EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY BRIEF

GEO-TECH POLITICS: WHY TECHNOLOGY SHAPES EUROPEAN POWER

Ulrike Franke, José Ignacio Torreblanca

July 2021

SUMMARY

- New technologies are a major redistributor of power among states and a significant force shaping international relations.
- The European Union has for too long seen technology primarily through an economic lens, disregarding its implications for its partnerships and for its own geopolitical influence.
- If the EU wants to be more than a mediator between the two real technological powers, the United States and China, it will need to change its mindset.
- For the EU and its partners, the vulnerabilities created by battles over technology divide into two types: new dependencies and openness to foreign interference.
- The EU and its member states need deeper engagement with the geopolitical implications and geopolitical power elements of technology.
- This engagement has an external element of reaching out to partners and an internal element of ensuring close cooperation between the EU and its member states.

Introduction

The European Union has unveiled the world's first plans to regulate artificial intelligence (AI). The publication of the rules is part of a frenzy of EU tech regulation and strategies: there is also the Digital Services Act, the Digital Markets Act, the Digital Decade, the Cybersecurity Strategy, the Data Strategy, and more. Most importantly, the AI regulation follows the implementation of another major EU technology regulation that anyone who accesses the internet has encountered many times: the 2018 General Data Protection Regulation (GDPR). The EU is doubling down on its role as a regulatory superpower.

Technology regulation may sound like (and, to some extent, is) a boring topic that should chiefly concern legal experts. But technology has found its way onto geopolitical battlegrounds. Throughout history, technology has not only transformed economies and societies but also been a major redistributor of power among states and a significant force shaping and reshaping international relations. New technologies can massively boost a country's economy and, therefore, global influence. They can enable capabilities that provide a country with military advantages or even dominance. And the values and standards that tech products embody are determined by whoever manufactures them.

But the EU, for all its pathbreaking work on regulation, does not appear to have fully recognised just how geopolitical technology can be – or how geopolitical the current generation of emerging, primarily digital, technologies has become. At the 2020 Munich Security Conference (the last one before the pandemic), it was painfully obvious that the EU was widely considered to be – at best – a mediator between the two real technological powers, the United States and China.

Since then, some things have changed. For one, technological competition between the US and China is increasingly fierce. The US has imposed export controls on semiconductors, aiming to cut off China's supply lines, and has pressed its allies worldwide to kick Chinese companies out of strategic markets, such as 5G. A recent report by the US National Security Commission on Artificial Intelligence mentions China a whopping 699 times (Europe appears 93 times; Russia 64). Meanwhile, China's central government wants Chinese AI to be the world's undisputed leader by 2030. And Chinese President Xi Jinping is pressing for greater independence from global supply chains. A fight for technological spheres of influence is playing out before our eyes, and the rhetoric around it is getting more heated.

In Europe, there has been some encouraging movement. The EU has begun to speak more forcefully about "digital and technological sovereignty"; the European Commission has laid out a strategic vision or "digital compass"; the European External Action Service has started regarding technology,

connectivity, and data flows as a key dimension of the EU's external relations and partnership agreements; and a few member states' foreign ministries have begun producing strategies on the geopolitical dimension of technology. More recently, the European Council has called for a "geostrategic and global approach to connectivity". And the US and the EU are looking into increased tech cooperation – most notably in the form of the Technology and Trade Council, which they announced at their June 2021 summit.

Nonetheless, Brussels and most member state capitals remain primarily focused on the economic, social, and labour implications of technology – almost as if they believe that, by ignoring tech geopolitics, they can escape it altogether. But the technological is geopolitical. States might not need to care about who owns the technology in a market-orientated, rules-based world order governed by solid multilateral institutions that enforced international norms. They could expect market forces and open and accessible global supply chains to take care of their technological needs, be it in the production of semiconductors or the construction of global networks to connect users to the internet.

Technological sovereignty becomes an existential question when the global market is hijacked by state actors, multipolarity and unilateralism replace multilateralism, and great powers turn interdependencies into vulnerabilities as they seek to set up spheres of influence. European countries and their partners risk becoming playgrounds of technological competition between great powers, which attempt to coerce them into joining a bloc. Countries could become economically dependent on others for key technologies, leaving them unable to influence standards in a way that corresponds with their values and even subject to direct foreign interference. Geopolitically speaking, technology is not neutral.

