friends of europe

SUMMER 2022

Europe in 2030: strengthening public-private cooperation in hybrid crises

EVENT REPORT

Cover image credits: Rost-9/Bigstock

Friends of Europe's Peace, Security and Defence programme aims to make sense of the emerging new geopolitical environment by analysing ongoing transnational challenges. To do so, we cover topics including the state of the EU's security and defence evolution, the transatlantic security partnership, peace and stability in the EU's neighbouring regions, the link between space, defence and security, the impact of increased digitization and emerging technologies on resilience, the integration of women into peace and security practices, the impact of conflict, and the value of peacebuilding initiatives.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

With the support of:

Co-funded by the European Union

Publisher: Geert Cami
Senior Fellows: Jamie Shea, Chris Kremidas-Courtney (author)
Director: Dharmendra Kanani
Programme Managers: Elena Saenz Feehan, Juraj Majcin
Programme Executive: Alejandro Esteso
Programme Assistant: Lena Loch (co-author)
Events Manager: Alexandra Binard
Editor: Anna Muizniece
Design: Lucien Leyh
Rapporteur: Emily Waterfield

Table of contents

Executive summary

On 19 May 2022, Friends of Europe held its third and latest tabletop exercise, titled 'Europe in 2030: Strengthening public-private cooperation in hybrid crises', in Brussels. This report shares the key findings of the exercise and provides recommendations for both the public and private sectors. It details steps to improve cooperation and adequately prepare Europe for the world in 2030.

Set in the year 2030, this year's scenario focused on a hybrid campaign directed against a large section of the European economy in the midst of other new challenges unrelated to any malign actions. In a world more digitalised and connected than ever before, markets in the scenario were highly influenced and constantly changed by new and disruptive technologies. Given the vital role of the private sector in addressing hybrid threats, this exercise once again highlighted the need for a coordinated public and private sector response.

1. Future trends are creating newly ungoverned and under-governed spaces. The tabletop exercise highlighted the potential for problems with geopolitical consequences in spaces that are either currently unregulated, or where technology and commerce have outstripped the existing regulation.

> "Many of the technologies we are relying on to enable our new green economy may also present risks to democracy, the rule of law and social order if they are not governed effectively.
>
> **Chris Kremidas-Courtney**, Senior Fellow at Friends of Europe

Extending democratic control and the rule of law into these spaces is an urgent matter requiring **informed public debate and a common public-private-civil society understanding of the choices we will be facing** as each new emerging and disruptive technology reaches the final development and deployment stage.

Policymakers need to **anticipate developments in order to adapt their legal frameworks in a timely manner.** The metaverse and outer space are two key areas where existing challenges and anticipated developments by 2030 will require urgent attention by regulatory authorities and/or the international community.

2. More **widespread use of immersive extended reality (XR)[1] technologies, which will comprise the metaverse, present a risk of further dividing our societies** into groups based on those who choose to spend more time in either

[1]Augmented reality (AR) + virtual reality (VR) = extended reality (XR)

reality or the immersive virtual world. To integrate the metaverse into real life, more awareness, specialised education and rules on the member state and EU levels were identified as necessary steps. The widespread use of immersive XR devices requires building effective rules on 'gamification' in each future update of the Digital Services Act (DSA). Otherwise, **potential misuse of private and public data on citizens and the ability to engage in gamification to manipulate behaviour and beliefs increases.**

The current disinformation challenges that democracies are facing in a world of interactive media will become even more challenging in a world of immersive XR experiences. Without prudent measures taken early, they could lead to even deeper societal divisions and an increase in the kind of disinformation-driven violence that we have witnessed from 2020 through 2022.

Finding the right balance between regulation and enabling innovation remains a perennial challenge identified by the participants. As in past exercises, the balancing act of maintaining the regulation-partnership dynamic between public and private entities requires a high degree of trust and cooperation.

Will a great firewall of Europe, Frontex or Europol for the metaverse(s) be required to protect citizens from external manipulations in the virtual world? As a borderless environment, the virtual world presents risks for the individual in the form of data misuse, lack of regulations and sanctions, as well as limited prosecution in real life for crimes experienced online. Additionally, a lack of effective metaverse governance outside of Europe could present risks to citizens within the Union in the form of criminal activity or other malign behaviour. In the coming years, EU leaders may face a decision on whether to institute **a Europe-wide institution to police the metaverse and impose virtual border controls and sanctions.**

3. Opt-in or opt-out? **The right to 'unplug' and its implications for privacy and equality were also identified as an emerging issue. In a future world in which virtually every transaction and interface will occur in an increasingly immersive digital world, will citizens have the right to opt-out and remain in the analogue world?** For example, in a future world of brain machine interfaces and cyber implants, will a worker within Europe be faced with a decision to either accept XR implants or lose their job?

Keeping citizens grounded within society is an ongoing effort, which may become more difficult in the future. Previous tabletop exercise findings strongly identified the need for building and maintaining social cohesion. In this iteration, **the need for efforts to keep citizens grounded in reality as XR technologies become more prevalent** was identified as a new emerging challenge.

4. Social inequality is also expected to be amplified by job losses due to digitalisation, which may create fertile ground for conflict and exploitation by disinformation. While most power regarding social and economic matters remains at the national level in Europe, the EU must act to raise consciousness on these potential social threats, notably by publishing scorecards and statistical evidence, and promoting an equality agenda, including through legislation on issues such as equal pay for women and the status of platform or self-employed workers.

