EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY BRIEF

THE GEOPOLITICS OF TECHNOLOGY: HOW THE EU CAN BECOME A GLOBAL PLAYER

Julian Ringhof, José Ignacio Torreblanca

May 2022

SUMMARY

- Battles in the digital space have taken centre stage in today's global power struggles. The EU cannot stay aside.
- To become a geopolitical actor, the EU needs to learn to play global technology politics and should adopt an ambitious digital diplomacy strategy.
- A digital diplomacy strategy will enable the EU to better defend its values, enhance its security, and foster digital markets at home and worldwide.
- To counter Chinese and Russian influence in the technology realm, the EU should build digital alliances with like-minded countries. The EU needs to seek greater convergence with the US and other Western allies, and offer the global south an attractive alternative path to digital development.
- For the European External Action Service and the European Commission to succeed in this task, the concurrence of the EU institutions, the member states, and a variety of private stakeholders is essential.

Introduction

Today's major powers engage in comprehensive global technology politics. The weaponisation, mastering, and control of digital technologies is the new 'Great Game'. These power dynamics are helping shape technological spheres of influence. Countries in Latin America and the Caribbean, Africa, and the Indo-Pacific – but also in central Eastern Europe and the Balkans – have fallen or may soon fall under Chinese or Russian technological influence or dominance. China is luring countries into technological dependencies to undermine their political sovereignty through its Digital Silk Road (DSR) initiative. Beijing also shields its own citizens from foreign influence with its 'great firewall' and develops industrial strategies to secure its technological autonomy from the West. It uses digital disinformation to influence public opinion in other countries, mounts cyberattacks and cyberespionage to strengthen its industrial base, strategically deploys attractively-priced 5G technologies abroad to gain control of telecom networks, and tries to impose its technical standards through international organisations.

Together with Russia, China is attempting to ingrain authoritarian values into the global cyberspace. Russia is also leveraging and restricting mass media and social networks to protect its interests, shielding its population from democratic temptations, and waging an information war against the West and its allies with the aim of undermining citizens' faith in democracy.

Meanwhile, the United States tries to offset Chinese and Russian influence, seeks to maintain its cutting-edge advantage on military artificial intelligence (AI) and other technologies, and backs and protects the interests of its major technology companies globally. It also denies other nations access to key technologies, monitors critical investments in the technology sector to avoid security risks, seeks to secure and control critical supply chains (especially of semiconductors), and imposes export controls and even embargoes on sensitive technologies.

As for the European Union, the Brussels institutions are trying to shape global standards of privacy and data protection, digital platforms, and AI according to European values using the attractiveness and power of its internal market. The EU also promotes digital partnerships with like-minded countries and allies – and announced, in December 2021, the "Global Gateway" initiative as the EU version of China's DSR.

All this implies that the EU has begun to play the global technology game. But it is nowhere near its rivals in terms of sophistication, strategy, resources, and vision. If the EU is to learn to speak the language of power, it needs to understand its efforts as part of an integrated digital strategy that can both cooperate and compete with those of China, Russia, and even the US.

The war in Ukraine is helping this EU strategy process. The war has become an accelerator of existing trends and challenges, turning technology into yet another key battleground. Before the war, the EU had already decided it needed to become a geopolitical actor. Indeed, Ursula von der Leyen declared in 2019 that she intended to form a "Geopolitical Commission". One can already see the effects of this new orientation in areas such as trade, defence, health, and digital technologies. The European Commission has already launched a variety of ambitious initiatives at the nexus of geopolitics and technology: digital partnerships with Japan and Singapore; the EU-US and the EU-India Trade and Technology Councils (TTCs); the Strategic Compass; and the Global Gateway.

But since the Russian invasion of Ukraine, the EU has found a renewed impetus to engage in global technology politics. The EU has expanded its assistance to Ukraine both in the cybersecurity and disinformation domains. It has also approved a comprehensive set of technology sanctions and renewed its commitment to strengthening EU technological sovereignty. Meanwhile, Russia and China have cemented their 'no-limits' alliance and committed themselves to accelerate their technological decoupling from the West.

At this difficult moment, the EU should speed up its plan to become a global technology player. It is now time to put all the union's technological and digital capabilities behind one vision and devise a joint strategy to deploy them. This paper sets out how the EU might accomplish that critical task. In the first section, its lays out the vision and the goals of such a strategy. Section two takes stock of EU technology and external digital policy initiatives so far. The next three sections look at what the EU should do along three digital diplomacy dimensions (values, security, and markets). Finally, the paper proposes a series of policy recommendations to help the EU bridge its current gap and move from its current stance to the status of a fully committed and capable global technology actor.

A digital vision

If the EU is to invest in setting up its own digital and technology foreign policy, it needs to be clear about what its goals are. The ultimate aim of this policy should be to give the EU both the strategy and the tools to transform it into a global technological actor able to sustain its interests and values at home and abroad, and in competition and cooperation with other powers. All the elements laid out in

this brief are therefore focused on turning the EU into a capable and effective geopolitical actor in the field of digital technology.

The need for such a strategy is clear. The EU has set itself the goal of becoming a technologically advanced and decarbonised economy. The success of this major economic transition crucially depends on the EU's capacity to master, command, and have full and unrestricted access to critical digital technologies. These technologies are increasingly contested, disputed, and even weaponised by third actors. Access to them may thus be denied or made conditional on political goals, jeopardising this transition. In a worst-case scenario, rather than allowing the EU to become a more autonomous and powerful actor, the transition to a digital and decarbonised economy may create new vulnerabilities and simply change the nature of the EU's geopolitical and economic dependence.

The future of the EU also depends on its capacity to sustain democracy and democratic institutions, both at home and abroad. However, for 15 consecutive years, democracy has been in decline around the world, both in the number and in the quality of democracies. Coincident with this decline, both born-again and long-standing authoritarian regimes are growing stronger and more challenging. Misuse of digital technologies has contributed to these trends. This not only serves to undermine democracies by fuelling political polarisation and providing the tools for foreign influence operations, but it also helps authoritarian governments cement their grip on their citizens. Countering these trends is not only a moral necessity for the EU but also essential to securing its global interests.

The vision behind EU digital policy should thus be to secure and promote both its economic power base and its political model, at home and globally. To achieve this vision, the EU needs to act strategically. Acting strategically means that in designing its means and ends, the union needs to understand what other countries and powers are doing and how it plans to compete and cooperate with them. China and Russia have started a process of decoupling from the West, to which they seek to attract other countries. The rules-based order is being replaced by a power-based order. Geoeconomics (or sheer mercantilism) is back. States are using economic and technological interdependencies to impose their views and secure their geopolitical interests. It is a new world order – and in that world, technology becomes a key element of power, sovereignty, and survival.

To secure its interests, values, and global standing, the EU should embed its open-market and human-centric approach to technology in its alliances, partnerships, and the multilateral organisations to which it belongs. In a world where technology is disputed and weaponised, the more technologically sovereign like-minded countries are, the more the EU's own sovereignty and its global geo-technology standing are assured; the more allies are protected against foreign influence operations, cyberattacks, and coercion derived from technological vulnerabilities, the more alignment and cooperation with the

EU at the global level will be facilitated. The EU should therefore aim not at technological independence but at mutually reinforced and shared technological sovereignty with its allies.

To achieve this aim, the EU first needs to become an attractive partner for other countries. This attraction should extend to those who have signed up to Chinese digital infrastructures and investments or are targeted by China's, Russia's, and other countries' propaganda and influence operations. The Global Gateway initiative can help this process if it focuses on strategic opportunities to strengthen alliances and undermine Chinese and Russian spheres of influence.