This is not just about Europe standing its ground – or choosing sides – in the Sino-American competition, which is what most European analyses now focus on. It goes beyond that. In fact, Europeans largely overlook two issues.

Firstly, all EU action – and inaction – on tech has consequences that reach beyond the union. The EU has a long history of ignoring, and being surprised by, the external implications of its actions. For instance, this was the case with the Common Agricultural Policy, which – despite being devised as a way to balance the Franco-German relationship – had huge global implications; the Ukraine Association Agreement, whose dramatic geopolitical consequences were not fully anticipated by EU policymakers; and, more recently, the GDPR, whose global impact was not foreseen by EU regulators.

Policymaking within the EU is so complicated and inward-looking that little time and space is left for anticipating the impact of EU regulations on external actors or, even more ambitiously, thinking strategically about which countries or regions may want to partner with the EU to pursue similar

goals. However, the sheer size of the EU's internal market means that external actors often have no option but to comply with EU rules even if they dislike them, see them as problematic and costly to implement, or had no role in their creation. The EU rarely acknowledges ahead of time how its actions will affect non-EU states. When it does, this usually involves a positive reading of the "Brussels effect" – the idea that EU regulation, through the weight of the bloc's market, will automatically become a model for other powers. European leaders often portray the Brussels effect as automatic, an almost magical occurrence rather than something that requires further thought. Generally, they pay little to no attention to second- and third-order effects on other players.

Secondly, the EU puts too little thought into the way in which its internal actions – or lack thereof – influence its geopolitical power, since this is a metric that rarely comes up in any European discussions. For others, AI means power: the US National Security Commission on Artificial Intelligence defines its own role as being to "prescribe actions to ensure the United States wins the AI competition and sets the foundation to win the broader technology competition". Russian President Vladimir Putin famously declared that whoever becomes the leader in AI "will become the ruler of the world".

But the EU, and most Europeans, do not think in these terms. This is partly due to issues of competency, but even more to the way the EU sees itself: despite much rhetoric on a "geopolitical union" – and the high representative for foreign affairs and security policy's insistence that the EU has to "learn to use the language of power" – Brussels remains largely uncomfortable with power politics. The EU's ethos is that of a market-driven, technocratically led entity that, from the start, has left 'high politics' (security and defence) in the hands of member states. This means that the European Commission sees the world in terms not of power, coercion, or relative gain but as a game of market regulation. Most member states are no different: on technology, few of them have picked up the geopolitical baton. It is possible to see this as one of the many civilisational advances of the EU – and these authors are not advocating that the EU take an adversarial, competitive stance – but the fact remains that, if Europe is not interested in geopolitics, geopolitics is interested in Europe.

The European Council on Foreign Relations is focusing on this external and geopolitical dimension of the development, adoption, and regulation of technology in Europe. In this dimension, it is important – and often necessary – for things to work at home: Europe needs to improve its connectivity; support its start-ups and established firms; invest in research, talent, and digital skills; strengthen its digital infrastructure; and more. But, broadly speaking, the EU and European experts are paying enough attention to these issues. What they overlook are the geopolitical implications of technology, which are playing out on many battlegrounds and creating two main types of vulnerability.

Battlegrounds of vulnerability

Battles over technology are being fought in a growing number of arenas, and are creating ever more vulnerabilities third countries can weaponise. The following assessment, therefore, only provides a snapshot of some of these battlefields, but it explains the origins of these vulnerabilities – which, generally, divide into two types: new dependencies and openness to foreign interference.

New dependencies

Countries around the world are pursuing AI, 5G, additive manufacturing, and other new technologies primarily because they promise to yield significant economic gains. Some of the ways in which governments try to support their domestic industries are already leading to concerns over protectionism and even techno-nationalism. For example, on 5G, the effect of China's protected home market advantage is making Chinese telecoms giants almost unbeatable in third-country markets, creating an uneven playing field.