The tabletop exercise broadly identified some of the decision points that our societies will face with regard to each new development, but **much work remains to be done on outlining the specific choices that will need to be made. Will we recognise these crossroads as we approach them?** Or will we speed on past them, not recognising what kinds of choices have already been made by default?

Moreover, there is an emerging **generational gap between digital natives (younger citizens) and digital immigrants** (everyone else), resulting in differing ideas about privacy. This points to a **need for intergenerational dialogue** in policy formulation on society and emerging technologies. In addition, educational efforts will need to be focused on citizens who have already completed their formal education, in particular with the advent of XR technologies and the metaverse.

5. The pace of social and technological change is currently advancing faster than democratic institutions are able to keep pace with, leaving them to play catch-up as they react to constantly changing dynamics. With the advent of artificial intelligence (AI), **we risk outsourcing decisions to AI systems that may move too fast for human intervention to prevent accidents.**

The rollout of **AI-driven transport also presents risks to supply chain and military mobility** in cases of software glitches or cyber-attacks. How much should be invested in systems with analogue or human operator redundancy to mitigate risks? While AI increases efficiency and reduces costs, it also brings new potential threats in the form of internal and external digital interference. In the event of such disruptions, human actors have the advantage of finding creative, non-predefined solutions, and thus reacting more quickly. So, finding the right balance of AI and human interface, in addition to investing in human interface redundancy, will be important considerations in the coming years.

6. EU plans to deploy quantum resistant cryptography should be accelerated. Given the trend of technological breakthroughs arriving sooner than expected, the Sputnik moment for quantum codebreaking could arrive well before 2030. To achieve that, the EU, member state governments and companies must urgently cooperate to develop the necessary standards and implementation plans.

However, much like the current cybersecurity situation, if the entire systems of finance, supply chains, communications, AI-enabled systems and the Internet of Things are not sufficiently protected in time with quantum resistant security, **societies could be left entering yet another age of digital vulnerability.**

The DSA, European Democracy Action Plan, legal framework for AI and General Data Protection Regulation (GDPR) are leading global standards, but each will require constant updates in a timely manner in order to remain effective. The DSA only came out after much damage had been done, exemplifying that timelines must be accelerated.

The EU's technology venture capital ecosystem is not currently fit to keep up with the United States, China, Canada or Japan. The outlook for the Union to lead on many of these emerging technologies in 2030 is in doubt without a significant increase in capital available to spur innovation. Otherwise, too many bright European scientists and innovators will continue to leave the EU in order to patent their discoveries and find venture capital to start new companies and expand into new markets.

7. Is space the new Wild West? The 1967 Outer Space Treaty and subsequent regulations are insufficient to handle the massive entry of private sector operators into the space domain. A single company today already owns more satellites in low earth orbit than all the states in the world combined, and there are far more plans for company-owned satellites by 2030. Moreover, there is **no adequate international or national legislation to cover growing problems of space debris and space traffic management.** UN bodies responsible for these issues are deadlocked, so a 'coalition of like-minded nations' may be the best initial approach.

Considering the current trend of private actors' impact on the war in Ukraine, will they always be on our side now that the genie is out of the bottle? **This points to a continued need to build public-private trust relationships and common understanding by conducting joint risk assessments, exercises and collaboration on recommendations for updated legislation.**

8. Finally, **climate migration will increase by 2030, both within Europe and from outside of the Union.** Extreme weather events and climate impact on living conditions and agriculture will result in displaced people moving into and across the EU. Climate must be clearly defined as a cause of migration. Consequently, the legal status of 'climate migrants' must be added to international treaties. Whether someone is considered a refugee or a migrant impacts admission processes in hosting states significantly.

Context

On 19 May 2022, Friends of Europe held its third and latest tabletop exercise, titled 'Europe in 2030: Strengthening public-private cooperation in hybrid crises', in Brussels. This report shares the key findings of the exercise and provides recommendations for both the public and private sectors. It details steps to improve cooperation and adequately prepare Europe for the world in 2030.

With increasing digitalisation, newly emerging (disruptive) technologies, stronger geopolitical tensions and global challenges like climate change, the nature, origin and handling of threats have changed completely. This exercise brought together around 40 senior experts from the European Union, NATO, as well as the private and civil society sectors, to discuss strategies and solutions to tackle hybrid threats.

Participants were presented with a rare opportunity to address the impacts of future developments and to reflect on what kinds of legal and policy updates will be required to maintain democracy and the rule of law in the face of these challenges. The result of these scenario-based discussions was a set of concrete recommendations on how to close projected gaps in governance and new ways to address future challenges.

Set in the year 2030, this year's scenario focused on a hybrid campaign directed against a large section of the European economy in the midst of other new challenges unrelated to any malign actions. In a world more digitalised and connected than ever before, markets in the scenario were highly influenced and constantly changed by new and disruptive technologies. Given the vital role of the private sector in addressing hybrid threats, this exercise once again highlighted the need for a coordinated public and private sector response.

A key outcome of tabletop exercises is building crucial relationships between actors from the public and private sectors and civil society regarding crisis response. Simultaneously, they familiarise individuals from this wide range of sectors by placing them in a fictional setting that challenges complex structures of cooperation and exposes gaps and seams in law, policy and cooperative mechanisms. Given the nature of a future-based scenario, new and existing frameworks, as well as intersections of partnerships, can be identified in a no-fail environment where participants can think and speak freely.

