# \*\*\*\*EU Counterplans—GDI22 Packet\*\*\*\*

# CP – EU Only

### 1NC – Shell

#### The European Union should increase its security cooperation by: encouraging Member States to incorporate resilience as a core concept; establishing common European cyber security standards for products across markets; supporting cyber coordination through Security Operation Centres, increasing coordination of the Joint Cyber Unit; supporting expansion of industry partnerships to appropriate non-members; supporting foresight analysis; supporting the development of a cyber code of conduct.

#### EU solves – cyber doctrine creates the conditions for collective cyber defense.

Breton 21 (Thierry Breton is a French business executive, politician, writer and the current Commissioner for Internal Market of the European Union, 9-16-2021, How a European Cyber Resilience Act will help protect Europe, published on LinkedIn, https://www.linkedin.com/pulse/how-european-cyber-resilience-act-help-protect-europe-thierry-breton/)

"If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. [...] This is why we need a European Cyber Defence Policy, including legislation setting common standards under a new European Cyber Resilience Act."

With these strong words in her 2021 State of the Union address, European Commission President Ursula von der Leyen expressed the geo-strategic dimension of cybersecurity and cyberdefence. And why it is essential for Europe to invest substantially and urgently in the face of cyber threats of all kinds: security, defence, hybrid.

The world is vulnerable to large-scale cyber attacks

Recent events remind us of the extent to which Europe, and more generally the world, remains vulnerable to large-scale cyber attacks. These include attacks on the Irish health care system in the midst of a health crisis. The ransomware identified by Kaseya. The hacking of the Colonial Pipeline. Or the cyber attacks against the municipality of Anhalt-Bitterfeld in Germany or those targeting Thessaloniki in Greece. According to the European Union Agency for Cyber Security, ENISA, attacks on our supply chains will increase fourfold in 2021 compared to last year. And attacks on cloud infrastructure have increased fivefold in one year. Transport, government and industry sectors are the most affected. With the explosion of connected objects and the increased use of industrial data, the risk surface is merging with our entire continent. Moreover, cyber technologies are by definition dual. The line between cyber security and cyber defence is becoming increasingly blurred. Whether the attack is motivated by greed or by a desire to destabilise a country, an economy, or democratic processes such as elections, the penetration techniques are often the same. Faced with these new kinds of threats, we cannot remain with our usual silo reflexes. We must have a common European approach that integrates all the dimensions of cyber, whether civilian or military. **To protect ourselves better, our only option is to act together, at European level.** In an interconnected single market, we are only as strong as the weakest link. We must therefore improve our level of security collectively. Today, given the diversity and sophistication of attacks, no country can face a cyber threat alone, as it knows no borders. To do this, we need advanced technology, secure infrastructure, common requirements, increased operational cooperation and effective sanctions. This is what President Ursula von der Leyen has announced.

Europe must become a leader in cybersecurity, through a genuine European Cyber Defence Policy, in order to protect, detect, defend and deter. This new policy will of course build on what has already been put on the table, both in terms of regulation and technology. It will be a matter of taking our ambition a step further.

Increasing our collective resilience

Firstly, protect, to increase our collective resilience.

To do this, we must ensure our technological sovereignty in the cyber field. Our real strategic autonomy and ability to act will depend on our ability to master and develop cutting-edge technologies in Europe.

We estimate that the EU, its Member States and the private sector could invest up to €4.5 billion over the period 2021-2027 in the development and deployment of cyber security technologies. This amount should be complemented by investments from Ministries of Defence as well as from the European Defence Fund.

I am counting heavily on our new European Cybersecurity Competence Centre based in Romania to organise European technological research more effectively and to strengthen our technological sovereignty. However, in order to mobilise all efforts in a coherent manner and to avoid duplication, I believe that we must work together, within the framework of the Cyber Defence Policy announced by the President, to draw up a specific European cyber capability plan integrating all civilian and military needs. This would make it possible, for example, to combine all efforts in the field of research and quantum technology, which will ultimately change the security of the digital space as we know it today. We will build on the Observatory of critical technologies that we have set up.

In addition to technology, we must also act on the regulatory front to raise the level of security within our single market. We have therefore proposed a revision of the Network Security Directives (NIS) to provide a framework for the obligations of the main economic players.

**In order to increase our resilience,** **we need to establish common European cyber security standards for products (especially connected objects) and services that are placed on our market**. This will be the purpose of the European Cyber Resilience Act announced by the President. I believe that this Act should also have a defence dimension in order to maximise synergies, enabling, for example, defence requirements to be taken into account.

From 190 days to several hours to detect a sophisticated attack

**Then, detect.**

**Today, it takes an average of 190 days to detect a sophisticated attack**. We must drastically reduce this time to a few hours. This is an imperative condition for greater resilience. Because early detection means that the necessary countermeasures can be put in place quickly.

This will involve setting up a European network of Security Operation Centres (SOCs) which will – in conjunction with national and private SOCs – scan the network using artificial intelligence technologies and detect weak signals of attacks. A true "cyber border guard" of our European information space, this network of SOCs must be able to integrate information from national or, in the long term, European military SOCs (financed, for example, by the European Defence Fund).

Joint Cyber Unit

Defend, too.

Europe must be better equipped to deal with a major attack. This is the ambition and the objective of the Joint Cyber Unit that we presented last June in order to lay the first foundations for an operational crisis management capability and European solidarity.

We have clearly identified the shortcomings of the current system: too many cybersecurity players, who work in silos, in a fragmented way.

So we need more operational and technical coordination.

Such a unit could thus work closely with the Joint Situation Awareness Centre mentioned by the President.

Develop a real doctrine on cyber attacks

Finally, dissuade.

To become a global player in the cyber field, Europe needs to develop a real doctrine on cyber attacks as well as operational and offensive cyber defence capabilities.

We must be able to move forward on our attribution capabilities and develop a real cyber diplomacy as we have just done with the first sanctions against those having carried out cyber attacks in Europe.

The aim must be to gradually develop a genuine operational cyber pillar as an integral part of our ambition for a common European defence. Yes, it is a complicated and delicate subject because it touches the heart of our Member States’ national sovereignty, but now is the time to address it. I believe that this will be one of the important elements of the Strategic Compass carried by the High Representative Josep Borrell.

\*\*\*

Faced with cyber threats, the European Union cannot compromise and must do everything possible to increase our resilience, together with its Member States. To preserve our industry, our public services, our infrastructures, our security and defence.

That is also what European technological sovereignty is all about.