The EU also needs to strengthen its existing alliances. This need affects first and most fundamentally the US, but also applies to other partners. With the US, which in many fields is a technology competitor, the EU must settle its differences. The EU and the US have distinct approaches to technology governance. In Europe, values and regulation play a greater role than they do in the US. This distinction has so far prevented regulatory harmonisation and led to tensions. Still, while these differences may prevent policy harmonisation, they should still allow policy convergence, or at least coexistence – particularly given the common global challenges the EU and the US face. Clearly, the EU and the US cannot counter Russia's and China's aggressive technological strategies while refusing to compromise among themselves. Much as they did after the second world war, the US and Europe need to reach a wide agreement to sustain a global and free democratic technology order. The post-war order required rules-based institutions and military alliances to secure free trade across key straits and blue waters. The new order will require the transatlantic alliance to work together to facilitate a flow of data that preserves privacy, and to embed democratic values in technology regulations and governance at the global level. In sum, to stand up for its interests and values, the EU must become a global technology player. The EU and its member states can deliver on this vision by acting along three policy dimensions (values, security, and markets) with a common strategy and new and enhanced policy tools. As the next section shows, the EU is already on the road to global influence in technology. But it has a long way to go, and the most difficult part still lies ahead.

The EU: a geo-technology player in the making

In the last decade, the EU has gradually woken up to the geopolitical implications of digital technologies. This awakening can be linked to a series of events beginning in 2013 with the disclosures by former NSA employee Edward Snowden followed by Russian interference in the 2016 US presidential election, the Brexit referendum, the 2019 European Parliament election, and various EU member states' national elections. The Cambridge Analytica scandal in 2018 helped put the spotlight on big US technology companies and the need to better regulate them. Similarly, the onset of international discussions over the Chinese 5G provider Huawei that same year raised greater

awareness of EU technology vulnerabilities.

In parallel to this, the global impact of the EU's 2018 General Data Protection Regulation (GDPR), even if unexpected, turned the EU into a global technology actor and showed it the way to leverage the attractiveness and power of its internal market. Equipped with these influential regulatory tools, the EU is now seeking to become the global leader in the regulation of digital technologies. EU digital legislation is no longer just inward-looking. The union now proactively seeks to leverage its regulatory capacity and nurture digital partnerships and alliances to globally project its values. Building on previous successes, the EU is now in the process of implementing innovative regulatory regimes for AI, data governance, and digital platforms that, like the GDPR, have the potential to go global.

This new geopolitical logic underpins several new EU geo-technology initiatives. In the EU-US TTC, launched in 2021, the union and the US are currently negotiating enhanced cooperation in technology and standards development, digital regulation, connectivity investments, and the security aspects of advanced technologies. The swift and harmonised EU and US export controls on advanced technologies imposed on Russia after the invasion of Ukraine in February this year are the first success story of this new transatlantic technology cooperation.

Beyond the EU-US TTC, the EU has announced a new TTC with India, launched its first digital partnership with Japan, while negotiating additional partnerships with Singapore and South Korea. With the Global Gateway initiative, the EU seeks to link digital development investments in lower income countries with values-based digital regulation and geopolitical thinking.

The EU has also taken steps to reduce its technological vulnerabilities and asymmetric dependencies through investment in technological capabilities. These efforts have been heavily influenced by China's technological assertiveness, the US-EU technology clashes during the Trump administration, and most recently the Russian invasion of Ukraine. Along these lines, the EU has developed new instruments and cooperation mechanisms, such as the Toolbox for 5G security and the Joint Cyber Unit, to secure EU cyberspace.

To further strengthen its technological capabilities and reduce its asymmetric dependencies, the union is decisively investing in the development of critical technologies including semiconductors, through the European Chips Act; supercomputing, through the European High-Performance Computing Joint Undertaking; and 6G development, for example, through the Hexa-X project. Moreover, the EU has rolled out a host of strategies addressing issues at the nexus of digital technology and geopolitics, including the 2030 Digital Compass, the Strategic Compass, the Cybersecurity Strategy, and the Standardisation Strategy. The breadth of the issues addressed in these various efforts underscore the ubiquity of geo-technological dynamics across diverse policy fields.

While the EU was building its digital standing, Russia invaded Ukraine for the second time. As so often, war became an accelerator of existing trends. Long before Russia's invasion on 24 February, Ukraine had become ground zero for Russian digital and hybrid warfare, with hundreds of thousands of cyber-attacks and mass disinformation campaigns intended to destabilise the country, undermine Ukraine's democratically elected government, confuse Western public opinion, and ensure the global south will rally around Russia.

In its response to the war, the West has deployed massive sanctions on advanced technologies with the intention of paralysing Russia's industrial base and weakening its military capabilities. And while the Kremlin has prohibited and blocked several foreign digital platforms in Russia to impede the flow of outside information into the country, many other Western technology companies independently decided to cease operating in Russia. Both developments foreshadow a new digital iron curtain. The war in Ukraine has already demonstrated that digital technologies now shape the response to international conflict.

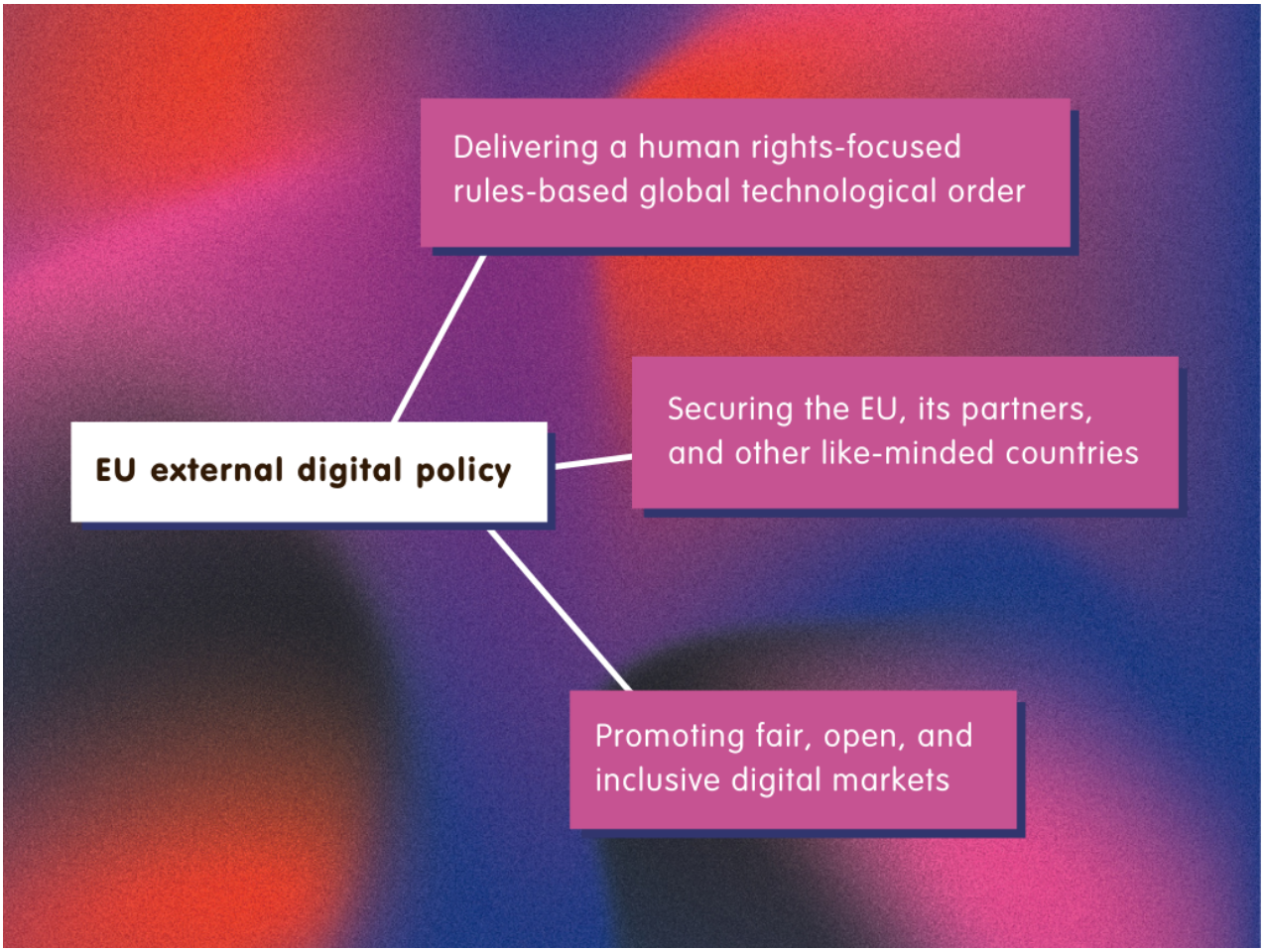
The legislative and policy measures taken so far by the EU are commendable. However, there is still much to do. The EU continues to be a technology research powerhouse, but its success in the commercialisation and the securing of significant market shares in digital technologies has been limited. Today, Europe is lagging in the development of advanced technologies including semiconductors, AI, and cloud and high-performance computing.