Geopolitically, these economic divergences are less important than the dependencies that result from particular states leading – or having monopolies – on some technologies. Such dominance can empower a state to give or withhold technologies from others, to pressure them to do its bidding, or to use these dependencies to force others to align or otherwise change its foreign policy. Members of the EU need to be wary of technological dependence on non-EU providers, particularly non-democratic states – or else they will become digital colonies of others. If Europe loses ground on technologies, it could also lead to European partners finding themselves dependent on other actors, as others fill the gap left by Europeans. Achieving technological sovereignty is, therefore, crucial for states that want to enjoy foreign policy autonomy. Two forms of critical infrastructure are of particular interest to the EU in this context: 5G and submarine cables.

5G independence

Europe's choice of vendors for the roll-out of 5G was at the centre of the first heavily and openly contested geopolitical struggle over a technological development since the end of the cold war. The US, under President Donald Trump, made the exclusion of Chinese suppliers from future European network infrastructure a test case for the transatlantic alliance. In many European capitals, Washington employed a 'with us or against us' logic that had a huge impact on an area previously deemed to be merely a commercial decision for European telecoms operators. The 5G debate thereby served as a geopolitical wake-up call for many EU member states in their thinking about technology.

Some, however, are still refusing to make hard choices on 5G, or are even continuing to play along with Chinese connectivity strategies and initiatives.

One odd feature of the debate is that, in fact, Europe is well placed on 5G – it has two companies that are global leaders in the area (to the extent that they are unrivalled even by US suppliers) and it could move to secure its 5G independence at a relatively low cost if it allocated additional resources to the task. But, for Europeans, the debate demonstrated for the first time the importance of access to competitive tech players. And this remains an important topic for Europe, since the development of the telecoms industry is continuing with 6G.

Undersea cables

Submarine cables are essential to the functioning of all digital sectors. Ninety-seven per cent of internet traffic and $10 trillion in daily financial transactions pass through these cables. Broadly speaking, the greater the number of undersea cables and the routes they provide, the swifter and stabler the internet access for the countries they connect – and, therefore, the lower the risk of interruptions that could lead to a digital network collapse.

In the last few years, Chinese and American companies such as Huawei, Amazon, Microsoft, Google, and Facebook have increased their presence in the market for undersea cables linking both European and non-European Mediterranean states to parts of the world such as Asia and Africa. European companies have adapted to this situation by forming consortia to compete with American or Chinese international groups. The EU lacks an all-encompassing strategy for a sector in which individual governments are still the key players. However, an initiative such as the BELLA submarine cable – which links Europe and Latin America, and will boost data-driven business, trade, education, and scientific research between the two regions – is a good example of how the EU can get it right by using its budget to support private-public cooperation in this key area.

If the EU fails to project its power in the Mediterranean, other global players will fill this space and create dependencies for Europe and its partners. These players will be able to penetrate the digital economy of Middle Eastern and African countries, to the detriment of European economic interests. Furthermore, there are also security risks associated with undersea cables. Companies often potentially have access to the data transmitted by the cables they manage. In this scenario, the physical protection of this type of infrastructure is likely to become increasingly difficult for the EU and for all organisations involved in the sector. Physical damage to this infrastructure could be catastrophic.

Setting standards

The process of setting technology standards is a subtle way to create dependencies. These standards, once set, can be difficult or costly to change. Unbeknown to most members of the public, there is a race on to set the standards on which digital infrastructure will run. Initially, the US mostly set up and administered digital standards, either publicly or via private firms. After a while, and with the support of the EU, countries 'multilateralised' technical standards to include stakeholders and government actors from third countries. This has largely served European interests well. Now, as globalisation fragments and China and the US decouple, the battle over technical standards has become critical.

If the EU does not set its own standards, it will be forced to adopt standards made by others – who may not share its values. Governance of the internet, including technical governance, is becoming increasingly bifurcated; the danger is that countries will be forced to choose between adopting the standards of a US internet or a Chinese internet, and to thereby give up access to the other market.

Artificial intelligence is one area in which an important standard-setting process is currently taking place. The EU chose early on to prioritise trustworthy or ethical AI. An EU high-level expert group developed ethics guidelines for trustworthy AI in 2018, and has since made policy and investment recommendations for trustworthy AI. The bloc's new AI regulation emphasises that it aims to become "a global leader" in the development of trustworthy and ethical AI, and concern about unethical AI is shared throughout the union.