Having pioneered the concept of the EU-NATO-private sector-civil society tabletop exercise, Friends of Europe continues to build and expand these efforts to provide more comprehensive and inclusive approaches to identifying future security issues and their solutions. Recommendations identified in Friends of Europe's 2019 and 2021 tabletop exercises have been put into practice during the Russian invasion of Ukraine with positive impacts for the entire transatlantic community. Furthermore, the new relationships and connective tissue formed during these tabletop exercises has created new public-private enterprise groups, which have been highly engaged in countering disinformation related to the coronavirus pandemic, as well as cyber and information attacks by the Kremlin in the wake of the war in Ukraine.

Participants were first given an overview of the political background of the world in 2030 and then presented with a three-stage scenario that gradually escalated into a

more complex crisis. After each stage was introduced, groups were given 45 minutes to discuss their response and identify the necessary tools and practices that needed to be implemented over the next eight years in the fictional scenario. Following each round, participants gathered in panel discussions to reflect on commonalities and differences in each group's findings. The public and private sectors learned from each other which initiatives were already underway and found possible intersections for working together to increase the efficiency and effectiveness of their emergency responses, arriving at a set of recommendations at the end of the exercise.

The exercise was held under the Chatham House Rule to promote a free and open discussion. Participants were speaking in their personal capacities.

Nature of the threat: the world in May 2030

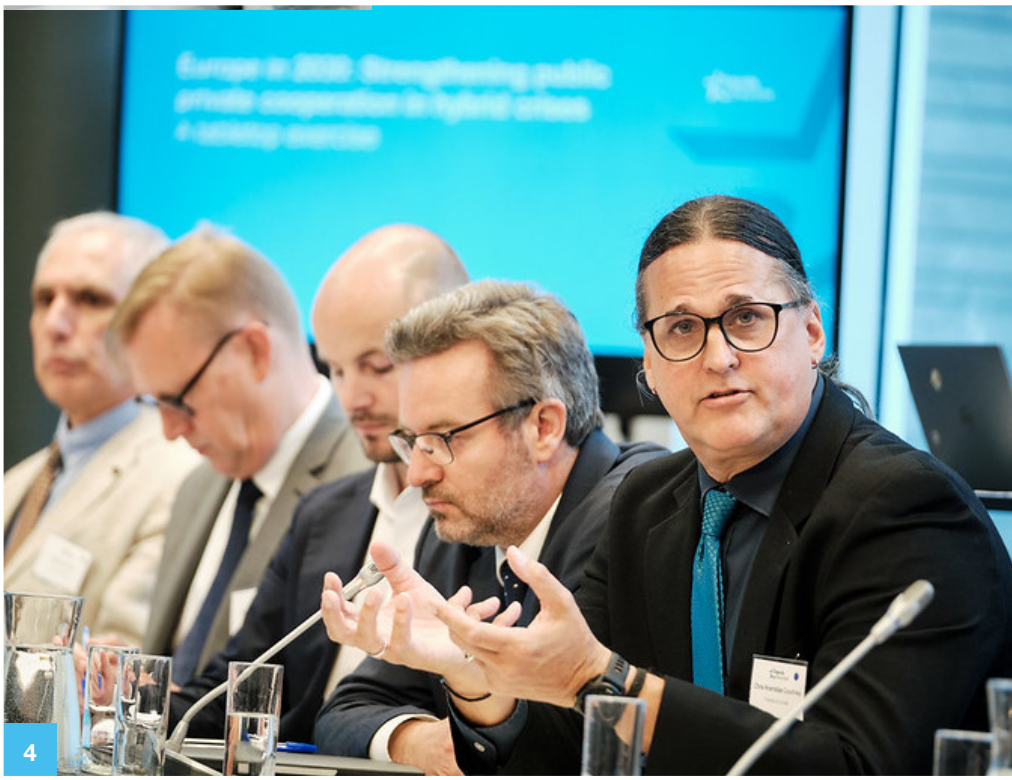
The world in 2030 was described as one in which emerging technologies – such as AI, additive manufacturing (3D printing), 6G and quantum technology – have changed and continue to change global markets substantially. Simultaneously, society was facing severe environmental issues, in particular far-reaching consequences of climate change and space debris. In addition, women maintained a more influential role in this fictional setting, controlling more than 55% of global wealth and maintaining significant influence on the priorities and practices of democratic governance.

The geopolitical background included seven fictional countries, plus citizens demanding official status for a nation created in the metaverse. The outlined states were a mix of EU, NATO and EU-NATO member states, as well as non-members. While theoretically all states were considered democratic, some were leaning towards authoritarianism.