As the EU rolls out initiative after initiative, a cohesive strategy is missing to tie these measures together to improve coordination, set priorities, and identify gaps. Due to a lack of information, resources, and engagement the union is currently not realising its full potential – and not reaping the full geopolitical benefits of its digital policy efforts. Because such an overarching framework is lacking, important information is not flowing between the relevant Brussels and member state institutions and towards the EU delegations around the world that play a crucial role in forwarding European digital foreign policy interests.

Both the European Commission and the member states have identified these challenges. The commission's 2030 Digital Compass, approved in March 2020, said that the EU needs a "comprehensive and coordinated approach to digital coalition-building and diplomatic outreach". This is a position shared by the member states, which at the 12 July 2021 Foreign Affairs Council (FAC) called for the EU high representative and vice president (HRVP) and the commission "to formulate a comprehensive, ambitious European external digital policy in coherence with existing internal policies".

The diagnosis is clear. If the EU wants to become a global technology actor, it must develop and deploy digital diplomacy tools. The next three sections spell out in detail how to deliver on this mandate and propose a policy approach along three dimensions: values, security, and markets. More precisely, they lay out a path:

1. to promote a human rights-focused and rules-based global technological order;
2. to secure the EU, its partners, and other like-minded countries in the analogical and digital worlds;
3. to promote fair, open, sustainable, and inclusive digital markets.


Delivering a human rights-focused rules-based global technological order
Securing the EU, its partners, and other like-minded countries
EU external digital policy
Promoting fair, open, and inclusive digital markets

Promoting human rights and a rules-based global technological order

- Between 2014 and 2020, foreign powers attempted to interfere in 33 elections, collectively involving 1.7 billion people. The misuse of digital technologies has eroded citizens' trust in technology companies and damaged democratic politics all over the world.
- Authoritarian regimes have used advanced digital technologies to strengthen their grip on power and step up repression on dissidents. In 2021, global internet freedom declined for the 15th consecutive year. More internet users were arrested for non-violent political, social, or religious speech in 2021 than ever before.
- Online hate speech and disinformation continue to spread division, violence, and distrust around the world. In 2017, disinformation and hate speech on social media contributed to the genocide of the Rohingya in Myanmar. During the covid pandemic, Bolivia was particularly afflicted by misinformation on dubious cures leading to exceptionally high infection and low vaccination rates.
- Between 2016 and 2019, every submission on surveillance technology standards to the UN's International Telecommunication Union was made by Chinese companies.

According to a paper endorsed by all EU member states in July 2021, "technology and online platforms can be a tool for democratic mobilization and enable a global positive transformation for human rights promotion and protection."[1] But as illustrated by the vast Russian disinformation campaigns in recent years, the very same digital technologies can be used as weapons for eroding the rules-based order and impairing the functioning of democracy.

It does not take war or bellicose autocrats for digital technologies to threaten human rights and democratic processes in Europe and beyond. As digital platforms have become essential forums for social and political engagement, hate speech and information bubbles resulting from "dangerous algorithms" have undermined social cohesion and democratic participation. Decreasing media diversity resulting from anti-competitive practices, and diminishing freedom of the press and

expression online resulting from digital censorship regimes pose significant threats to democratic development.

Internet shutdowns are used by autocratic and democratic governments alike to prevent protests and hide governmental actions. AI is used for all-encompassing surveillance of citizens. Vast amounts of data on citizens, journalists, and officials is exploited by governments within and across borders to refine propaganda and "guide public opinion". Foreign election interference campaigns on digital platforms have become a big issue for democracies around the world. The widespread violation of data privacy and the deployment of discriminatory algorithms by technology companies and government authorities alike undermine democratic values from within.

The lack of international cooperation on technology regulation and the 'geopoliticisation' of technology standards contributes to further fragmentation of the global digital ecosystem. As it stands, the massive data flows between the US and the EU – among the highest cross-border data flows in the world, underpinning digital trade worth more than $264 billion in 2020 – stand on shaky legal ground. Today, the EU has only recognised 14 countries as providing adequate data protection, thereby allowing personal data to flow freely to and from Europe.

Technology standards, which are essential to allow for interoperability between systems and to guarantee agreed upon levels of security, have meanwhile become a field of geopolitical competition. The battles take place in international standards organisations, where China and Russia have redoubled their efforts to build autocratic norms in digital technology standards, such as those for 5G telecoms or surveillance equipment.

Many thinkers in the West have long believed that digital technologies like the internet and social media platforms would inherently spread democratic liberal values around the world and unrestrictedly connect economies and people. In hindsight, this view was naïve. China managed to nail jelly to the wall and control and misuse the internet to reinforce its authoritarian regime. Now, a similar digital curtain is rising over Russia. This anti-democratic use of digital technologies is testing established democracies. And a 'splinternet' appears to be around the corner as global digital protectionism rises and international cooperation diminishes.

These developments imply that preventing democracy and human rights from being undermined by technology misuse and abuse, both at home and abroad, must be the EU's number one priority.

The successful international proliferation of Europe's GDPR showed how EU democratic norms can shape global standards on privacy issues. The Digital Services Act (DSA) and the Digital Markets Act, which "aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses

", as well as European regulations on artificial intelligence and data governance, have the potential to yield similar global effects.

Yet, the EU cannot sit back and wait for international spillover effects of these regulations to take off. Europe must seek greater regulatory rapprochement with its allies and further increase coordinated activity and build alliances in the technology forums of multilateral institutions, including the UN's International Telecommunication Union (ITU), and technology standards bodies such as the International Organization for Standardization.

EU initiatives such as the EU-US and EU-India TTCs; the digital partnerships with Japan, South Korea, and Singapore; or the Global Partnership on Artificial Intelligence at the OECD, have great potential to shape democratic technology standards globally. They should therefore be fully supported. Similarly, measures "to support the EU's leading position as a forerunner in key technologies" proposed in the Strategy on Standardisation are laudable. The EU should swiftly implement the mechanisms for better monitoring and cooperation in standardisation bodies.

But as these initiatives and measures take root, the EU must expand their scope. The union needs to work more closely with vulnerable democracies and less developed countries that may not have the capacity or expertise to develop sound digital regulation to ensure data protection and fight disinformation, or to engage in standardisation negotiations.

The Global Gateway initiative addresses some of these 'soft' digital infrastructure issues, but currently these efforts lack coherence and are eclipsed by the initiative's overall focus on 'hard' infrastructure investment. Digital legislation should become a priority of EU engagement in less developed countries. Policy dialogues and regulatory capacity building measures must be at the heart of digital development engagements. The Declaration on the Future of the Internet, recently launched by the EU and the US and already endorsed by 60 countries, provides a valuable diplomatic tool that the EU should use to promote its democratic digital principles globally.

Moreover, the EU should increase cooperation with international companies and civil society around the world to jointly develop solutions where regulation falls short or has not yet emerged. The war in Ukraine has already shown that large digital companies and civil society are important actors in international policy. Much of the decision-making to combat Russian disinformation in the EU, Ukraine, and Russia was left to private companies and NGOs amidst a lack of content moderation regulation. In response to public pressure, often fostered by civil society actors, big Western technology companies have effectively deployed their own sanctions against Russia, halting services and sales in Russia even in areas intentionally exempted from governmental sanction regimes. To ensure Europe's foreign policy objectives are not undermined by private sector and civil society

action, it is essential for the EU to continuously engage with these actors on matters of digital diplomacy.

Lastly, Europe must better and more structurally incorporate foreign policy objectives into its own digital policies. The EU's DSA and the AI Act have great potential to positively impact digital governance in third countries, and these effects must be thoroughly considered during the legislative process. GDPR was a great success, but its global proliferation was not entirely expected and not all the consequences were fully thought through.