If no ethical standards are established, AI-enabled systems could create or reinforce biases without allowing for any appeal or rectification. There might be no limitations on states' misuse of AI to, for example, control populations. Individuals' lives could be destroyed or severely curtailed by opaque AI-enabled systems in areas such as the judicial system, law enforcement, or credit ratings. People would be unprotected from manipulation through AI-enabled disinformation. While such developments might slightly hamper the adoption of AI, states would still likely use these systems extensively, creating an AI-enabled dystopia.

Alternatively, if the EU does not act, others will impose their AI standards. Many actors, including private firms, are already working on rules for ethical AI. Should they develop and promote these rules sufficiently, the EU would be reduced to following standards that it could not influence.

As such, there is a substantial upside for the EU if it gets trustworthy AI right. By ensuring that AI developed in the union is trustworthy, Europe can provide benefits to all users of AI-enabled systems. Ensuring that all AI-enabled systems used in the EU are ethical is directly beneficial for Europeans,

who can trust that their technologies will not be biased, illegal, or otherwise harmful. This is likely to encourage and, therefore, increase AI adoption rates, which one can expect to have a positive economic impact. If the EU succeeds in encouraging others to adopt trustworthy AI standards, this would further widen the circle of beneficiaries. Even better would be if the EU established itself as a leader in ethical AI, prompting others to follow its regulations. This would ensure that the ideals that Europeans value would be adequately reflected in AI systems. Furthermore, the EU could gain a location advantage – meaning that, because of its leadership on ethical AI, "AI made in Europe" would be widely seen as following the highest standards, thereby becoming a sought-after commodity.

Another area of standard-setting is data privacy. Few topics are as important to the EU's self-image as the protection of individual privacy. The EU made history with its GDPR regulation – which has changed the way that millions, if not billions, of people engage with the internet. But guaranteeing that everybody can be free in the digital realm is an ongoing effort. Privacy is under threat from state actors and private firms, which are fighting efforts to curb their access to private data.

If the EU fails to secure data privacy, its citizens will see their data flowing out of Europe, treated according to the lowest privacy standards available, and used to feed the AI industrial development and surveillance capacity of third countries and their companies. Europeans' fundamental rights would be damaged, and European firms would lose their competitive edge, market opportunities, and revenue.

Apps with lax data privacy standards developed by third countries – most often authoritarian states such as China – are already collecting enormous amounts of Europeans' data, which may be used for surveillance, coercion, and aggressive marketing techniques. The EU's failure to act would aggravate these problems. The worst-case scenarios of digital surveillance and surveillance capitalism running wild are truly dystopian. People risk being tracked in every aspect of their lives, and being influenced without realising it – be it in buying certain products or voting for certain political actors.

If the EU does not export these regulations and ensure that the global governance of data is regulated according to European-like standards, its citizens will not be fully protected. At the same time, billions of people will lose their rights to privacy. Surveillance regimes would be strengthened, and democracies weakened. This could undermine and even destroy the democratic process and embolden authoritarian regimes.

Foreign interference

Technologies can create not only dependencies but also direct ways for states to interfere with others.

The EU will need to protect itself against such interference – but should also keep in mind that it may be able to utilise these tools itself.

Disinformation and securing democracy

Back in 2010, at the time of the Arab uprisings, the belief was that the internet would help democracy spread and consolidate across the globe. A decade later, Freedom House is reporting a sustained global decline in democracy, and the World Health Organization is using the word "infodemic" to characterise the influence of disinformation on the covid-19 crisis.

Contrary to the expectation that the open, horizontal, and decentralised nature of the internet would help citizens connect with each other and push for democracy, authoritarian governments have successfully mastered digital technologies to enhance their power and control over their citizens, help other authoritarian or illiberal governments control and repress their citizens, and undermine democracies. While citizens in established democracies have lost faith in democracy and supported populist or illiberal forces, authoritarian regimes have turned social media and digital technologies into effective tools of surveillance and social control, suppressing democratic opposition.