#### Overextending NATO presents financial and security risks – offloading is necessary to preserve collective defense.

Moller & Rynning, Seton Hall & University of Southern Denmark Professors, ‘21

[Sara Fjerg Moller, Assistant Professor, School of Diplomacy and International Relations, Seton Hall University and Sten Rynning, Professor, Center for War Studies, University of Southern Denmark, “Revitalizing Transatlantic Relations: NATO 2030 and Beyond,” WASHINGTON QUARTERLY v. 44 n. 1, Spring 2021, p. 193]

NATO’s continued transformation in the coming years seems all but certain; less certain is what it will transform into. The alliance has survived this long by adapting. But unlike during previous rounds of adaptation that involved the alliance taking on more responsibilities and tasks, the coming decades—whose defining feature will be the continued rise of China—will require a much more narrowly focused alliance. For nigh on three decades, NATO had the luxury of pondering what kind of alliance it wanted to be as it searched for a new raison d’etre in the reduced threat environment following the end of the Cold War. But the contrast between the 1990s and today’s deluge of challenges and threats is stark, and NATO **no longer has the luxury of time.**

To ensure the alliance’s future operational utility, the alliance must embrace its original collective defense identity and **look for ways to streamline, and** where possible **reduce**, its **existing collective security and crisis management activities**. In addition to offloading existing responsibilities to the EU and UN, NATO should think twice before taking on new mandates and **avoid elevating new tasks like resiliency** or counterterrorism missions and assigning them equal importance to Article 5. The alternative to the vision outlined here is an alliance increasingly weighed down by a myriad of tasks, unable to prioritize among them, and lacking both the political will and financial resources to perform its main function. An overburdened NATO risks being unable to fulfill its chief purpose of collective defense, thereby increasing the risk of further fracturing within the alliance. The proposed course of action will by no means be an easy one. But it provides the best chance to guarantee that the transatlantic alliance will have the capabilities and assets needed to meet the challenges posed by China’s rise.

#### Increased presence in digital diplomacy and global security initiatives aligns the EU with the U.S. as a catalyst for global leadership

Ringhof and Torreblanca 22 (Julian, Visiting Fellow at ECFR, José Ignacio Torreblanca; Head, ECFR Madrid Senior Policy Fello, 5-17-2022, The geopolitics of technology: How the EU can become a global player, European Council on Foreign Relations, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/#the-eu-a-geo-technology-player-in-the-making)

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.

#### US-EU leadership is zero-sum and EU regulatory cred prevents global war

* Trade wars, great power conflict, multilateral institution breakdown

Dworkin, 18 (Anthony Dworkin, visiting lecturer in the Paris School of International Affairs, and Mark Leonard, co-founder and director of ECFR, "Can Europe save the world order?," European Council on Foreign Relations, 5-24-2018, https://ecfr.eu/publication/can\_europe\_save\_the\_world\_order)

The world is becoming a scarier place. Trade wars loom, great-power competition is returning, proxy conflict is spreading, and President Donald Trump has withdrawn the United States from the Iran nuclear deal and the Paris agreement on climate change. Rules and alliances that once promoted international cooperation and stability seem to be losing their hold. In their place, there is a resurgence of international relations based on assertive nationalism, winner-takes-all competition, and disdain for the rule of law. Hopes that international politics would encourage the spread of democracy and human rights have faltered, while authoritarianism and illiberalism are in the ascendant. These changes have led many people to argue that the liberal international order developed after the second world war is breaking down.

The rules-based order is under threat both from inside and outside. For most of the period since 1945, it was a joint project of the US and its European allies. But now Europe must respond to a radical shift in which the US – under Trump – has become a significant threat to the system. Trump’s policies and disregard for European views and interests have created a crisis that compounds longer-term strains on the international order. In response, the European Union urgently needs to design and implement a strategy for preserving the core elements of a rules-based order. This policy brief attempts to work out a vision of international order that could guide the EU, and to suggest how the EU could put this vision into practice.

The EU is heavily invested in the idea of a rules-based international order. The Union exemplifies the belief that states are most able to prosper through cooperation, openness, and a rule of law that incorporates a commitment to democracy and human rights. The EU’s international standing is linked to the credibility of the principles it embodies. More practically, European countries want an international order that protects them from external threats and allows them to promote their economic interests through worldwide trade and investment. European public policy is committed to the principle that multilateralism is the best way to create global public goods. Given these positions, the EU has good reason to be concerned about the condition of the liberal order, and to develop policies that aim to restore or preserve the order’s most important elements.

Yet this goal cannot be achieved merely by trying to roll back attacks on the order to recreate the international system as it existed in the past. The liberal order was never settled or perfect. It was an evolving, multilayered framework of norms, institutions, and practices that had internal tensions and weak points. Although it offered many benefits to its participants, the order was less consistent and inclusive than its proponents liked to think, and it was based on a distribution of global power that no longer exists. The task for the EU is not to look back but to shape a renewed vision of international order that is suited to today’s world, and to European interests and influence as they are now.

The liberal order’s evolution and challenges

The effort to develop a European vision for an adapted rules-based order requires an understanding of the international system’s evolution since the second world war. In the aftermath of the conflict, its victors set up a system of collective security focused on the United Nations and based on the principles of the prohibition of aggression and the peaceful settlement of disputes. As the cold war began, the US took the lead in establishing an alliance system that aimed to shore up democratic capitalism among its European allies by containing the advance of communism, liberalising trade with US allies, and promoting economic stability through international institutions.[1] This system could be described as “liberal order 1.0”. Although American leaders often presented themselves as defending the free world, some countries that the US supported – especially beyond the “core” of western Europe, Japan, Canada, Australia, and New Zealand – were more obviously capitalist and anti-communist than democratic. This order largely stopped at the borders of states and was less concerned about how they exercised sovereignty internally.

After the end of the cold war in 1989, the system evolved. The US promoted the development of a new settlement during the 1990s and early 2000s, creating what can be described as “liberal order 2.0”. The guiding idea was that the principled order established in the West after the second world war would be progressively rolled out to states not originally included. At the same time, in large part under European impetus, there was a deepening of the order to take account of the rights of individuals as well as states, and a partial embrace of a more constrained idea of sovereignty.

This second phase of liberal international order was not only a system of rules and institutions, but also a bet. It involved an expanded system of trade rules based on the World Trade Organisation (WTO) and mechanisms for enhancing economic coordination through international financial institutions and the G8. There were also gestures towards a greater commitment to human rights through institutions such as the International Criminal Court (ICC) and the norm of the responsibility to protect civilians from large-scale violence. The bet was that countries of the former Soviet Union and emerging powers such as China would converge on a basic minimum of liberal norms, and that global security cooperation through the UN could focus on new goals such as averting mass atrocities or suppressing international terrorism.