The union's foreign policy objectives, whether in its immediate neighbourhood or across the seas, cannot be achieved if the EU fails to address these global digital threats to fundamental rights, democracy, and the multilateral order. The promotion of a human rights and rules-based international technological order must therefore be at the heart of an EU external digital policy.

Delivering a human rights-focused, rules-based global technological order

- **Regulatory alignment**: Increased bilateral and multilateral engagement with like-minded and interested countries to share best practices, foster legislative alignment, and build regulatory capacities in less developed countries.
- **International technology principles and standards**: Improved European public and private participation, alignment, and alliance-building in international organisations to promote human-centric and democratic standards and principles for global technology development.
- **Critical dialogue and cooperation with the private sector**: Enhanced engagement and collaboration with the private sector and civil society to jointly develop solutions for tackling and responding to the issues and the misuse of technologies, especially in countries where diplomatic or political cooperation is restricted.
- **Incorporation of foreign policy objectives into EU digital policies**: Improved awareness of international digital policy developments and greater incorporation of foreign policy implications into European digital policy initiatives.

Securing the EU and its partners

- Leading up to Russia's invasion in February 2021, Ukraine suffered 288,000 cyber-attacks in the first ten months of 2021 and 397,000 in 2020. Shortly before the outbreak of the war, US cyber experts detected particularly pernicious malware in Ukrainian Railways' information systems, which – if it had not been detected and disabled – could have paralysed the countries' railway system used by a million civilians to escape the war.
- In 2020, cyberattacks cost the world economy more than $1 trillion, equivalent to more than 1 per cent of global GDP – an increase of 50 per cent compared to 2018.
- In 2013, the Snowden disclosures revealed that dominant market positions in critical digital technologies imply threats of foreign espionage. In 2018, American technology companies owned or leased more than 50 per cent of the global submarine bandwidth. In 2020, Chinese companies Huawei and ZTE held a combined market share of 40 per cent in telecoms network equipment.
- In 2018, various news outlets alleged that China had been transferring confidential data for five years from the Chinese-built information infrastructure in the African Union's headquarters in Addis Ababa.
- Misuse of surveillance and dual-use technologies undermines human rights and security globally. Pegasus spyware operations have been detected in at least 45 countries, of which at least six are linked to abusive use of spyware against political opponents and civil society. The sale of Pegasus software to other governments played a crucial role in advancing Israeli foreign policy objectives.

Today's societies and economies hinge on secure digital technologies and interconnections within and between countries. As a result, technological vulnerabilities have become some of the greatest security risks for states, companies, and citizens.

The threats of cyber-attacks, technical backdoors, and coercion or espionage resulting from one-sided dependencies in critical technologies and infrastructures are undermining political processes,

economic development, and digital trust. As the EU's Strategic Compass notes, "[Europe's] competitors are not shying away from using emerging and disruptive technologies to take strategic advantages." Increasingly, the lack of sovereign control over essential technological assets and infrastructures undermines autonomous national decision-making in security and foreign policy.

Beyond 'peacetime' geopolitics, digital technologies and cyberspace also play a central role in ongoing military conflicts. In the Strategic Compass, the EU stresses that "the armed aggression against Ukraine is showing the readiness to use the highest level of military force [...] combined with hybrid tactics, cyberattacks and foreign information manipulation and interference". Russia's military invasion was preceded and accompanied by massive cyberattacks and disinformation campaigns intended to undermine Ukrainian unity and morale.

Another issue connecting foreign and security policy to the digital realm are advanced military and dual-use technologies. New military technologies, such as unmanned drones and autonomous weapon systems, can swiftly change the course of war, as in the 2020 Nagorno-Karabakh conflict between Armenia and Azerbaijan. Export controls on these and other dual-use and advanced technologies play a central role in sanction regimes intended to deter or end military aggression. The West's vast technology sanctions against Russia are only the latest example of this practice.

In recent years, the EU has put great effort into securing its internal digital market and addressing technological vulnerabilities stemming from the proliferation of foreign technologies within the union. It has developed a foreign direct investment screening mechanism to prevent foreign take-over of critical technology assets and updated its export control regimes to combat the uncontrolled dissemination of dual-use technologies. The EU has developed a cybersecurity strategy, enforced the Cybersecurity Act, is finalising the second Network and Information Security Directive, and is currently developing the Cyber Resilience Act to bolster Europe's resilience against cyber-threats. It is developing mechanisms to detect and possibly deter hybrid threats, and to tackle foreign influence operations inside the union. The EU is establishing structures for greater cybersecurity cooperation and has built rapid response teams to collectively respond to cyber incidents within its borders. Lastly, the EU has come up with a Toolbox for 5G Security that aims to facilitate and streamline the deployment of secure 5G telecommunication networks within the digital single market through risk mitigating technical and strategic measures.

All these initiatives place the EU on a path to achieve a higher degree of cybersecurity and reduce its technological vulnerabilities. However, because the union is deeply embedded in an international trade and technology system, the EU has a strong interest in securing cyberspace and digital technologies beyond the continent. As Russia's NotPetya cyberattack against Ukraine in 2017

illustrated, cybersecurity is indivisible. As the NotPetya malware developed by Russian intelligence officers wreaked havoc on Ukrainian networks, it also spread across borders – with Danish global logistics giant Maersk becoming one of the attacks of most prominent victims.

Similarly, it is essential that the EU's democratic partners have the capacity to protect themselves against foreign influence campaigns, coercion, and cyber-attacks that attempt to undermine governmental authority and autonomy. The union thus has an interest in securing cyberspace and digital infrastructures beyond the continent.

The EU should structurally incorporate security standards and mechanisms, as will be proposed in the EU Cybersecurity Resilience Act and is being developed within the 5G Toolbox, into international partnerships and investment initiatives such as the TTCs, the digital partnerships, and the Global Gateway. The union should help its allies and strategically important countries to identify and reduce asymmetric dependencies in critical technologies that could undermine their sovereignty and EU foreign policy objectives.

The union should also improve bilateral cybersecurity cooperation with trusted third countries by sharing threat information, providing technical expertise and training, and coordinating diplomatic responses to cyber-attacks. The proposals for an EU Cyber Diplomacy Network and EU External Cyber Capacity Building Agenda, set out within the Cybersecurity Strategy, are a step in that direction. But they must be filled with life – that is, with funding and political backing. Most importantly, they should be embedded into an overarching geopolitical strategy. The EU's decision to deploy the Cyber Rapid Response Team for the first time in Ukraine to help fend off Russian cyberattacks was laudable, but it came late.

Similarly, the EU should help countries beyond the continent combat disinformation and election interference. The East Stratcom EUvsDisinfo initiative continues to play an important role in debunking Russian disinformation in the context of the war in Ukraine, but its efforts and scope must be greatly expanded to other particularly vulnerable countries and strategically important regions. Commentators have lavished praise on Ukraine for winning the information war against Russia. But in regions such as Latin America, India, Africa, and Southeast Asia that victory is far from clear. The EU should establish new partnerships and cooperation mechanisms with governments, the private sector, and civil society to counter Russian and Chinese disinformation in these regions.

As international negotiations on state behaviour in cyberspace continue at the UN, the EU should seek greater European engagement and alignment in these discussions and foster alliances in line with its foreign policy goals. Moreover, the EU should further the development of shared capabilities with its allies in emerging defence technologies. Deepening cooperation with NATO, which is

launching a civil-military Defence Innovation Accelerator for the North Atlantic and establishing a NATO Innovation Fund, is essential.

Lastly, Europe should continue to deepen cooperation with its allies to align and enforce its export controls for dual-use and advanced technologies. As noted, the joint EU-US technology sanctions against Russia are an early success story of TTC cooperation. But the EU and the US should further leverage their strategic positions in technology development, their regulatory expertise, and their diplomatic ties to strengthen the multi-lateral approach to export controls and jointly address the security concerns associated with emerging technologies. Together with the US and other allies, the EU should work to prevent the uncontrolled proliferation of dual-use technologies that undermine human rights, democracy, and global security. Digital technologies are often inherently dual-use, and their uncontrolled dissemination poses great threats.

As all these initiatives make clear, the union cannot achieve its policy objectives if it does not adequately address, together with its international partners, the global security issues related to digital technologies.