Social media companies' business model of advertising to captive audiences and harvesting user data has led to an economy of attention that prizes emotion, increases political polarisation, and erodes trust in institutions. And, because of a lack of adequate regulation, these companies are vulnerable to foreign influence operations and electoral interference designed to fuel extremism, undermine citizens' trust in political institutions, and suppress criticism of authoritarian regimes. However, the problems of disinformation and the use of emerging technologies for interference in the political process go beyond social networks. AI-enabled "deepfakes", for example, have already been used to trick EU politicians, a tactic that one can expect to become an ever-greater problem.

Unless democracies curtail foreign influence operations and electoral interference, they risk decline as more and more voters lose trust in political institutions. Citizens might stop supporting democracy – at home and abroad – and human rights promotion policies, alliances of democracies, and rules-based multilateral solutions to world problems. All this could lead to a values-free EU foreign policy. At the same time, authoritarian regimes could tighten their grip on their citizens by showing them that democracy is not a model they should aspire to. If democracy and liberal values lose their pre-eminence, this will undermine the liberal multilateral order – helping authoritarian regimes capture or weaken global governance institutions. Much as authoritarian governments export AI surveillance technologies to like-minded partners and allies, the EU should, apart from protecting democracy at home, provide struggling democracies abroad with the technology to protect their public sphere and

elections.

Military and defence

There have been moments in history when warfare changed because of the introduction and innovative use of new military technology. From the crossbow to gunpowder, tanks to nuclear weapons – when technologies are introduced and used in novel ways, they can have a fundamental impact on how wars are fought, militaries are organised, and strategies are developed. New technologies, particularly AI, might initiate such a fundamental change. Artificial intelligence can enable new types of military systems in everything from logistics and sustainment to cyber operations and autonomous weapons. The adoption of AI in the military realm could change the global balance of power, by giving new actors decisive military capabilities. Military AI is emerging as a new frontier for great power rivalry.

If Europe does not address the changes in warfare that AI is likely to bring about, it will become vulnerable to new forms of attack. In the worst-case scenario, Europe's defences could be fundamentally compromised (through, for example, the erosion of nuclear deterrence). European countries' interoperability with the US, their most important NATO ally, would be weakened and their opponents militarily emboldened. Even if it avoids this scenario, Europe will be unable to shape the debate on the use and possible regulation of AI-enabled military systems if it avoids the issue.

In contrast, by engaging with the military applications of new technologies such as AI, the EU could strengthen its capabilities, thereby helping guarantee the safety and security of its citizens. Europe's military-industrial base could receive a boost through work on cutting-edge technology. AI-enabled capabilities could become an important area of cooperation between European companies, thereby strengthening common European defence. Working with allies to streamline the use of AI within NATO would not only guarantee a continuation of interoperability but could also improve interoperability between allied forces – through the use of AI-enabled command and control. Finally, by engaging in the debate on the military applications of AI, Europe could help mitigate the most problematic uses of systems such as lethal autonomous weapons.

What Europe needs to do

ECFR has put forward recommendations on how to address all these sources of vulnerability, from 5G and undersea cables to military AI. The EU needs to improve its data sovereignty by adopting strict regulations on data privacy and ensuring that these are exported to countries and companies that access Europeans' data. EU member states should create an ecosystem in which smaller 5G players

that focus on software and virtualisation can scale up their operations and cooperate effectively with larger European and US companies. The EU should heavily invest in exporting technologies and practices that protect democracy and help achieve technological sovereignty, and in learning from others' experiences in this realm.

But more important than these individual fixes is deeper engagement with the external implications and geopolitical power elements of technology. This engagement has an external element of reaching out to partners and an internal element of ensuring close cooperation between the EU and its member states.

Outreach to partners

The EU needs a global strategy for improving its partners' access to reliable and safe technology. Otherwise, the bloc will leave a space that others will fill. Democracies would be further weakened and impoverished. Autocracies would thrive. Europe would be wrong if it thought it could set out its own rules and standards and let the rest of the world adapt. The Brussels effect, by which Europe silently exported its data privacy regulation to the rest of the world, will not easily repeat itself. GDPR happened when technology was still under the geopolitical radar. Now, technology has been (geo)politicised and both governments and industry actors know how closely intertwined power, technology, and regulation are.