The problem now is that, while the goal of knitting the world together economically has been achieved, the bet on the consequences of this integration has not paid off. Non-Western powers have gained in wealth and global influence; however, there has been a decline in liberal democracy. At the same time, the supposed defenders of liberal order implemented its principles in ways that were sometimes self-interested or inconsistent, forfeiting the support of even emerging democracies while failing to convince their own populations of the benefits of internationalism.[2] The liberal international order turned out to be a work in progress that was capable of regression. More precisely, the aspirational goals embodied in the ideal of liberal international order are being challenged on three axes:

Externally, many countries that were supposed to join the system are instead using their influence to pursue an old vision of great power politics in new ways; these states include China, Russia, Iran, Saudi Arabia, and Turkey.[3] As the distribution of power shifts, even emerging democracies look at the world through a post-colonial mindset rather than a post-cold war one – and they are unwilling to endorse an order that they see as linked to the dominance of the US and the West more broadly. For these powers, the liberal international order looks like “the world imperialism made”, in the words of the writer Pankaj Mishra.[4]

Internally, the bargain that supported liberal foreign policies has come apart. Many citizens in the West now see openness and international engagement as working against their interests – as reflected in declining support for liberal internationalism in European countries. This public disenchantment lies behind the United States’ willingness to maintain its traditional role as the military and economic anchor of the system – as shown in Trump’s dramatic policy reversals.

Transnationally, new challenges and forms of disorder have emerged that current structures fail to address, necessitating the development of new norms. Changes in the nature of conflict threaten to loosen the international rule of law; there are no adequate regimes for dealing with migration and refugees; and the regulation of cyberspace has failed to keep pace with its impact on people’s lives.

One interpretation of these developments is that the guardians of world order over-reached in the years after 1989. The rise of sovereigntist powers such as Russia and China, and liberal countries’ actions that undermined the legitimacy of the system, halted the utopian project of building liberal order 2.0. Partly due to the calamity of the 2003 US-led invasion of Iraq, the onset of the financial crisis in 2007-2008, and the subsequent travails of the euro, support for liberal order 2.0 will collapse. In its place there will be a return to a “thinner” international order – closer to liberal order 1.0 – that strips out any orientation towards human rights and democracy, focusing more on non-intervention and minimal rules of coexistence between great powers with different political visions. In this account, Trump does not represent a major break with past US administrations. Very few of them believed that the US should be subject to binding rules – they were just keener to impose them on other countries.

But there is a darker reading of our situation. In this view, we will face a rollback of even liberal order 1.0, driven not just by revisionist external powers but also by a political counter-revolution within the West. A new kind of globalisation – “world order 0.5” – will combine the technologies of the future with the enmities of the past. Military interventions will continue, but not in the humanitarian form that saw Western powers curtail genocide in Kosovo and Sierra Leone. The development of technology will spur a series of connectivity wars as states weaponise trade, the internet, and even migration.[5] In this world, multilateral institutions and regimes will become battlegrounds rather than brakes on conflict. Domestic politics that increasingly revolves around identity politics, distrust of institutions, and nationalism will foster greater international conflict.

The task for Europe is to find an alternative to these two regressive scenarios, one that accounts for both the rising influence of illiberal powers and the extent of global connectivity, and that European citizens can endorse. This will mean finding principles of order that can be effective in a multipolar world while working to advance progressive solutions to global problems as far as possible and craft a new social and economic compact within Europe’s borders. Pursuing this vision will require Europe to differentiate between the separate components of international order, matching priorities to capacities in different areas. It will also mean developing a specifically European strategy on international order.

Much discussion of the fate of liberal international order has come from analysts in the US and has adopted a US perspective. It tends to focus on promoting internationalist stances within the US policy debate.[6] But, while Europe and the US were closely aligned on questions of global order during the cold war, their interests today are more divergent. Europe has greater exposure to the effects of conflicts to its east and south, different economic concerns and regulatory standards, and a political culture that is much more accepting of multilateralism and international judicial oversight. The EU may be better placed than the US to distinguish between the preservation of a rules-based system and the maintenance of the US military and economic hegemony that has supported the liberal order up until now.[7] And Europe must adjust to the shifts in US policy that Trump has made – including his rejection of the Iran nuclear deal, or Joint Comprehensive Plan of Action (JCPOA), which the EU saw as one of its main diplomatic successes of recent years.

The effort to renew the foundations of international order should also incorporate a clear vision of its underlying purpose. The idea that internationalism has benefited some groups or countries unequally, and that interconnection is a source of more threats than opportunities, lies behind the loss of support for multilateralism. In this sense, Europe must construct a renewed order on the basis of the needs and concerns that it addresses. In the way that French president Emmanuel Macron has called for a “Europe that protects”, the EU should seek to promote a “multilateralism that protects”, showing more clearly how the elements of international order that it prioritises work to the benefit of European citizens’ security and prosperity.

Europe should adopt a three-dimensional strategy on the future of international order:

The EU must invest in defending liberal order 2.0 within the European sphere. This involves an attempt to strengthen the EU’s defences and resilience across several policy areas, as well as an effort to strike a new bargain between losers and winners within the EU.

Beyond Europe, the EU should explore ways to develop an adapted version of a principled, rules-based order. Because the EU cannot (and would not want to) close itself off from the world, it should work to, as far as possible, establish the kind of order it sees as the best foundation for long-term stability and development in Europe and elsewhere. To do this, it will have to identify a wide range of potential partners and be prepared to rethink some of the supposed premises of liberal order 2.0.

On a global level, there are areas in which the EU will need to prioritise a minimal threshold of rules-based order over any more ambitious attempt to promote liberal goals. Because even a renewed coalition of like-minded states cannot achieve its objectives in the face of more assertive and powerful illiberal states, this may involve compromising on European ideals in some cases and pulling back to a more sovereigntist agenda.

Given that the international order is not monolithic, we can identify priorities for Europe by breaking down the challenges it faces into four thematic areas. Two of them – security and trade – involve central features of the existing order that are increasingly under strain. In the other two – the global challenges of migration and climate change, and cyberspace – the existing order is underdeveloped and Europe needs to work with others to help build new regimes.

War, crisis management, and human rights

It is often said that recent years have seen the return of geopolitics, led by a newly assertive Russia and China. Both countries have challenged existing regional settlements, albeit in different ways. Russia’s actions in Ukraine, including its annexation of Crimea, attacked the post-cold war dispensation in Europe and the principle that states should not acquire territory through force. In other areas, Russia has sought to project its power through grey-area interventions or through support for allies such as the Syrian regime. Russia aims to limit the advance of Western institutions and norms in its neighbourhood, and to promote an order based on realpolitik rather than liberal principles.[8] China has acted forcefully to pursue what it regards as core interests in its maritime neighbourhood, including through extensive land reclamation in the South China Sea. It rejected a ruling against it from the Permanent Court of Arbitration at The Hague, and has pursued a strategy of legal ambiguity about its maritime claims.[9] China has dramatically increased its defence capabilities in recent years with the apparent goal of achieving military parity with the US, if not dominance, in east Asia.