Securing the EU, its partners, and other like-minded countries

- **Dual-use and military technologies**: Raise awareness and develop capacities in emerging military and dual-usetechnologies among member states and together with like-minded countries.Prevent the uncontrolled dissemination of dual-use and security undermining technologies.
- **Securing digital infrastructure and critical assets**: Increased and structured provision of technical and political assistance as well as financial supportfor third countries to warrant secure digital infrastructure and critical assets.
- **International cyberspace standards**: Advance global norms for secure digital technologies and responsible state behaviour in cyberspace.
- **Cyberspace cooperation**: Improved information sharing on cyber threats and coordination of technical and diplomatic responses to cyber-attacks among member states with trusted third countries, and private capacity building in like-minded less developed countries.

Promoting open, competitive and inclusive digital markets

- Digital protectionism is on the rise. The number of data-localisation measures imposed by governments has doubled from 67 barriers in 35 countries in 2017 to 144 restrictions in 62 countries in 2021.
- The combination of US-China trade disputes, the covid-19 pandemic, and the lack of diversified supply chains and competition in cutting-edge semiconductor manufacturing led to large shortages of microchips in factories around the world. The war in Ukraine is causing additional shocks to already unstable semiconductor supply chains, in part because half the world's neon gas used in chip production comes from Ukraine.
- To date, China has exported surveillance technology to more than 60 countries, including Myanmar, Venezuela, and Zimbabwe. Thirty six of those states have signed on to China's Belt and Road Initiative, giving them access to attractive loans to purchase 'authoritarian technology' from Chinese companies.
- The information and communications technology (ICT) funding gap for Africa is estimated at $3 billion per year. Africa needs 250,000 new 4G base stations and 250,000 km of fibre. In 2015 and 2017, Chinese ICT infrastructure investment in Africa surpassed the combined funds from African governments, multilateral agencies, and G7 nations.

Since the beginning of the twenty-first century, digital technologies, trade, and connectivity have fostered rapid economic development within and beyond the EU. According to the World Bank, "the digital economy is equivalent to 15.5% of global GDP, growing two and a half times faster than global GDP over the past 15 years." Similarly, digital trade has grown rapidly in the last two decades with trade of ICT services between the US and the EU alone being worth more than $264 billion in 2020.

However, growing restrictions on digital trade and insufficient digital infrastructures, especially in the global south, are currently preventing greater digitally-spurred growth and inclusion. In Africa, for example, the ITU estimates that just a 10 per cent increase in mobile broadband penetration would

result in an increase of 2.5 per cent of GDP per capita. Similarly, the UN Conference on Trade and Development estimates that data flow restrictions reduce medium- to long-term real GDP by more than 0.5 per cent. Nevertheless, countries around the world – especially emerging economies such as China, India, and Indonesia – are increasingly closing their digital markets to shield them from foreign competition.

In recent years, China has sought to fill the digital investment gaps in less developed countries as part of the Belt and Road Initiative with its DSR component. China offers countries attractive loans for investments in digital infrastructures that rely on Chinese technologies. This is part of a dual economic and geopolitical agenda to increase Chinese technological and political influence, and to create one-sided dependencies. For the DSR 'partner' countries, however, these digital investments have a significant downside. Alongside the security risks linked to Chinese digital technologies, countries partnering with Beijing have often suffered both from Chinese economic coercion measures and intellectual property theft.

In general, abuses of one-sided trade dependencies in critical technologies and raw materials are becoming more common. Alleging espionage, security concerns, and likely diversion to the Chinese military, the US has successfully leveraged its technological power to deprive the Chinese technology company Huawei of high-end microchip supplies. Similarly, China in the past has stopped exports of critical minerals in the context of political disputes with countries in the region.

The growing 'geopoliticisation' of technology intensifies the risks arising from currently under-diversified supply chains in critical technologies, such as semiconductors. Furthermore, the monopolistic and oligopolistic market structures in the global digital economy are limiting consumer choice, increasing costs, hampering innovation, and undermining democratic processes around the world. Effective antitrust policy to foster more competition in digital technologies, however, requires international cooperation. Similarly, more international cooperation is required for effective taxation of multinational digital companies and to conclude important agreements on digital trade in multilateral trade forums such as the WTO.

The EU continues to be a great beneficiary of open global trade, not only in analogue but also in digital goods. The EU thus has an interest in investing more political ambition and strategic thinking into the promotion of open, competitive, and inclusive global digital markets. It remains an open question, however, whether such tough antitrust enforcement will strengthen or weaken Europe's capacity to promote digital champions that can effectively compete with US or Chinese giants.

The TTC and the digital partnerships with Asian partners address many of these trade and market issues, including supply chain security, global trade challenges, connectivity, and data flows. But the

EU cannot stop there: it needs to pay greater attention to the global south. The EU should offer less developed countries a real alternative to China's DSR for digital development. Building on the EU's economic power, its technological capabilities, and its political credibility and diplomatic ties, the union should seek to foster greater connectivity investments in the global south, especially in geostrategically important countries such as India, South Africa, and Brazil.

The Global Gateway initiative could represent such a triangular 'geo-tech development' tool that allows the EU to better leverage its political and economic position. The initiative could help the union become an attractive and trusted partner for third countries seeking an alternative path to digital development based on democratic values, open markets, and sustainable investments.

Digital issues should also play a role in any new or updated bilateral trade and partnership agreements. This includes, for example, the currently stalled negotiations with Chile and New Zealand – which will include provisions on data flows and localisation – as well as the free trade agreement negotiations with India. Agreements on digital trade not only provide opportunities for economic growth but also for the EU to promote its approach of values-based regulation and trusted connectivity. As the new Standardisation Strategy puts it: "There is scope for a more strategic approach in leveraging trade agreements and partnerships to support shared interests in international standards-setting with key partners."

Lastly, the EU should seek greater joint investments with like-minded countries in research and development in critical technologies. It is not realistic for the EU, or any country for that matter, to develop leading capabilities across all critical technologies. But cooperation with allies can enhance shared capacities and reduce common dependencies.

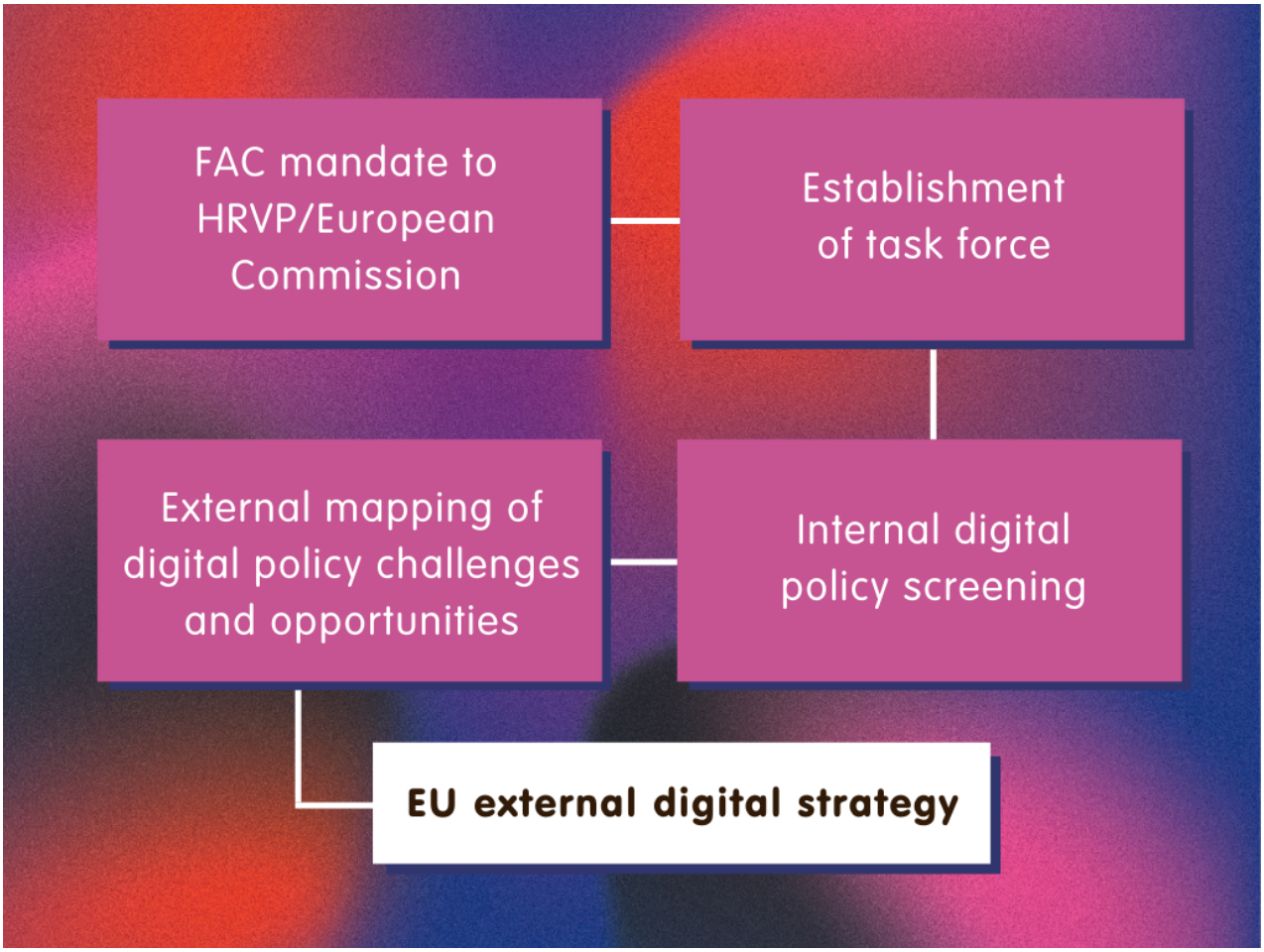
Inasmuch as the EU would greatly benefit from values-based technology regulation and a secure cyberspace in Europe and beyond, a well-functioning, well-integrated, and well-developed global digital economy would serve Europe's interest. The more connected, balanced, and inclusive global digital markets are, the less individual countries or companies will be able to abuse their power – and the more digital technology can contribute to economic growth and democratic development, especially in the global south.