1

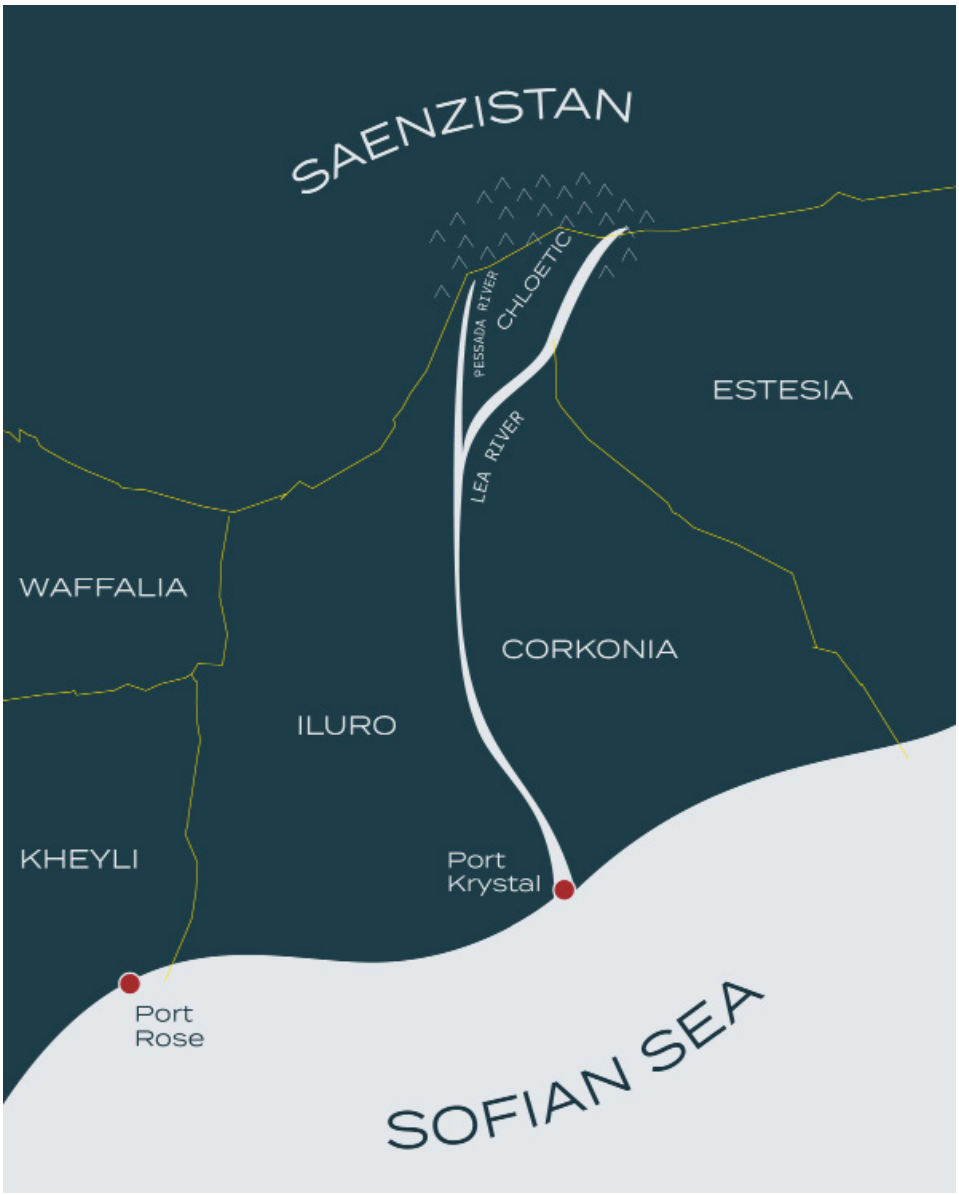

2


3


4

1. **Alice Stollmeyer**, Founder & Executive Director at Defend Democracy
2. **Jaap de Hoop Scheffer**, President of the Dutch Advisory Council on International Affairs, former NATO secretary general, former Dutch minister for foreign affairs and Trustee of Friends of Europe
3. **Julie Cairns**, Senior Staff Officer on critical infrastructure at NATO Operations Division (OPS)
4. **Chris Kremidas-Courtney**, Senior Fellow at Friends of Europe
5. **Jamie Shea**, Senior Fellow at Friends of Europe


5



Scenario

States were put under pressure through social unrest due to mistrust of widespread AI surveillance, cyber disruptions of both supply chains and an AI-driven NATO exercise, as well as disinformation campaigns. Distrust in governments and private companies led to accusations of misuse and illegal storage of private data, which only made the crisis more difficult to solve. In the development of the crisis, legal questions regarding frameworks and rules for the metaverse and disinformation campaigns, which resulted in violence and hostile attitudes towards, for example, migrants, deteriorated the situation. Furthermore, a collective failure of governments to investigate the source of cyber-attacks, as well as the unclear allocation of responsibilities for space debris after a collision between a satellite and space junk, increased the pressure on the public sector to act. Finally, a power outage, which affected several states due to energy dependencies, increased existing social unrest and supply chain issues.

Findings

Emerging technologies, regulation and cooperation

Among participants' main findings, the vulnerability of supply chain security emerged as an area of concern. 3D printing challenges the current structures and will render local manufacturing easier, paving the way for new business opportunities. However, questions were raised around intellectual property rights and the responsibilities in case of misuse, such as the private, illegal production of weapons.

AI technologies, especially when used for surveillance, require a considerable allocation of resources – for which near total societal acceptance is necessary, participants noted. One participant summarised: "The problem with reacting to crisis in an AI-led world is that the reaction is that of the machine, not of the human." Regarding the establishment of the EU AI Act, considered the first regional AI regulation worldwide, **Sacha Alanoca**, Senior AI Policy Researcher and Head of Community Development at The Future Society, asserted: "We need a clear narrative when it comes to AI technologies, especially around trustworthiness. In 10 years' time, when there is potentially more surveillance, who would not want an AI technology that is trustworthy? This is a differentiating asset for the European market, especially with the upcoming EU AI Act."

Participants also picked up on the implications of data storage by public and private entities and discussed who should be entitled to having the hold on information. Participants agreed, in principle, that data storage is beneficial in some instances, such as attribution of cyber-attacks, provided that information on who controls and 'owns' the data is transparent and easily accessible.

A representative from an EU institution noted that when it comes to data sharing, benefits must outweigh the risks, explaining that citizens are willing to share their personal data if they receive something in return. This view was widely shared across the group.

Given the prevalence of 6G technology in the scenario, another participant added the question: "Whose 6G standards will it be in 2023? Chinese, US or coming from the EU for once?" A facilitator noted that it is also "important to remember, that in 2030 [as described in the scenario], there is a transition from an interactive to an immersive world, and the new level of intensification is an issue we have to deal with."