This newly competitive environment emerged as Western enthusiasm for military intervention waned in the aftermath of costly and unsuccessful wars in Iraq and Afghanistan. President Barack Obama shifted the US in the direction of “light footprint” (albeit extensive) counter-terrorism operations; Trump has followed the same approach, while stepping up the level of force involved. Beyond their lack of success, the United States’ wars in the Middle East and south Asia also undercut its claims that it was upholding a principled, rules-based international order. Even within the West, many people believed that the invasion of Iraq was an act of aggression. Many emerging democracies thought that Western military action in Libya in 2011 went beyond the Security Council’s authorisation of the use of force for civilian protection, and became an illegitimate campaign aimed at regime change. The fallout from the Libya operation was one factor in emerging democracies’ decision to abstain in the UN General Assembly vote on Ukraine in March 2014, as they wanted to distance themselves from what they saw as the double standards of Western powers.[10]

The military priorities of Western states have also diverged since the end of the cold war. The US does not believe that it needs to invest as heavily in the defence of Europe as it once did, and has a much lower stake than the EU in the stability of Europe’s eastern and southern neighbourhoods.[11] Early doubts about Trump’s commitment to NATO have subsided for the moment, while his administration has published a National Security Strategy that focuses heavily on renewed great power competition. Under Trump, the military part of the Western alliance has fared better than many people feared it would during the early months of his presidency.[12] Resisting Russian and Chinese assertiveness – including through the use of sanctions and actions to reinforce the principle of freedom of navigation in open waters – remains a viable Western strategy under US leadership. Indeed, it is disconcertingly unclear whether Europe should worry more about US hawkishness towards or accommodation of rival powers. Nevertheless, Trump could change his mind on Russia (though this would meet with serious opposition in Washington) or take steps to further weaken the US system of alliances in east Asia. Either way, Europe will have to take more responsibility for its own defence – as a condition of continued US engagement, and to promote its interests by helping stabilise neighbouring regions.

Together, these trends point towards a more limited vision of international order than some people hoped for after the end of the cold war. In the 1990s, many Europeans came to see sovereignty as an occasionally regrettable constraint on intervention to halt mass atrocities and efforts to bring those responsible to justice. Now, at a time of assertive rival powers and widespread disorder that is often fuelled by external intervention, it seems more of a priority to reduce the threat or use of force across state borders in violation of the UN Charter. Russian and Chinese opposition means that Western-led military intervention against a state oppressing its own people would be unlikely to gain Security Council authorisation – and could undermine the international rule of law at the same time as it sought to uphold international norms.[13] It may also be harder to win Security Council approval for referrals to the ICC. While the court will continue to play a role in global politics (particularly in cases involving countries that are party to it), the EU should temper its expectations that the ICC will, in the short term, bring members of hostile regimes to justice or have significant influence on active conflicts.

In a world in which great powers embrace a range of different value systems, the EU would be more able to sustain international order if it shifted back towards emphasising the value of sovereignty. In the categories of the Danish political scientist Georg Sørensen, this would mean prioritising a “liberalism of restraint” above a “liberalism of imposition”.[14] The former approach would be more likely to win support from non-Western democracies and to make it easier to build broad coalitions for Western efforts to constrain the use or threat of force by other powers. It would also accommodate the reality that, in a more competitive geopolitical environment, the West will be less able to dictate the terms on which conflicts are settled and may have to accept an imperfect and illiberal peace as the price for ending violence.[15] This effect is clearly visible in the case of Syria: it is hard to see how any peace agreement will involve President Bashar al-Assad’s swift departure from power or measures to bring regime officials to trial for war crimes.

Against this background, Europeans may need to fight a fallback campaign to try to keep their humanitarian vision of multilateralism alive in other ways. The most important is through diplomacy and mediation. Despite attempting to organise a summit with North Korean leader Kim Jong Un, Trump’s strongest effect on international politics has occurred through his rejection of predictable and consistent negotiations aimed at reducing international tensions. Trump’s abandonment of the JCPOA, decision to move the US embassy in Israel to Jerusalem, and apparent embrace of Saudi Arabia’s hard line on Iran are making the Middle East more volatile. The shift in US policy has created a global diplomacy deficit, and the EU should make it a priority to try to fill this gap. In the short term, this means trying to save the JCPOA by encouraging Iran to stay within the deal while trying to limit the effect of renewed US sanctions on European companies.[16] Beyond this, the EU may need to think creatively about how to bolster the global non-proliferation regime and make a greater effort to de-escalate tensions and promote peace in conflicts from Yemen to Ukraine.

The EU should also fight to support humanitarian and human rights principles within the UN system, at a time when they are increasingly being challenged.[17] Even in conflicts in which great powers are not involved through the support of proxies, the Security Council is finding it harder to agree on peacekeeping interventions.[18] Meanwhile, China has become increasingly active at the UN in promoting a state-centric vision of human rights and in limiting the organisation’s human rights activities through budget cuts.[19] With a US administration that is less committed to multilateralism than its predecessor, it is up to Europe to try to build broad coalitions that can counteract these trends. The EU should also work with like-minded countries to reinforce standards for upholding the rule of law in armed conflict.[20] This effort is especially important at a time when widespread violations of international humanitarian law, the growing role of non-state groups as government proxies, and the evolution of transnational counter-terrorism campaigns – many of which rely on armed drones – are eroding these standards.[21]

The EU will be best able to fight a normative battle against the conceptions of international order presented by Russia, China, and perhaps the US if it presents a convincing case for its own model. Strengthening the EU’s internal cohesion and resolving cleavages within European countries will allow the EU to be more resilient in the face of external campaigns of disruption.

Trade and investment

The development of open, rules-based economic interaction between states is at the heart of the European vision of international order. Taken as a whole, the growth in international trade since the second world war has had impressive economic benefits. Between 1950 and 2015, global average real income per head rose nearly fivefold, and the proportion of the world’s population in extreme poverty fell from 72 percent to 10 percent.[22] In the decades following the 1980s, there was a particularly large increase in cross-border flows of goods, services, and finance.[23] But it is now clear that the Western-led economic order has been, in one sense, too successful and, at the same time, not successful enough.[24] The rising wealth of the developing world has made the West’s dominant role in the economic order unsustainable. Meanwhile, the gains from the market-driven globalisation of recent decades were unequally distributed in a way that has undermined the legitimacy of the entire order.

The liberal order put in place after the second world war was meant to provide an international infrastructure that allowed states to pursue progressive policies at home. The corollary of an open world economy was that governments would stabilise and protect market economies at home through the development of welfare states.[25] However, in the last two decades, as globalisation has accelerated, this link appeared to break. Many Europeans and Americans now see economic openness as benefiting emerging economies and privileged Westerners at the expense of large sectors of the Western working and middle classes (although, in much of Europe, the persistence of social spending moderates this effect). While many economists believe that technological change drives much of the loss of manufacturing jobs in Western societies, recent research suggests that the entrance of China and other emerging economies into the global trading system has also contributed significantly.