Both China and the US are reaching out to third countries. The US has programmes such as The Clean Network, which aims to help its allies end their use of Chinese 5G. The Chinese Belt and Road Initiative includes a digital component. And Chinese firms, with governmental support, export facial recognition and surveillance techniques to autocracies around the world.

The challenge for the EU is in working with like-minded countries and multilateral bodies – such as the Organisation for Economic Co-operation and Development (OECD), but also regional arrangements such as those in Latin America, Africa, and the Indo-Pacific – to develop fair, open, and values-driven technological standards. The EU should deploy the incentive of access to its digital market to strengthen its alliances. The bloc should use its financial institutions to incentivise EU firms to invest in countries that are seeking to adopt these critical technologies but, at the same time, want to reduce their technological dependence on China. The EU should also consider establishing a comprehensive and compelling tech package that would allow it to become a geopolitical player in the area. This 'tech compact' should include: upgrading existing or prospective trade agreements to grant improved access to the EU digital services market to countries that comply with EU standards in areas such as data flows, privacy, and AI; offering technical assistance to governments and parliaments

wishing to align with the EU on regulatory issues; offering funding guarantees for connectivity investments; coordinating positions on technical standards in multilateral organisations; and offering cyber security and democracy-protection packages. In contrast to other great powers, whose tech offers are often based on coercion and the exploitation of weakness, the EU should stand for a principled approach based on partnerships, mutual interests, consent, and solidarity. Also, as it is already doing, the EU should continue scanning its internal market for vulnerabilities in critical technological sectors, identifying high-risk vendors, and ensuring reciprocity in market access to these technologies for countries that restrict or curtail digital trade.

It will not be sufficient for the EU to merely approve internal regulations in the expectation that others will accept them, such as in the case of the GDPR. For example, the bloc is already operating on bilateral agreements with like-minded countries such as Japan to implement data privacy clauses that ensure the free and safe flow of data. But this is not enough in itself. The EU should aim higher – through multilateral institutions such as the OECD and the International Monetary Fund, or through groupings such as the G20 – to establish a global data privacy regime whose standards are valid for most democracies, if not for all countries (as those ruled by authoritarian regimes may opt out).

A key component of this is the transatlantic relationship. A major agreement on data privacy with the US would help break the current dynamic of regulatory fragmentation, helping both the country and the EU jointly take on China and other illiberal regimes.

The importance of cooperation between the EU and its member states

The European Commission and other Brussels institutions are positioning the EU as a powerful actor in the global debates about tech regulation. But not all member states appear to feel the same sense of urgency. As of today, 21 member states have now published AI policy documents in which they identify areas of focus, develop recommendations, and decide funding priorities. These strategies reveal that most EU member states primarily see AI through an economic lens. Almost all the strategies were written by or under the leadership of economics ministries (or variations thereof) or, less often, ministries of innovation. With very few exceptions – such as France – most EU countries do not engage with the challenges posed by the way that the development and use of AI might affect the international balance of power. Even fewer discuss or even mention the impact of AI on defence.

If the EU moves forward on technology issues without the support of its member states, it risks losing credibility and the capability to influence others. Worse, it could leave empty spaces in Europe that external actors fill.

But, if the EU and its member states work together closely on technology issues, the bloc will be strengthened – and will lead by showing that its rules and regulations, such as those on privacy or trustworthy AI, work at home. In this, the EU can benefit from member states' diplomatic reach in various regions.

It is crucial for Europe to recognise and consider the international second- and third-order effects of any actions it takes in the technological space. It needs to acknowledge that these actions have an impact on its geopolitical power. They influence the EU's soft power as a role model, its positioning relative to other major players' plans, and its geopolitical room for manoeuvre.

Acknowledgments

The authors would like to thank the ECFR 'tech team' and other ECFR colleagues for their input and expertise, particularly Anthony Dworkin, Carla Hobbs, Mark Leonard, Janka Oertel, and Arturo Varvelli, as well as ECFR council members Christoph Steck and Andrew Puddephatt. They are also grateful for the support of the ECFR editorial team.

About the authors

Ulrike Franke is a senior policy fellow at ECFR and leads ECFR's Technology and European Power Initiative.

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

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: 978-1-914572-06-7. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.