"Are we too digitalised?" a participant asked upon discussing whether the world is able to go back to an analogue state. Concerns emerged around the consolidation of an immersive life, where people will be constantly connected, making way for questions around the right to unplug as a human right. "Can you opt-out and keep your job?" asked one participant. The question was later answered by another participant: "It should be a fundamental right to opt-out, but it would then be hard to be full citizen."

Additionally, the limits of the metaverse were widely discussed by participants, who reached the conclusion that clarity is needed around the metaverse's compliance with international law. 'Physical' states can nowadays track down citizens for statements and crimes committed online; however, the metaverse gradually puts state sovereignty into question given the international platforms it may be based on. Thus, participants agreed that law needs to be expanded to regulate this new dimension.

"Could there be a European firewall?" a facilitator asked when faced with the dilemma of how to deal with crimes committed in the metaverse. "What would potential sanctions look like?" Participants furthermore agreed that a lot of things regarding the metaverse and necessary regulation are matters of 'when' and not 'if'.

As a representative from the private sector highlighted, Europe is today lacking 300,000 trained cybersecurity staff. To this end, a member of the public security sector qualified that "classical criminals having access to new technologies are not as dangerous

> "Globally the average person spends about 11 hours online each day, and with XR, that number is expected to climb to around 14 to 16 hours per day and be a more immersive experience. So, preparing our societies for this immersive age is vital for maintaining both democracy and the rule of law.
>
> **Chris Kremidas-Courtney**, Senior Fellow at Friends of Europe

as the radicalisation of riot groups." While these groups are strongly connected to disinformation, participants noted, the establishment of other online movements with genuine shared interests should also not be overlooked.

Participants also acknowledged that adopting energy legislation at the EU level would enhance capabilities and allow for better storage. Turning to the question of quantum tools, they discussed the risk that these new technologies could represent if accessible to non-state actors. Indeed, it would mark the end of encryption as we know it. It may even temporarily compromise the reliability of all data.

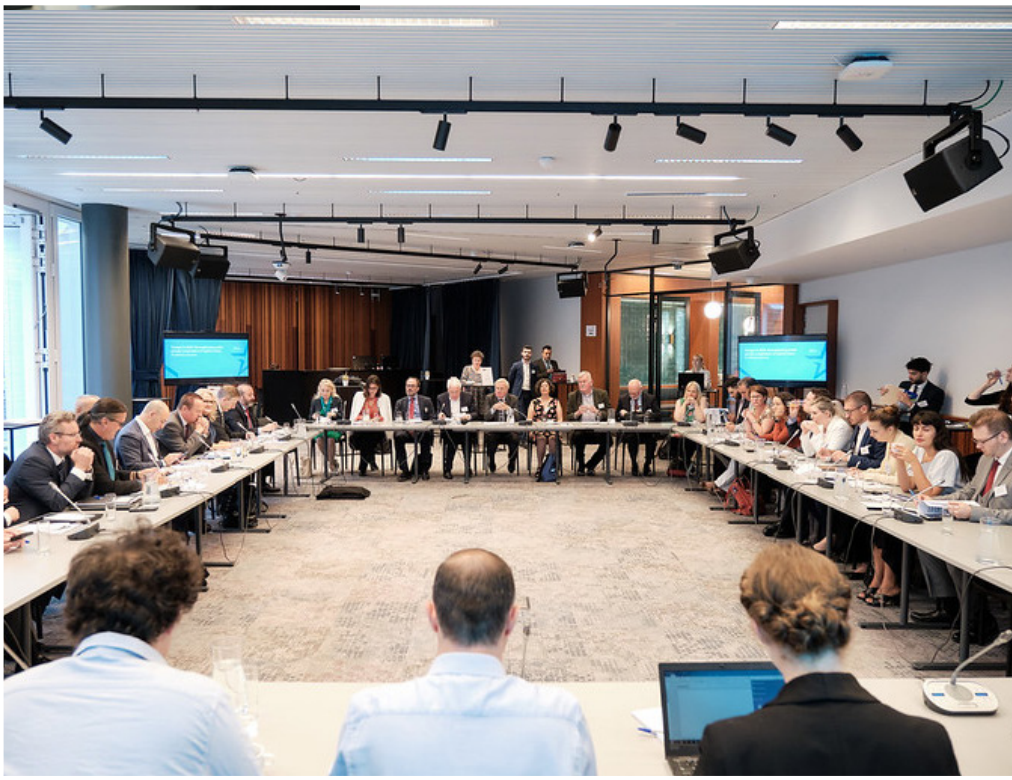
Without preparedness, regulation and effective disinformation prevention on the EU level, it could turn into "a poison without an antidote" as one participant concluded. Another warned to not fall into the trap of over-regulating, stating that "you wait, you see, and then you regulate. Sometimes you let the thing evolve, and then you regulate."

"Anticipating is not the same as over-regulating," another participant countered. "It's just a question of balance. We don't know where we will be in the near future – just look at the last five years."


1


2


3



1. **Elizabeth Wiltshire**, Programme Manager at Friends of Europe
2. **Juha Heikkila**, Head of Unit for Robotics and Artificial Intelligence at the European Commission Directorate-General for Communications Networks, Content & Technology (DG CNECT)
3. **Andrea G. Rodriguez**, Lead Digital Policy Analyst at the European Policy Centre (EPC)
4. **Sacha Alanoca**, Senior AI Policy Researcher & Head of Community Development at The Future Society


5

Making institutions fit for the future

Participants' findings furthermore focused on the limitations to current military mobility. A participant from NATO asked: "When I look at AI-led trucks, reprogramming ships, etc., do we have the skills needed for the future?"