Trump has acted on this perception by withdrawing the US from the Trans-Pacific Partnership trade agreement and calling for the renegotiation of the North American Free Trade Agreement. More alarmingly for Europe, he has also moved to undermine the essential basis of the rules-based multilateral trading system by attacking the WTO. Trump has repeatedly called the WTO a “disaster” for the US.[26] Under his leadership, the US has held up the appointment of judges to the WTO’s appellate body, threatening to bring the organisation’s dispute settlement mechanism to a halt. Trump has also imposed unilateral tariffs on steel and aluminium under a spurious “national security” justification that weakens the system’s credibility, and promised further tariffs aimed at China without following WTO procedures – raising fears of an all-out trade war between the world’s two leading economies.

The irony is that Trump’s pushback against free trade comes at a time when there is growing acceptance in both Europe and the US that China has exploited the international trading system to its advantage.[27] China’s accession to the WTO did not lead to further steps in the progressive opening of its economy, and the WTO system has proved unsuccessful in regulating asymmetries in China’s approach to trade as the country’s income has increased. The EU, the US, and other economic powers such as Japan might still be able to work together within the WTO rules to seek greater reciprocity in economic relations with China. But faced with a threat to the equal-access trading regime of the WTO, the EU’s priority should be preserving the rules-based system.[28] The EU should combine its offer to work with the US in correcting imbalances in global trade with a clear statement that it would oppose moves designed to weaken the WTO. The size of the EU market gives it the power to stand up credibly to the US if need be.

In any case, many of Trump’s complaints are backward-looking and fail to address the most urgent current concerns. Shifting patterns of global trade, including the growth of global supply chains, have brought new issues such as investment and trade in intermediate goods and services to the top of the agenda.[29] An earlier ECFR report suggested that the construction of an EU-wide system of investment screening is now the priority in European economic relations with China.[30] These issues have been the focus of a wave of bilateral and regional treaties that provide the EU with the opportunity to pursue a vision of international trade that protects its values. European participation in recent bilateral or regional treaties is predicated on their inclusion of regulatory standards in areas such as labour rights, environmental standards, and data protection. In this way, these treaties add an additional layer of social protection to the WTO system – although critics suggest their impact has been limited so far.[31]

At the same time, as an economic heavyweight the EU is able to unilaterally create regulatory standards that exert a broader international influence through what has been called the “Brussels effect”.[32] The European market is so large that many exporters around the world voluntarily and comprehensively comply with the standards it sets in areas such as food safety, consumer protection, chemicals, and airline emissions. This is because it is often too costly to manufacture different product lines for different markets.

Yet, in other ways, the EU has been forced to come to terms with the fragmentation of the international economic order as non-Western powers, led by China, increase their influence. The creation of institutions such as the Asian Infrastructure Investment Bank (AIIB) and the BRICS-based New Development Bank has challenged the role of the International Monetary Fund (IMF) and the World Bank. Indeed, the veto power that China holds in the AIIB through its voting share mirrors the role of the US in the IMF. According to their supporters, these organisations complement rather than replace traditional international financial institutions for emerging powers, which gain access to bodies more focused on their needs.[33]

Western observers feared that these new financial institutions would undercut the conditionality of the World Bank and the IMF by lending without imposing requirements in areas such as governance and transparency. However, there is growing recognition that the record so far is more nuanced, with the AIIB having aligned more closely than expected with the policies and standards of traditional multilateral development banks.[34] Moreover, Western development assistance has sometimes promoted human rights standards more in rhetoric than reality. There seems greater reason for concern about China’s Belt and Road Initiative, which appears tied to a narrower vision of Chinese economic and strategic advantage.[35] Nevertheless, as reflected in the reach of this initiative, China’s economic power is too substantial to be contained by European policy

Global challenges: Migration and climate change

Even when the liberal international order was at it strongest, there were some areas in which it clearly remained incomplete. One of its most obvious weaknesses was that it did not include an adequate regime for governing the large-scale movement of people across borders. Refugees have continued to suffer from a lack of international protection, and there has never been an effective framework that allocates responsibility for meeting their needs. The 1951 Refugee Convention established the principle of non-refoulement, which protects refugees from forcible return to a country in which they would face persecution. This principle remains at the core of refugee protection but, in other respects, the convention has proven increasingly unfit to cope with changing patterns of displacement. The convention only covers those who are fleeing persecution (as opposed to, for instance, endemic disorder or natural disaster); is geared towards the provision of relief rather than more long-term opportunities; and leaves countries that refugees reach first to bear most of the responsibility for helping them.[36] This regime is now struggling to deal with the highest level of displacement in the history of the convention. Most refugees live in a small number of developing countries, which cannot afford to provide them with the services and economic opportunities they need.

More broadly, there has been a rapid increase in migration worldwide in the last two decades, in line with the development of other facets of globalisation, such transportation and communication. In 2017, there were an estimated 258 million international migrants, accounting for 3.4 percent of the global population.[37] No issue has done more than migration to make citizens of Western countries see international openness as a threat rather than a source of opportunities. This trend has increasingly driven governments in the developed world to adopt an approach to irregular migration that aims to, as far as possible, deter asylum seekers and other migrants from reaching their countries. They have done so by exploiting gaps in the regime of international protection, complying with the law while leaving vulnerable people with inadequate protection.[38] There is a need for an international regime that offers better prospects to those who are forcibly displaced, but that does so in a way that is politically sustainable among electorates in developed democracies.

The classic multilateral method of addressing global challenges such as mass displacement is to negotiate a new international treaty that imposes binding responsibilities on all parties. But in the case of refugees and migration, this path appears blocked. States have no appetite for taking on new responsibilities under the Refugee Convention, and few developed countries have signed the UN Convention on the Rights of Migrant Workers. The Refugee Convention’s definition of refugees is plainly insufficient, but it is likely that opening the convention to renegotiation would lead to fewer protections.[39] Instead, the most promising path towards collective action on migration seems to lie in a newer and more informal vision of global governance based on pragmatism, voluntary adherence, and a diversity of responsible actors.