Promoting fair, open, and inclusive digital markets

- **Connectivity partnerships and investments**: Increase public and private connectivity investments in less developed countries; offer technology development partnerships based on democratic values, thereby cooperating with like-minded countries; and develop initiatives to efficiently expand the volume and scope of investment.
- **Bilateral and multilateral trade agreements**: Explore additional and expand current trade, association, and regional agreements to foster digital trade, ensuring level market access and securing international supply chains.
- **International trade rules**: Better leverage the EU's economic strength and diplomatic ties to build strong alliances in international forums to promote a reliable rules-based order for international trade
- **Joint research and development**: Expand on international joint research and development opportunities in critical technologies with like-minded countries to strengthen technological competitiveness and build pooled capacities.

The path to an EU digital diplomacy strategy

Russia's war against Ukraine and the prospect of tighter Sino-Russian geopolitical and technological cooperation are giving new urgency to the EU's quest to become a geopolitical technology actor.



The following sections set out a path towards an EU external digital policy, lay out substantive policy proposals to be contained in the strategy, and propose structures and processes for its effective implementation.

Step 1: The mandate

On 12 July 2021, the FAC unanimously called for the HRVP and the European Commission to jointly draft an initial policy paper for an EU external digital policy. Building on this preliminary mandate, and given the new urgency for EU geopolitical thinking, several member states – including, most prominently, Denmark – are seeking to provide the HRVP and the commission with a strong dual

mandate to lead the development of an ambitious EU digital diplomacy strategy.

Shared leadership in Brussels can run afoul of interinstitutional issues. But this model of a dual commission/HRVP mandate to address complex strategic foreign policy issues has worked in the past. EU parliamentarians have hailed the EU's 2019 Communication on China, which emerged from such a dual mandate, as a successful effort at European External Action Service (EEAS)/commission cooperation.[2]

Step 2: The task force

The HRVP and the European Commission should set up a task force responsible for developing a digital diplomacy strategy.

Importantly, this task force should comprise representatives from the EEAS and digital policy experts from the Directorate-General for Communications Networks, Content and Technology (DG CONNECT), the part of the commission responsible for most digital policy. Additionally, experts from other relevant commission directorates working on digital issues, including the Directorate-General for International Partnerships (which is leading the work on the Global Gateway), the Directorate-General for Trade (which is strongly involved in the TTCs), and the Directorate-General for Competition (which is currently engaged in antitrust policy dialogues with the US), should be included in this working group.

Moreover, it will be essential to incorporate the knowledge of the EEAS and member states' international delegations into this strategy group. It is often these delegations that engage in dialogues on digital issues in their countries or international organisations of deployment. Their experience of how the EU can more effectively externalise and promote its digital policy is essential.

Lastly, the task force should be in regular exchange with the FAC, which should provide strategic guidance and political impetus. The FAC is the arena in which member states need to find alignment on the central themes, priorities, and funding of EU foreign policy. The intricacies of these complex digital issues, however, means that the FAC will need to delegate continuous oversight of the task force. Members of the EU technology ambassador grouping can continuously represent the FAC within the working group.

Step 3: Internal digital policy screening

The new digital diplomacy task force needs to develop a comprehensive overview and analysis of the

EU's and member states' ongoing digital policy initiatives.

As described, the EU has passed a lot of legislation on digital issues and has developed a wide variety of new instruments, initiatives, units, and cooperation mechanisms. Many of these efforts are of great relevance to EU foreign policy, and an external digital strategy should logically build upon them.

Importantly, this digital diplomacy mapping must include all EU legal initiatives that are likely to yield an impact beyond the union – as well as current digital policy dialogues with third countries, existing or ongoing EU trade agreements, and negotiations within which digital aspects are incorporated. It should also include EU connectivity and cybersecurity partnerships.

Such mapping is essential for the identification of gaps between and within current initiatives, and to determine priorities for new or increased engagements. Furthermore, it can identify potential synergies between distinct ongoing activities. For example, the Policy and Regulation Initiative for Digital Africa set up in 2018 and the EU-AU Data Flagship set up in 2021 overlap considerably with the new Global Gateway programme. Similarly, the EU-US TTC and the EU-India TTC negotiations should be well integrated and coordinated with one another.

Beyond the many initiatives stemming from Brussels, member states have launched various digital diplomacy projects. This includes the Estonian Trusted Connectivity proposal and the Paris Call for Trust and Security in Cyberspace. It is crucial to assess the contribution of member states' initiatives to a broader EU strategy and to direct greater overall EU attention towards the most relevant efforts.

Step 4: External mapping of digital policy challenges and opportunities

The internal digital policy screening should be complemented by a comprehensive mapping of external policy challenges and opportunities. In that effort, the European Commission, with support from the EEAS and member state delegations, should conduct a review of recent international developments in digital policy that might negatively affect EU foreign policy, or provide strategically important opportunities for EU engagement.

Digital regulation in other major economies is now of great relevance to EU foreign policy. For example, Chinese data privacy or antitrust regulation directly affects international data flows and international market competition. Similarly, digital partnerships between third countries, such as the Sino-Russian 'no-limits' agreement from February 2022 or the Digital Economy Partnership between Singapore, Chile, and New Zealand – which is open to other WTO members to join – are of relevance to EU digital diplomacy thinking.

The EU Excellence Hub on Standards, set forth in the EU's Standardisation Strategy, and the Strategic Standardisation Information mechanism, launched at the recent EU-US TTC Summit – both tasked with monitoring international standardisation activities – are important steps. But beyond international norms and standard negotiations, the EU should seek a better overall understanding of important international digital policy developments. This includes improved awareness of digital legislation in major economies, patterns of digital trade, and partnership negotiations between third countries – as well as the connectivity initiatives of EU partners and competitors.

Beyond international digital policy developments, the EU should gain a better understanding of third countries' technological development needs and vulnerabilities. For instance, for the EU's Global Gateway to become a success, the EU will have to quickly identify strategic opportunities and make third countries convincing digital development offers before they get lured into greater dependence on China.