Paul Taylor, Senior Fellow at Friends of Europe, explained how a NATO admiral had to tell his captains to revert to old-fashioned pre-digital navigation techniques to counter GPS jamming and spoofing by the Russians during a NATO exercise. He asked: "Can we get a car back on manual? Can we get ships back in port? Can we override a hostile takeover of the programming system?" Competition with the private sector for human resources that have these skills can be mitigated through outsourcing, which is, in itself, not exempt from risks.

Participants expressed the importance of communicating on the real-life violence that can originate from disinformation campaigns. Especially as younger generations spend more and more time online, it is important "to clamp down much more forcefully on sources of disinformation," one participant said. The violence based on it needs to be made much more visible by security authorities through clearly naming disinformation as a source and educating people about polarisation and radicalisation through such campaigns. In addition, the implementation of social safety nets is necessary to combat disinformation, such as establishing disinformation first responders.

Consequently, this also means implementing safeguards to improve their protection and an overall more active role of law enforcement institutions within cyberspace and, subsequently, the metaverse. "Empirical research has demonstrated that social media facilitates division," one participant warned. "If we continue as we are today, we may not have many functioning democracies in five years' time."

Participants shared that EU and NATO-wide initiatives are partly already in place. Whereas the EU is focussing on improving information sharing based on lessons learned from the pandemic, NATO is working with member states to brief them on resilience and civil communication. This is all the more important when looking at "post-COVID rejection of the pillars of society", as one participant said. They went on to explain that for parts of the younger generation and ethnic minorities, "public authorities and the police are not your friends. We now have an opportunity to think about this."

Similar to the emerging metaverse, dealing with space requires updated treaties. Regarding space debris, two treaties from 1967 and 1972 are currently in place.[2] The consensus among participants was here that the EU needs to give the first impulse and others need to follow. As one participant described it: "Space junk as a problem is comparable to climate change but without an organisation to give it a voice." New treaties most urgently have to address the question of responsibility with already 35,000 parts of trackable space junk in lower orbit.

[2]Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967), and Convention on International Liability for Damage Caused by Space Objects (1972)

Based on the current treaties, states are ultimately responsible, while in reality, private companies are increasingly active in space and do not necessarily respect international commitments made by their countries of origin or incorporations. One expert from the private sector raised the concern that "creating liability in space is deemed to be a challenging task, especially given how doing that on earth is often impossible." In addition, the promotion of state-sponsored innovations was discussed as a possible solution for increased cooperation and a clearer delineation of responsibilities.

Once again, trust was identified as an absolute requirement on various levels. One participant raised the question: "Is the age of enlightenment over?" After a wave of prominence and respect during the beginning of the pandemic, experts are now losing trust and credibility as an increasing polarisation of society continues to develop.

In all debates of the day, it became clear that **trust in governments – a key ingredient of resilient societies – is being challenged more than ever.** To counter this trend, consensus prevailed that enhancing transparency of and citizens' participation in policymaking processes is indispensable to digital democracy.

As one facilitator put it: "In such a troubled and troubling world, doing business as usual will only exacerbate existing problems – not to mention create new ones." Another participant added: "The current crisis shows us many inequalities. Maybe this is an opportunity to confront ourselves. Technology is not neutral. We need the people who are impacted at the policy table."

In addition to transparency and citizens' participation, participants also acknowledged the importance of **intergenerational dialogue as a means to advance and sustain societal resilience.** Reflecting on the issue, one of the moderators asserted the need "to listen to young people and delegate power to them".

Combining a few of the overarching topics discussed during the tabletop exercise, participant **Alice Stollmeyer**, Founder and Executive Director at Defend Democracy, drew the following conclusion: "We should co-design technologies with values by-design, involving not just the private sector but also the public sector — and let's not forget about civil society. We need a whole-of-society approach to prevent anti-democratic technologies from coming into being." This incorporates trust, regulation, system resilience and foresight.

Recommendations: how can Europe be ready for the world in 2030?

A Europe that is pro-active, not reactive

The Digital Services Act, European Democracy Action Plan, legal framework for AI and General Data Protection Regulation (GDPR) are a good start, but each will require constant updates to remain effective. Regardless, we will need more stringent transparency regulation of technology companies to protect citizens, their privacy and society as a whole. We must also adapt the EU workforce and society for the age of immersive technologies. Nonetheless, EU regulators must ensure that new norms and standards do not stifle innovation. On this point, raising their concerns, a participant from the private sector noted: "When done in reaction, regulation in most cases kills innovation more than it solves problems."

As far as climate change mitigation and adaptation are concerned, it is important to keep in mind that while new technologies can reduce our carbon footprint, they will increase our demand for electricity. Figuring out how to address this new demand without burning more fossil fuels is an urgent challenge for the energy sector and EU leaders.

Digital sovereignty in 2030 means regulating the metaverse

EU and national legislation seeking to regulate the digital universe will need to be updated frequently to take account of new technological developments such as the metaverse(s), where it is anticipated that millions of people will spend ever more of their waking hours by 2030. Participants agreed that more widespread use of immersive technologies and personal modifications available within the metaverse(s) may also lead citizens to new ideas about identity and citizenship.