This year, UN member states are due to adopt two global compacts on refugees and migration respectively – non-binding frameworks that aim to set out guiding principles for collective action. They will be based on the 2016 New York Declaration, which reaffirmed that protecting refugees is a shared international responsibility and pledged “robust support” to countries affected by large-scale migration. This approach builds on the Nansen Initiative on migration caused by natural disasters. Led by a coalition of states from different regions – with the extensive involvement of civil society groups, businesses, and other organisations – the initiative produced an Agenda for Protection that has been widely endorsed.[40] Following this model, refugee and development scholars Alexander Betts and Paul Collier have called for an approach to refugee protection based on pragmatic partnerships involving both states and non-state actors rather than a new or revised legally binding instrument.[41] Similarly, political theorist Michael Ignatieff has identified the response to refugees as exemplifying “a genuine crisis of the universal amidst a return of the sovereign”, arguing that an approach based on generosity and compassion will be more effective than one based on legal obligation.[42] In his words, “maintaining public support to assist strangers and refugees is more likely to succeed if the appeal is cast in the language of the gift, rather than the language of rights”.[43]

There is a precedent for this kind of an inclusive, voluntary approach to global governance in the world’s response to the other great collective challenge of our time: climate change.[44] Climate change has long spurred migration, an effect that will likely become increasingly apparent as temperatures and sea levels rise. In 2015, a worldwide “high-ambition coalition” of states forged the 21st Conference of Parties (COP21) agreement as a hybrid model combining voluntary national commitments with obligations on transparency and reporting.[45] Based on the aspirational principle that parties will increase their commitments over time, the agreement includes a significant role for non-state entities such as businesses, civil society groups, and local governments. These diverse participants will help the COP21 regime survive Trump’s decision to withdraw the US from the agreement (just as he withdrew it from negotiations on the Global Compact for Migration). The “We Are Still In” collection of US states, cities, and businesses that have pledged to continue working towards the US commitment under COP21 would, if treated as a country, have the world’s third-largest economy (after the wider US and China).[46]

This evolving approach to global governance has won support from both the West and emerging powers such as India and China due to its voluntary nature and its embrace of the principle of “common but differentiated responsibilities”.[47] The EU can contribute to its success first and foremost by setting an example, adhering to its targets, and embracing a share of global responsibilities that will be seen as fair. On migration, this will require the EU to find a sustainable balance between showing Europeans that it can control Europe’s borders while offering some legal pathways for immigration. The aim should be to present immigration as a managed and fair process that meets European needs rather than as something to be halted at all costs. At the same time, the EU should increase investment in education and family planning to try to limit population growth in neighbouring regions and hence reduce migratory pressure. On climate change, the EU should supplement its current commitments with a carbon border-adjustment tax to encourage adherence overseas, and make sure that European businesses do not suffer for their efforts to cut greenhouse gas emissions.

Cyberspace

Although policymakers often treat it as a self-contained domain, cyberspace is a dimension of the contemporary world that cuts across all the areas discussed in this report.[48] Indeed, cyber security increasingly preoccupies governments everywhere. Having been largely neglected in the early days of the internet, cyber security concerns have become increasingly prominent in recent years due to attacks on countries’ infrastructure, commercial enterprises, and elections. At the same time, the internet is revolutionising the global economy: it is the world’s most important piece of infrastructure and is set to underpin all infrastructure.[49] Having evolved in a lightly regulated way, the internet has now become the focus of a global debate about the norms that should govern its operations, as people take in the revolutionary impact it is having on both governance and individuals’ private lives.

The governance of cyberspace is an important part of the international order – one in which the principles of openness, security, and inclusivity are at stake.[50] The revelations about data surveillance by the US National Security Agency and other intelligence services, and of the use of data gathered by Facebook, Google, and other companies, has eroded users’ trust in the protection of their privacy online. A handful of companies based in the US now constitute a vital part of the public sphere in countries around the world, and unaccountable algorithms play a significant role in determining people’s financial and life opportunities.[51] At the same time, China’s “Great Firewall” and Russian efforts to control online content herald a future in which a growing number of countries are likely to attempt to create segregated national internets.[52] Efforts to agree on international principles for state behaviour in cyberspace through a UN-sponsored process have faltered.[53] There is a danger that the global nature of the internet, with all the advantages it has for economic growth and free expression, could be further undermined if people in democratic states come to see online connectivity as a more of a threat than a source of opportunities.

It would fit well with the EU’s interests and values to take a leading role in promoting a liberal internet that remains open but offers better protection for users and national security. Europe can stake out a global position that counterbalances both the Sino-Russian sovereigntist approach and US acquiescence to the loosely regulated operation of digital monopolies.[54]

In one respect, the EU has already established itself as a global standard-setter in internet regulation. Its General Data Protection Regulation (GDPR), implemented in May 2018, provides EU citizens with greater control over how companies around the world handle their data. In an example of the Brussels effect described above, some non-European companies have adopted these rules for all their customers, while some non-European countries have accepted the GDPR as the gold standard for data protection.[55] Facebook said it would comply with the regulation “in spirit” for all its customers, although it also gave itself the option of applying looser rules for non-European users by transferring their contracts away from the company’s international headquarters in Ireland. The European Commission has also begun to develop a policy on “fake news”, centring on a call for companies to adopt a voluntary code of conduct on online disinformation.[56]

Despite the importance of these measures, they still fall short of a comprehensive approach that takes account of all the areas cyber policy affects. Europe lacks an integrated vision of how to balance the often competing demands of commercial interests, human rights, national security, and public consent in internet governance.[57] For example, it does not have a considered position on the extent to which political actors should be allowed to exploit personal data. The EU essentially treats personal data as a privacy issue, but it is also a resource that potentially has enormous value to global public goods in areas such as healthcare, security, and environmental protection. European countries should work towards the development of an international system that secures, while distributing the benefits of, personal data.[58]

The EU also has a key role as a supporter of the principle of multi-stakeholder governance of the internet, in the face of new developments such as the sharing economy and the internet of things.[59] The US was a strong backer of the multi-stakeholder principle under Obama, passing authority over domain name administrator the Internet Corporation for Assigned Names and Numbers (ICANN) to a multi-stakeholder coalition in 2016. But Trump has adopted a very different line. There are indications that his administration may look for ways to reverse the handover of ICANN (although it is unclear how this could be achieved).[60] Since US advocacy was important in persuading emerging democracies such as India, Brazil, and South Africa to support a multi-stakeholder approach to internet governance, there is a danger that the Trump administration’s position will have an international ripple effect.

In 2017, states taking part in the UN-sponsored Group of Governmental Experts failed to reach an agreement on how international law applies to offensive cyber operations – particularly on states’ legal right to respond to cyber attacks. In any case, some of the states involved appear to have ignored the norms agreed on earlier in the process, including those on cyber attacks against critical infrastructure. In the absence of international agreement, groups of like-minded states can best advance the formation of norms by developing their own guidelines on applying international law in this area. EU member states should coordinate with allies and partners such as the United States, Australia, New Zealand, Canada, and Japan in developing standards that can guide state practice on issues such as the definition of an armed attack in cyberspace and the appropriate use of countermeasures.[61] Some of the most difficult strategic questions raised by offensive cyber operations concern actions that fall short of a conventional armed attack yet rise above the level of intelligence operations because they have an effect on political or commercial life. The challenges here include defining the threshold at which an action counts as an unlawful intervention, and finding a way to deter attacks that is both effective and compatible with the principles of democratic, law-abiding societies.