The toolbox for EU digital diplomacy

The previous sections established why the EU needs an external digital strategy and discussed the institutional steps necessary to bring it about. But the mandate, the taskforce, and the screening exercises are all means to an end. The goal is for the EU to develop a policy toolbox that will allow it to become a geopolitical actor. Accordingly, this section makes some concrete proposals for policy tools the EU could design and deploy to achieve its policy goals.

Policy Recommendation 1: a worldwide democracy protection fund

The EU should set up an initiative and a financial fund to protect democratic elections worldwide from foreign influence operations and cyber-attacks. This initiative should be aligned with the proposals in the Strategic Compass which would, for instance, expand the foresight activities of the Hybrid Fusion Cell and allow for the potential deployment of Hybrid Rapid Response Teams to third

countries. Moreover, this fund will aim to:

- Facilitate partner countries in **designating political and democratic institutions such as parliaments, political parties, and elections as critical infrastructures.**
- Fund the necessary measures to **protect such critical infrastructure from external interference,** including providing the EEAS with a budget for **external online election assistance and for the deployment of rapid response teams** to help counter election interference.
- Bring national parliaments and regulatory authorities in partner countries together with technology companies and civil society organisations to **supervise the fair and free online dimension of electoral campaigns.**
- Help countries fight foreign influence operations by setting up a **Global Disinformation Observatory** or equivalent regional disinformation observatories.
- Include **online election monitoring** in EU electoral observation missions intended to measure and counter polarisation, disinformation, and foreign influence operations – and promote transparency in political advertising and campaigning.
- Help countries develop **regulations to hold foreign and state-owned disinformation outlets**, such as Russia Today and Sputnik, accountable for spreading disinformation.
- Help allies and partners achieve regulatory alignment on measures to preserve traditional **media independence** and viability, such as those included in the European Democracy Action Plan. And give that plan a foreign technical assistance dimension and a budget to act outside Europe.
- Support members of the **European Parliament** to engage with third countries to help EU partners and allies align their regulations on illegal content, transparent advertising, and disinformation with the EU DSA.
- Promote the inclusion in EU Association Agreements of legislation ensuring that **internet shutdowns** are limited and controlled by parliaments and courts, and that norms protecting online free speech are enforced both by governments and by platforms.

Policy Recommendation 2: a worldwide digital rights initiative

The EU should set up a fund facilitating global regulatory convergence on digital rights. This should provide funding to:

- Support governments of partner countries to implement better **standards for data privacy protection, secure e-communications, and ethical AI.** This support would involve funding partner countries' parliamentary committees that work with the European Parliament and the European Commission, and establishing **twinning programmes** to strengthen capacity in partner countries.
- Make additional funds available to **civil society organisations** promoting digital rights and help set up **independent agencies** to monitor digital rights and train members of parliament in basic digital skills. The aim is to facilitate the creation of **Digital Rights Committees** in national parliaments.
- Fund **assistance and research missions** from the EU to other countries and vice-versa.
- Help partner countries obtain **adequacy decisions** on data privacy from the European Commission to foster foreign investment and an increase in digital goods trade.
- Work with partners on **a global ban on social scoring and predictive policing** and on limiting biometric surveillance and prohibiting algorithmic discrimination.

Policy Recommendation 3: a democratic technology standards initiative

The EU should lead in the establishment of a **global alliance on democratic and ethical tech governance.** For this purpose, the EU should:

- Convene a **Global Summit for the Democratic Governance of Technology** and invite countries to join and to push for the adoption of **ethical, safe, and inclusive technology standards**. The summit will eventually produce a **'Brussels declaration'**, stating EU support for countries adopting these kinds of commitments. The commission should invite the private sector and civil society to join.

- Seek a series of **structured cooperation and policy dialogues** with partners and private stakeholders on multilateral norms and the governance of standards organisations. Expanding on the proposals in the Standardisation Strategy, the EU should **empower EEAS delegations** in these organisations with the resources to understand the organisations, as well as coordinate EU and allied action and support for the private sector within them. The aim would be to create a **democratic technology caucus at multilateral organisations**, including the UN.

- Make the **Global Gateway** a central part of this strategy, which means in part making **regulatory and standards convergence** along ethical and democratic lines a key element of the Global Gateway packages offered to third countries.

Policy Recommendation 4: a global cybersecurity fund

The EU should set up a cybersecurity fund within the EU Cyber Diplomacy Network envisioned in the Cybersecurity Strategy, and enhance the external role of its cybersecurity agency. Its aims should be to:

- Help partner countries develop cybersecurity strategies to **protect their critical infrastructures, firms, and public administration** from cyber-attacks. This would also include the protection of the financial sector, secure mobile payments, and the establishment of secure digital IDs and certificates, among other efforts.

- Create within the EU Intelligence and Situation Centre **a 24/7/365 capacity to monitor** global cybersecurity risks in real time. It should develop **early-warning mechanisms** and set up additional **rapid-reaction** teams or expand the scope of the Permanent Structured Cooperation cyber rapid response team to assist third countries facing sustained cyber-attacks

- Assist partner countries in passing legislation and setting up institutions to **identify and sanction perpetrators**, whether individuals or entities, responsible for cyber-attacks. Establishing mechanisms and bodies to cooperate with partners to quickly attribute cyber-attacks, as a precondition for an appropriate response, is essential to this effort.

- **Train police, judges, and prosecutors** in third countries to handle cyber-attacks.

Policy Recommendation 5: A secure technology initiative

Monitoring foreign investments in critical digital infrastructures and technologies, and better

evaluating risks associated with new technologies, is now a critical state function. The goal of a secure technology initiative would be to:

- Help partner countries set up **investment screening mechanisms** to address risks and vulnerabilities in critical technologies, including 5G telecommunications, semiconductors, and AI.
- Help partner governments to **regulate risks** from foreign investments, and include security and geopolitical criteria in public tenders for digital infrastructures.
- Cooperate with partner countries to identify **asymmetric technological dependencies** and to develop common strategies to mitigate them.
- Help partner countries to develop or update **export control regulations for dual-use technologies**.
- Foster the development of new or updated **multilateral agreements on dual-use trade controls**.

Policy Recommendation 6: a sanctions' monitoring and implementation initiative

The EU has begun to leverage technology sanctions as a foreign policy tool. It now needs to ensure effective implementation as well as coherence with its allies. Effective technology export controls will require more international cooperation with partners. This initiative thus seeks to:

- Develop mechanisms for **structured cooperation in sanctions deployment**, monitoring, and enforcement, and – where possible – set up common compensation mechanisms. At present, sanctions are approved by the European Council but enforced by member states. The EU lacks a centralised institution to monitor their enforcement. More cooperation, including setting up ad hoc mechanisms, could help these sanctions become more efficient. Moreover, since the impact of sanctions is asymmetric for member states, compensation mechanisms ensuring a fair distribution of costs may help get reluctant member states on board.
- Provide EU assistance to countries threatened by **extra-territorial or secondary sanctions** by opening policy dialogues on anti-coercion instruments.

Policy Recommendation 7: enhancement of the Global Gateway initiative

The Global Gateway initiative is the right answer to today's dynamics of spheres of influence in the technology domain. It is a much-needed tool to keep global digital markets open, safe, and inclusive. It is also a key instrument for closing connectivity gaps between and within countries, bringing swing and vulnerable countries closer to the EU, and countering Chinese and Russian influence. To ensure its success, the Global Gateway features should:

- Contain a strong **conditional regulatory and standards convergence** component to facilitate partner country support for rules-based institutions and ethical alignment with the EU.
- Promote **regulatory convergence**, through the Global Gateway programme on standards for secure, safe, and ethical international data flows.
- Include funds to foster cooperation in **scientific research** and technology development in critical technologies.
- Strengthen European **links to civil society** in third countries.