Seek greater transatlantic cooperation

The EU should use the recently created Trade and Technology Council with the US to address these issues and then widen the regulatory forum to other like-minded democracies. It should move fast to use the window of opportunity with a US administration that is open to technology regulation, before the possible return of a nationalist, anti-regulatory administration.

Prepare for the age of immersive technologies

Given the risks identified by the early arrival of quantum technology, the EU and its member states should identify and prioritise key information systems and seek a public-private approach to address these responsibilities to achieve faster results. Updates to regulations will require more attention and not only in terms of content published

in cyberspace. Going beyond mere fact checking, regulation will also require much attention on platform governance and the risks associated with microtargeting and audience manipulation.

Few studies are being conducted on the impact of XR on individuals and almost no studies exist on their impacts on groups and societies. The EU should earmark funding to support the latter to better inform the public and enable policymakers and technology regulators to improve foresight and decision-making.

One outcome of these studies may indicate the need for the active defence of citizens and societies within the XR metaverse, especially as parallel economies and societies (which already exist) begin to grow within them. In any case, we will need to develop and agree on a new governance framework in which we define and balance rights and responsibilities within the immersive digital world.

Prepare for the Quantum Age

Given the risks identified by the early arrival of quantum technology, the EU and its member states should **identify key systems of cooperation and responsibilities in the government and private sector.** Additionally, several strategies for the transition to quantum-resilient cybersecurity need to be explored, as well as substantial funding to accelerate the process. Protecting the private data of citizens must be prioritised within this effort at the earliest stages.

Next, they must **address the ongoing shortage of cybersecurity experts** and start training prospective experts in the use of AI tools and quantum cybersecurity to grow Europe's talent pool. This may be best be achieved through a federated public-private partnership (PPP) that is funded by the EU and implemented by the member states and tech companies.

"We should talk about how to upgrade our educational system, so the next generation is better equipped than we are," said one participant. Another one added: "I don't think we are prepared as citizens to be able to do our part. I don't think we understand that electricity powers everything we do. When there is a major power cut, who will go and fix it? When the NATO vehicles are all hacked into, who will go and fix that?" It will be important to work out this problem through entire systems, "so we don't just lose one person and lose all the necessary knowledge", stressed another participant.

Finally, **funding for quantum research and development (R&D)** should continue and member states should be supported in developing AI-enabled organisations and industries.

Define a new EU social compact

Our efforts to prepare for 2030 will fail if the EU does not **reduce economic inequality and define the relationship between the state and the individual**, achieving a balance between social welfare and individual enterprise. Digital advances can emancipate or imprison; level the economic playing field or exacerbate the socio-economic divide; enhance justice and the rule of law or lead to a more chaotic and unjust order. "We need to really understand the problem to disrupt what's happening. This means an increased focus for EU countries on education and diplomacy in the offline world," one participant concluded. In light of future-projected job losses as a result of new disruptive technologies, tackling inequality remains an important

aspect today. Additionally, **XR technologies present a danger of exacerbating inequality** and the weakening of societal cohesion and resilience if we don't think and act together with foresight.

> "For all its faults, the liberal democracy we have is worth saving. And of course, it's the job of everyone to get involved for that particular task of saving it, and not to rely upon just one generation or one branch of society to save it or to take the blame.
>
> **Jamie Shea**, Senior Fellow at Friends of Europe

Tackling inequality also means **closing the gap between older generations and digital natives.** In addition to digital training for all age groups, intergenerational dialogues and the delegation of power to younger people, especially regarding emerging technologies, are necessary. The EU needs to understand that there are differences between generations regarding the willingness to disclose private data online and the perception of rights in the digital environment. Younger people "don't value privacy like older generations do," as one participant said. Younger generations trust private companies more easily with their data based on the perception that they use the latest technologies and security standards. As a participant from the private sector rightfully noted: "At a time when new generations attach overwhelming importance to digital interactions, regulating digital could be perceived as young people as a denial of their free spaces and rights." Cooperation between public and private sector is here essential to instate trust in institutions and governments.

Climate migrants initially trigger community mobilisation for solidarity and the EU Temporary Protection Directive offers a consistent legal framework to integrate newcomers. But, if this is not supported by structural government investments in additional capacity of public services, such as housing, health and education, it can exacerbate social tensions and fuel extremist movements. Europe needs to develop **a coherent narrative and identity with a framework for legal migration and an approach for meeting international commitments on accepting refugees.** Furthermore, cities need to adapt – not only to climate change, but also to changes within society. The EU needs to draw lessons learned regarding effective integration from large refugee and migrant movements witnessed in Europe in 2015 and currently as a consequence of the war in Ukraine.

Set global rules for tech and space regulation

The EU must continue to **set global rules for tech and space regulation according to open and transparent democratic norms** that respect the rights of the individual and diversity of information and opinion. The EU's strength as a normative power is well recognised and effective in the present but may lose influence in the technology

arena as the power of market access loses its sway in a world where the West is no longer the global economic centre of gravity.

For the EU to assert its technology standards globally, it must be a leader in at least a few key technology areas, such as digital goods, intellectual property or cloud computing, to name a few. A critical area to focus on is setting standards for the attribution for goods manufactured by additive manufacturing (AM) since this will be an important aspect not only to prevent weapons proliferation but to protect intellectual property rights.

The EU will need to strive for **more stringent transparency regulation of technology companies** to protect citizens and society as a whole. It will also need to maintain better situational awareness of what updates and regulation changes are required as developments unfold. **Public-private dialogue on future technologies and their impact on society cannot lie solely with big companies.** SMEs must be part of the process, especially since they are often on the cutting edge of various developments.