Conclusion: Putting the defence of liberal order at the heart of the European Global Strategy

The EU can best support the preservation of a rules-based system by promoting an adapted vision of international order that takes account of recent developments and new challenges. The EU should place an updated idea of liberal order at the centre of its Global Strategy, and build the capacity to implement this strategy.

In doing so, the EU should follow an approach that aims to reconcile some of the tensions between sovereignty and international order that have become problematic in recent years due to the rise of assertive illiberal powers, inconsistencies in Western practice, and a pervasive belief among Western electorates that globalisation is more a threat than an opportunity. A liberal order reinvented along the lines suggested above would offer greater recognition of the value of sovereignty by strengthening constraints on unlawful intervention; providing greater scope for Europe to reaffirm its standards through regulation and trade; and accepting voluntary commitments as a basis for some international agreements. The EU would offset this with a **renewed commitment to multilateralism** as the best way of securing Europeans’ security and prosperity; attempts to develop new norms for a more connected world; and support for the inclusion of businesses and civil society groups as participants in the order.[62]

In practical terms, this agenda gives rise to several priorities. Firstly, the EU needs to focus on its resilience as the keystone of a rules-based and liberal order. This involves major initiatives in several areas:

Security: Step up defence spending while pooling and sharing resources, to establish strategic autonomy at a time when the US commitment to European security is fading. European countries could strengthen their coordination within NATO by establishing a European caucus and outside the organisation by developing intra-European coordination, particularly through the nascent European Intervention Initiative.[63]

Economics: Invest in a new economic settlement at home to help those who feel left behind by globalisation, while developing tougher measures to stop China and other emerging players from creating an uneven playing field, including through investment screening.

Migration: Build up the EU’s ability to police its external border as a complement to managed pathways for legal migration.

Internet governance: Introduce regulation that creates a better balance between security, privacy rights, commercial opportunities, and the welfare of society as a whole.

Secondly, Europe needs to help compensate for the global diplomacy deficit by far more actively reaching out to other players, as well as pushing for a mediation role in crises and conflicts in the European neighbourhood:

Working in coordination with the European External Action Service (EEAS), member states should reach out to other great powers and swing states such as Brazil, India, and Indonesia on essential questions of order – and place the defence of the rules-based order at the heart of EU summits and meetings.

The EU should make better use of its financial engagement with many of the world’s most troubled states – including Syria, Iraq, Yemen, and Ukraine – to play a greater political role in support of stabilisation.

Thirdly, the EU should make greater use of its economic leverage to preserve the rules-based order. In this, it should:

Support the COP21 agreement by further promoting trade deals that incorporate environmental requirements, and by implementing a carbon border-adjustment tax at the EU’s borders.

Use the size of the EU market to define and export standards for better regulation of the internet.

Create the space to establish decision-making power on questions of order by pushing back against the extra-territoriality of US sanctions. In the short term, the EU should take steps such as establishing euro credit lines and special purpose vehicles to assist companies doing business with Iran, while pursuing measures to reduce the impact of US sanctions.[64] The EU should also set up an action task force that, bringing together all relevant parts of EU institutions, explores longer-term options for establishing greater financial independence from the US.

Fourthly, the EU should develop a series of sectoral strategies for preserving the rules-based order – in trade, arms proliferation, and environmental protection. These strategies should involve a set of complementary instruments, including trade, defence, diplomacy, development, financial, and regulatory tools. The EEAS should coordinate the use of the tools, but sub-groups of member states should create them. Such an approach would improve the links between EU institutions and member states in these strategies.

To implement this agenda, the EU will need to overhaul its ways of working. Internally, it will need to find a method for operating with the flexibility and speed required for greater diplomatic engagement, while keeping the collective weight of the EU behind its initiatives. Coordinating EU efforts with the United Kingdom after Brexit will also be important. Externally, the EU will need to make an especially large investment in its relations with like-minded powers. Conversely, it will need to develop a more independent posture towards the US. The EU should continue to cooperate with the US wherever possible, but it should put its commitment to the rules-based order above its traditional instinct to follow the American lead.

Some Europeans will worry that an independent and sometimes defiant attitude to the US will jeopardise the security relationship on which the EU continues to depend. But Trump has shown clearly that he does not reward concessions. Under his leadership, the United States’ security policy reflects its calculation of its own interests rather than any concern for repaying allies’ loyalty. The EU can best manage its relationship with the US and its support for a rules-based international system if it develops and acts on a sense of itself as an independent strategic actor. Europe needs to set its own course to secure the world order it wants.

## Solvency

### 2NC -- CP Solvency Block

#### CP sufficiently solves the case --- the EU stepping up in cyber policy increases global momentum to change norms and cyber doctrine – that’s Breton

#### It solves for China – a stronger Europe is able to counter China if collective defense is prioritized

Ables et al 20 [Christopher, PhD candidate at Hertie, Helmut K. Anheier is Professor of Sociology at the Hertie School, Iain Begg is a Professorial Research Fellow at the European Institute, London School of Economics and Political Science, and Featherstone, Kevin, Kevin Featherstone is Eleftherios Venizelos Professor in Contemporary Greek Studies and Professor in European Politics in the European Institute at LSE, 2-28-2020, “Enhancing Europe’s Global Power: A Scenario Exercise with Eight Proposals,” 2-28-2020, *Global Policy*, https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12792)

