been the convenor.

Modularity benefits governments, industry, civil society and users alike.

Alignment of such cross-border mechanisms will benefit all stakeholders. For governments, it can lower the cost of regulation by reducing the volume of implementation rules to be drafted. For businesses, it can reduce uncertainty and inefficiencies from having to design and run multiple operations to meet different national requirements. For civil society, it can offer a seat at the table for crafting and running the mechanisms and protocols. And for users, it reduces the confusion of navigating multiple systems that are serving the same function.

Another long-term benefit of modularity: as democratic governments become comfortable working across borders and partnering with stakeholders, they build trust and the collective muscle memory to expand collaboration beyond narrowly constructed modular operational systems, further strengthening the global internet.

Nations aren't waiting for alignment; they are rapidly pursuing their own solutions.

Despite concerns about internet fragmentation, for now, national and regional governments are asserting their sovereignty by enacting their own comprehensive legislation to rein in the global internet rather than pursuing shared legal frameworks. In early July, the European Union achieved political closure on the landmark Digital Services Act and the Digital Markets Act, which the EU hopes will become the global gold standard for platform regulation, just as GDPR did for privacy and data protection. Across the Channel, the United Kingdom had been moving apace with parliamentary negotiations on the Online Safety Bill, but has paused its debate pending the Conservative Party leadership change. Australia updated its online safety laws with the Online Safety Act 2021, while Canada has circulated a white paper on a legislative framework for platform regulation.

The United States, in contrast is, well, exactly nowhere. While Congress is flooded with bills to regulate the tech industry, none commands a clear path to enactment, given the lack of consensus on what is needed and the scarcity of legislative days before mid-term elections.

The EU/US Trade and Technology Partnership has provided a long-sought bridge for transatlantic tech policy discussions, although to date it has avoided delving into DSA implementation. The TTC is well-positioned to initiate experiments with modularity as a vehicle for greater EU-US alignment; whether it has the ambition to take on anything so proactive remains to be seen.

Modularity could face political pushback by governments that are reluctant to cede any amount of regulatory control.

Acceptance by multiple nations of common modules will occur only if the perceived benefits of having one system to complete a function – instead of several different systems necessitating multiple platform responses and public confusion – outweighs a government's predisposition to control the entire process.

Governments often conduct multistakeholder consultations before drafting rules. Indeed, the DSA and the OSB explicitly require such outreach. But such notice and comment procedures are not the same as multinational and stakeholder collaboration on developing and implementing the mechanisms, protocols, or codes with cross-border application.

Encouragingly, both the DSA and the current OSB draft include language that could ultimately permit some form of modularity. For example, Article 34 of the DSA requires the Commission to support international standards bodies that are developing voluntary standards for platform audits and other technical items, and, Article 35 requires it to engage civil society and industry participation in drafting voluntary codes of conduct.

The current version of the OSB similarly requires Ofcom, the UK communications regulatory commission, to consult with various stakeholders before drafting regulations and codes to implement the law. Critically, the OSB also envisions that compliance with equivalent standards may suffice, which could lead to acceptance of modular standards and codes.

The opportunity for alignment is there, but ambition and agreement are needed.

What is missing is explicit agreement by transatlantic governments to work together to allow narrowly-crafted common modules to satisfy requirements in their laws, and to add enabling legislation where it is needed.

Now is a powerful but fleeting opportunity for democracies to collaborate on the technical systems and protocols that underpin governance of the digital realm. It will slow down the splintering of the internet, speed up the ability to adapt processes and rules to a rapidly evolving digital ecosystem, and support the survival of an open and safer internet that respects free expression and human rights.

Contributors

Christakis, Théodore

Professor of Law and Chair on the Legal and Regulatory Implications of Artificial Intelligence (AI-regulation.com) at University Grenoble Alpes (France). Director of Research for Europe with the Cross-Border Data Forum and Senior Fellow with the Future of Privacy Forum. He has advised governments, international organizations, and private companies on issues concerning International and European law, cybersecurity, artificial intelligence, and data protection law.

Erixon, Fredrik

Fredrik Erixon is a Swedish economist, writer and the founding director of the European Centre for International Political Economy (ECIPE). He is the author of several books and studies in the fields of international economics, economic policy, and regulatory affairs.

Góra, Maciej

Maciej Góra is a Project Coordinator and Analyst at the Kosciuszko Institute. He studied National Security at the Jagiellonian University, Cybersecurity at the AGH University of Science and Technology and International Relations at Charles University. At the Institute, he manages cybersecurity-related projects, operationalises the agenda for the CYBERSEC conference, co-authors reports and policy briefs, and represents the Institute as an expert in the media and during external events.

Kasprzyk, Ewelina

Ewelina Kasprzyk is a Researcher, Project Manager and Chief Editor of the European Cybersecurity Journal at the Kosciuszko Institute. She coordinates the Institute's key projects, including CYBERSEC Forum. Her research interests include the impact of technology on societies, in particular the role of social media in shaping democracy. She holds MA in American Studies and MSc in International Relations, earned at the Jagiellonian University.

Krawczyk, Michał

Disinformation Analyst and Project Coordinator at the Kosciuszko Institute. Graduate of the Jagiellonian University in Krakow, majoring in Security Studies. Participant of the "Changing Security and Hybrid Threats" summer school at the University of Jyvaskyla. Member of the "Prozodia" research team focused on developing an ICT tool to analyse disinformation, an author of numerous publications, and a host of the General Talk podcast.

Ness, Susan

Susan Ness is a nonresident senior fellow at the Europe Center of the Atlantic Council, focusing on transatlantic digital policy. She also is a Distinguished Fellow at the University of Pennsylvania's Annenberg Public Policy Center, leading a project on 'modularity' to better align transatlantic digital governance despite dissimilar legal frameworks. Previously, she served as a U.S. Federal Communications Commissioner.

Piatkiewicz, Danielle

Danielle Piatkiewicz is a research fellow at EUROPEUM focusing on Transatlantic, Central, and Eastern European foreign and security relations. She is also a Program Director at the Alliance of Democracies Foundation. She holds an M.A. from Jagiellonian University (Krakow, Poland) and a B.A. from the University of California, Santa Barbara.

Riley, Chris

Chris Riley is a distinguished research fellow at the Annenberg Public Policy Center at the University of Pennsylvania, the principal at Cedar Road Consulting and a senior fellow for internet governance at the R Street Institute. He holds a Ph.D. in computer science from Johns Hopkins University and a J.D. from Yale Law School.

Strojin, Gregor

Gregor Strojin is the Vice Chair of the Committee on AI at the Council of Europe and former Chair of CAHAI. Gregor holds degrees in International and Comparative Law and IT&IP. His work interests lie at the crossroads of technology, information, and law, and he is active in several related bodies and initiatives.


Atlantic Council


EUROPEUM
INSTITUT PRO EVROPSKOU POLITIKU
INSTITUTE FOR EUROPEAN POLICY


THE KOSCIUSZKO INSTITUTE


AI-REGULATION.COM


ECIPE
EUROPEAN CENTRE
FOR INTERNATIONAL
POLITICAL ECONOMY


CENTER
ZA EVROPSKO
PRIHODNOST
CENTRE
FOR EUROPEAN
PERSPECTIVE
CEP