The Union must strengthen its research and innovation base to better compete globally while protecting the EU's social market model. Currently, the EU trails major global economic competitors in R&D funding, with Japan leading at 3.2% of GDP, the US in second with 2.79%, followed by China at 2.07% and the EU at 2.03%.

The EU's growth in the new digital economy and preparedness for the Quantum Age can only be maintained if the Union can increase R&D funding to 3% of GDP and targets it at advances to maximise its competitive advantages. It will also require new focus on building digital infrastructure and continued technical education funding to produce a high-performing, digitally literate Europe.

Europe should also upgrade its technology patent and venture capital ecosystem to keep more of the EU's innovation and talent in Europe rather than forcing them to seek friendlier environments to seek patents and growth capital.

Look beyond the West for best practices

Some of the best practices for how to make digitalisation strengthen democracy and not weaken it are found in Asia. For example, Taiwanese Digital Minister Audrey Tang's approach to **increasing transparency and citizen engagement via digital means** is a practice EU member states should seek to learn from and emulate.

List of participants

Sacha Alanoca
Senior AI Policy Researcher & Head of Community Development at The Future Society

Sari Arho Havren
Counsellor and Senior Advisor at Business Finland

Cristiana Lavinia Badulescu
Co-founder and Head of Research & Policy at Sigma Think Tank, and Co-Managing Director of Young Professionals in Foreign Policy (YPFP)

Xavier Bento
Programme Assistant at Friends of Europe

Jim Bergeron
Political Adviser at NATO Maritime Command (MARCOM)

Julie Cairns
Senior staff officer on critical infrastructure at NATO Operations Division (OPS)

Geert Cami
Co-Founder and Secretary-General at Friends of Europe

Edoardo Camilli
Co-Founder & CEO at Hozint - Horizon Intelligence, and 2017 European Young Leader (EYL40)

Jaap de Hoop Scheffer
Former NATO secretary general, former Dutch minister of foreign affairs, President of the Dutch Advisory Council on International Affairs, and Trustee of Friends of Europe

Kostas Dervenis
Cyber-security expert, corporate professional and author

Deniz Duru Aydin
Product Policy Manager – Misinformation at Meta

Alejandro Esteso
Programme Executive at Friends of Europe

Alexander Fotescu
Global Affairs, Innovation, Strategy & Human Capital at Smartlink Communications

Andrea G. Rodriguez
Lead Digital Policy Analyst at the European Policy Centre (EPC)

Jessica Giandomenico
Head of Research and Analysis at Earhart Business Protection Agency

Caroline Groene
Cyber Policy Advisor at Microsoft

Juha Heikkila
Head of Unit for Robotics and Artificial Intelligence at the European Commission Directorate-General for Communications Networks, Content & Technology (CNECT)

Jimmy Jaber Bringas
President of Uniport Bilbao, and Founding Partner and CEO of Sparber Group

Khan Jahier
Lead Resilience Staff Officer at the Enablement & Resilience Section at NATO, Defence Policy and Planning Division (DPP)

Rainer Jungwirth
Project Officer for Technology Innovation in Security at the European Commission Joint Research Centre: Space, Security and Migration (ISPRA)

Pawel Kasprzyk
Deputy Director for Training and Exercises at The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Chris Kremidas Courtney
Senior Fellow for Peace and Security at Friends of Europe

Mindaugas Lašas
Head of Sector - Hybrid Threats at the European External Action Service (EEAS) Service of Deputy Secretary General CSDP and crisis response

Terhi Lehtinen
Head of Division - Horizontal Coordination, European External Action Service (EEAS), European Union Military Committee (EUMS)

Hanna Linderstål
CEO at Earhart Business Protection Agency

Lena Loch
Programme Assistant at Friends of Europe

Guillaume Loonis-Quelen
Maritime and space law expert

Tarik Meziani
Head of Unit - Media Operations at the Council of the European Union Directorate-General for Communication and Information (COMM)

Francisco Javier Molinera De Diego
Police Superintendent - Multilateral Cooperation Section at the Spanish National Police

Konstantinos Ntantinos
Policy Assistant to the Vice-President of the European Commission, Cabinet of Vice-President Margaritis Schinas

Franck Peinaud
International and European Affairs Senior Advisor at the National Gendarmerie

Shaun Romeril
Lead consultant at 2creatEffects, former police officer at the Metropolitan Police and senior advisor for counter terrorism strategy

Tamsin Rose
Senior Fellow at Friends of Europe

Jamie Shea
Senior Fellow at Friends of Europe

Richard Spearman
Senior External Affairs Advisor for Security and Resilience at Vodafone

Sabrina Spieleder
Information and Communication Officer - Division Strategic Communications at the European External Action Service (EEAS)

Simon Stermann
Policy Officer - Civil Protection Horizontal Issues at the European Commission Directorate-General for Humanitarian Aid and Civil Protection (ECHO)

Alice Stollmeijer
Founder & Executive Director at Defend Democracy

Paul Taylor
Senior Fellow at Friends of Europe and Contributing Editor at Politico

Sam Traynor
Product Policy Manager - Inauthentic Behavior at Meta

Florin Urseanu
Head of Unit - Crisis Management, European Commission Secretariat-General

Juan Luis Valero
Head of Brussels Office, European Union Satellite Centre (EUSC) EU SatCen

Nicholas Vinocur
Editor at Politico Pro

Rayan Vugdalic
Programme Officer at Friends of Europe

Elizabeth Wiltshire
Programme Manager at Friends of Europe

Friends of Europe
Connect. Debate. Change.

juraj.majcin@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think-tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.