Policy Recommendation 8: establishment of the EU-US TTC as a geopolitical vehicle for transatlantic technology cooperation

The Ukraine war and the strengthening of the Sino-Russian alliance make it imperative to bring the EU and the US closer together. The US and the EU have different approaches to technology regulations, but the two models are not antagonistic. The TTC is a potential vehicle to improve relations, to make these models more compatible, and to advance shared foreign policy interests. Therefore, the EU and the US should:

- Strengthen their cooperation **on export controls, technology platform regulation, standards development, and telecoms security and connectivity investments in third countries** – within the agenda of the TTC's ten working groups.
- Consider **expanding the TTC** to other democratic technology powers such as Japan or South Korea so that it can become an embryo for a global democratic deal on digital technologies. The

recent announcement of an EU-India TTC points in that direction and is crucial for the EU to integrate both initiatives into a coherent strategy. Hence TTC work must focus on concrete deliverables in the near-term, while simultaneously not losing sight of an ambitious overall strategy.

Deploying the strategy

The Russian invasion of Ukraine offers some important lessons for EU digital diplomacy. Before the the war, the union was already supporting Ukraine in digital regulatory alignment as part of the EU-Ukraine Association Agreement. However, the EU had not engaged in a sufficiently long-term and deep effort to restructure and align Ukraine's digital environment. Supporting third countries, especially those in the EU's immediate neighbourhood, in sound digital regulation is crucial not only for the economic development of those countries but also for their political stability and security. Stronger regulatory alignment, as Ukraine shows, can already substantially pull countries towards the EU economically and politically – and contribute to EU foreign policy objectives. In strategically important countries, the EU should double-down on efforts to foster such processes.

Similarly, as set out in the Strategic Compass, the EU should now increase its efforts to fight disinformation and expand them to other regions where Russian and Chinese disinformation is spreading rapidly. The EU will not be able to fend off disinformation everywhere, but by devising a comprehensive strategy and setting priorities the EU can move from a reactive to a pro-active stance and create a structured approach to fighting disinformation globally.

Lastly, the EU's decision to deploy its cyber rapid response team in Ukraine certainly came too late and was outperformed by that of the US. If the EU wants to be a geopolitical actor, it must increase its capacity to swiftly assist third countries in cyber-defence and have a greater awareness of when and where to deploy that capacity.

Ukraine shows that not only does the EU need to have the right instruments for digital diplomacy, but it must also have the awareness, strategy, resources, and structures to deploy them. The previous section laid out a large toolbox of potential digital diplomacy instruments. To effectively use these tools, the EU must establish new structures and devote more resources to enabling EU delegations to inform Brussels, engaging in cooperation with third countries, and deploying support systems in third countries.

Therefore, a comprehensive mapping of both EU internal digital policy as well global developments at the intersection of technology and geopolitics is needed, not only for the strategy's development but

also to inform the deployment of many of the proposed instruments. The EU needs to gain a better understanding of when to best initiate policy dialogues, and with which third countries to do so. The union needs to better understand where and how to strategically invest in digital development in other regions. The EU also needs greater awareness of when swift action and cooperation with allies is necessary in international standards forums. And it should know when and where to deploy countering disinformation efforts, election interference, and cyber rapid response teams.

Our interviews with the heads of EEAS delegations show that the global network of EEAS and member states' delegations should be better leveraged. These delegations already engage in digital diplomacy, but they often do so reactively and inadequately because of a lack of expertise, insufficient resources, and too little support and information from Brussels and other capitals.

As a first step, the EEAS and member states' delegations should receive digital diplomacy training. The EU and the member states should educate their diplomats in the geopolitical importance of digital technologies and provide them with a comprehensive overview and analysis of the tools at their disposal for EU digital diplomacy. They should have the ability to screen important digital policy developments in their countries or international organisations – and, importantly, they should have reporting structures to engage with Brussels and member state capitals on important digital policy developments.

However, training delegations will not be enough to meet EU digital diplomacy objectives around the world. Even when trained on digital policy, delegations will not be capable of fully engaging in the often highly technical discussions of digital technologies. Rather, delegations should serve as the union's eyes, ears, and initiators for further EU digital policy engagement.

Support structures should thus be created through which delegations can request additional digital policy expertise. The EU can establish this additional digital diplomacy expertise both on the regional level as well as in Brussels. The EEAS already has a system in some larger countries or in regional hubs in which delegation teams have additional policy experts dedicated to specific policy fields – including trade, health, and environment – at their disposal. However, only in very few countries is such expertise on digital policy available. The union should therefore assign additional digital policy experts to regional hubs to support country delegations in the more in-depth aspects of digital diplomacy.

Similarly, the EU already has a unit at DG CONNECT dedicated to policy outreach and international affairs. But this unit's work is currently mostly limited to the EU's large technology diplomacy initiatives, including the TTCs, the Global Gateway, and the digital partnerships. This unit should be provided with significant additional resources to expand its work. Furthermore, it should provide on-

demand support to European delegations around the world seeking to move ahead with, for example, digital policy dialogues, standardisation cooperation, or connectivity investments.

Moreover, the EU should establish cooperation structures between the EEAS and member states' delegations in third countries and, most importantly, in international organisations. It is crucial that the EU acts decisively and with one voice in international negotiations on digital technologies. The EEAS and the member states should ensure continuous information sharing to, for example, coordinate their negotiating strategies in multilateral technology forums. Such cooperation can of course be expanded to the EU's international allies and should often incorporate private sector actors.

To effectively deploy all the instruments proposed in the previous section, more structural changes and additional units and resources are needed across various EU bodies. This includes lines of communication between delegations and the EU's cybersecurity bodies and more coordination between the union's international affairs, trade, and development units. It should be within the responsibility of the task force established for the development of the strategy, and led by the HRVP and the European Commission, to expand on these proposals and oversee the realisation of the strategy and the deployment of its tools.

With a hybrid war raging in Europe and in cyberspace, geo-technology battles between the great powers are intensifying. And with new technologies on the rise, the EU must seize this moment of increased political alignment with the US and other countries to set forth an ambitious agenda for digital diplomacy. With this digital diplomacy effort, the EU should promote a democratic, human rights-focused, and rules-based global technological order. It should work more closely with its partners to improve global security in the physical and digital spheres. And it should promote open, balanced, and inclusive digital markets and facilitate secure connectivity – especially in the global south. To reach these goals, it is essential for the commission and the EEAS to work together, and for EU member states to align their external and digital policies more closely to enhance the efficacy of this policy.

The authors of this policy brief believe that the vision, strategy, and tools laid out in this paper can give direction and contribute to this process. They can also lay the foundations for the EU to become a global player in the geopolitics of technology.

About the authors

Julian Ringhof is a visiting fellow at the European Council on Foreign Relations through Mercator Stiftung's *Mercator Fellowship on International Affairs* programme.

José Ignacio Torreblanca is a senior policy fellow at ECFR and head of ECFR's Madrid office.

Acknowledgements

We want to thank the Danish Ministry of Foreign Affairs and the Spanish Ministry of Foreign Affairs, European Union, and Cooperation for supporting this project. The Office of the Tech Ambassador at the Danish Ministry of Foreign Affairs, the Directorate for the Global Agenda and Multilateral Relations at the European External Action Service, and the Directorate for Policy Strategy and Outreach at DG CONNECT in the European Commission, have been invaluable partners in this project. We thank them for the time they dedicated to us and for their readiness to exchange ideas and read and comment earlier drafts of this policy brief. Of course, the final responsibility for the text rests solely with the authors. We also want to thank all the participants from the European Commission and the Political and Security Committee for the insights they shared with us in the closed-door workshop we held in Brussels in October 2021. To complete this project, we held numerous interviews with heads of EU delegations around the world, officials at DG INTPA, and the European Council Secretariat, as well as with several MEPs. We are most grateful for their help.

At ECFR, we want to thank our colleagues in the European Power Programme for their support throughout the process. Programme director, Susi Dennison; Carla Hobbs, the manager of the Technology Initiative; and Jenny Söderström, the programme coordinator, were essential for the completion of this project. Jeremy Shapiro, our research director, did an incredible job in editing this paper and making valuable suggestions to improve it. Finally, we want to give a special thanks to Astrid Portero, our research assistant, for her help throughout this project. We would not have been able to complete it without her dedication and eye for detail.

---

[1] "Strengthening the European External Digital Policy", Non-paper presented to the EU Foreign Affairs Council, July 2021, mimeo.

[2] Authors' interview with a senior member of the European Parliament's Foreign Affairs Committee, Brussels, 22 March, 2022.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.

- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. ecfr.eu

 ISBN: 978-1-914572-50-0. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.