Europe is generally seen as ‘punching beneath its weight.’ Too often, it falls short of its own ambitions, takes third place behind the US and China in international affairs, and frequently lacks strategic ambitions. As a result, Europe risks falling behind these other global powers. To explore options on how to counteract this tendency, we developed a number of proposals for enhancing Europe’s soft and sharp power. While each measure can certainly stand on its own merits, combining them to create synergies will add to their overall effectiveness and impact: Internationalisation of the euro and Sanctions. Enhancing the euro’s role as a global reserve currency is an important building block for an effective sanctions repertoire. As the US is using the dollar’s global importance to strong‐arm countries into compliance, the EU could similarly use the euro to increase the bite of its sanctions. Triggering sanctions could involve the European data rating agency: if ratings for privacy are below a certain threshold, companies could be denied access to European markets or become subjects to fines. Erasmus Global, Smart Clusters, and Culture Europe. The alumni network of Erasmus Global can be employed in smart innovation clusters, thereby effectively serving as a recruiting tool which funnels talent into relevant projects and creates opportunities to keep foreign brain capital in Europe. Alumni activities could also be supported by Culture Europe by providing opportunities for exchange and local outreach. Digital Development Initiative, Smart Clustering. The DDI could build on the smart clustering proposal by creating digital hubs alongside a growing digital infrastructure, funded by InvestEU. This would also address criticism directed at the Juncker Plan’s lack of geographical diversity (European Court of Auditors, 2019), as the DDI intends to establish infrastructure across the EU. As the DDI aims to promote European standards beyond EU borders, the link could counteract China’s advances in digital authoritarianism (Shabaz, 2018). Irrespective of synergies that can be achieved by combining measures, there are several implications that have come up repeatedly and strongly in both the back‐casting exercise and the validations. If, by 2030, Europe wants to become a self‐confident and united market power, offering a democratic and socially inclusive alternative globally, with economic growth, open trade and a rule‐based, multilateral order, these implications offer crucial lessons. First, despite significant advances in European coordination and integration, Europe continues to be fragmented, and the sum of its parts (member states) appear less than the concord needed for enhancing its sharp and soft power, and indeed what is needed to implement the measures suggested here. This fragmentation applies both internally, but critically also to the way Europe is perceived by China and the United States, or indeed Russia. Fragmentation equals weakness, and reducing it in key policy fields should be a priority for the EU institutions, as well as the member states. A related weakness is the procrastination often visible in pursuing necessary reforms or in solving problems at home. Without internal cohesion, external power projection will struggle. At some point, soft and sharp power advances become ineffective without being backed up with sufficient hard power. With NATO weakening, and with new security threats in Europe’s neighbourhood and in cyber space arising, Europe needs to review fundamentally how hard and sharp power relate to each other. Europe needs to seek a better balance. Recent initiatives like PESCO are useful first steps, but more is needed to make the development of European hard power a pressing matter for debate and policy action across relevant EU institutions and all member states. What is more, Europe is simply not strategic enough. Geopolitically, especially compared to China, Europe seems less focused on specific parts of the world, lacking even a coherent approach to what the Americans think of as the immediate ‘back‐yard’, and timid in linking its strategic interests to economic interests and its values. In key policy fields, Europe is less clear about its role and less willing to act in its own interest than the US. However, the success of the GDPR and regulatory actions to curb the power of digital near‐monopolies like Facebook and Amazon have shown that Europe can act assertively, and that it will be quickly recognised globally as doing so. This paper has identified some of the key impediments to utilising the EU’s potential in its external relations. Such potential is realised when governments forgo their autonomy (and weakness) for collective gains. This will enable the EU to become more effective in meeting current public aspirations on key policy agendas – such as climate change, human rights; etc. – as signalled in the 2019 European elections, thereby overcoming the ‘capability‐expectations gap’ (Hill, 1993). It will also place the EU in a more proactive position in the face of current trends and future threats. It is an agenda for the EU’s own transformation as an external actor. Indeed, in terms of sharp power, we suggest that Europe needs to punch above its weight when necessary, and when called for strategically. This more ‘assertive Europe’ should be balanced by the ‘ethical Europe’ of its soft power. The measures proposed here offer ways and means of achieving this vision.

#### It solves cyber threats – the EU is an experienced player:

Ilves et al., Estonian Counselor at EU, ‘16

[Luukas K. Ilves, Counselor for Digital Affairs, Permanent Represnetation of Estonia to the EU, Timothy J. Evans, Senior Advisor, Cyber Strategy and Policy, Johns Hopkins University Applied Physics Laboratory, Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington Univesity, and Alec A. Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM v. 6 n. 2, 2016, p. 134]

Operational cooperation among European governments has improved, with EU structures playing a growing role. The EU’s best performance has been in the area of cyber crime, where cooperation among national cyber crime units and prosecutors has become frequent and close. The legal framework for cooperation on cyber crime is comparatively robust. The 2013 Directive on attacks against information systems includes a requirement for member states to respond to urgent requests within 8 hours. In 2013, EU member states also agreed to use an existing mutual evaluation mechanism to conduct thorough peer reviews of national cyber crime units.44 Europol, Eurojust (the EU’s agency for cooperation on prosecutions), and ENISA all have roles in cooperation with national authorities.

#### It solves in place of NATO – European unity creates cohesion around hybrid threats and attacks from Russia and China

### EU Only – 2NC – Permutation Block

#### Links to the net benefit – NATO still has to redirect its priorities towards cyber resilience – that’s Moller

#### U.S.-EU leadership trades off – the EU has to distance itself from the U.S. to achieve broader diplomatic control – that’s Dworkin

#### The permutation causes operational redundancy – decks any increased cybersecurity measures

Atlamazoglou and Moyer 22 (Constantine Atlamazoglou, European Security Analyst/Journalist; Jason C. Moyer, Program Associate, Global Europe Program, 6/1/22, A Strategic Compass: The European Union expands its toolbox, Wilson Center, https://www.wilsoncenter.org/article/strategic-compass-european-union-expands-its-toolbox)

Nevertheless, the EU needs to ensure that its mechanisms contribute effectively to transatlantic unity.

Perhaps the most striking stipulation of the Strategic Compass is the creation of a 5,000-strong force able to swiftly deploy to non-permissive environments. The force is to include air, land, and maritime components along with strategic enablers. It will be enabled through the substantial modification of the EU Battlegroups and the member-states that will participate with troops and capabilities will be pre-identified.

However, NATO currently has the NATO Response Force (NRF) which can start deploying globally within one to four weeks and a Very High Readiness Joint Task Force (VJTF) that can start deploying within two days. EU member-states that are also part of NATO are major contributors to the NRF and VJTF. Therefore, there is risk of **operational redundancy between the EU and NATO**’s components.

Additionally, due to the high number of initiatives put forth by the Strategic Compass the risk of some of them falling behind schedule or underdelivering is present. Nevertheless, besides the obstacles ahead, the importance of the document for the geopolitical future of the EU should not be underestimated.

### EU S: Cyber—General

#### U.S. strategic influence in technology sectors decks any shot at safe and open cyberspace – the EU is key.

Bradford 22 (Anu Bradford is a nonresident scholar in the Europe Program at the Carnegie Endowment for International Peace. Raluca Csernatoni is a visiting scholar at Carnegie Europe, where she works on European security and defense, 1-20-2022, *“How the Transatlantic Relationship Has Evolved, One Year Into the Biden Administration*”, Carnegie Europe, https://carnegieeurope.eu/2022/01/20/how-transatlantic-relationship-has-evolved-one-year-into-biden-administration-pub-86213)

After the friction-filled era under Trump, Europe has welcomed the new U.S. administration with optimism. Consistent with Biden’s lifelong commitment to transatlanticism, this past year has witnessed a shift in U.S. diplomatic rhetoric, from outright hostility toward a more normalized tone supporting enhanced EU-U.S. collaboration. This is also the case for the technological domain, with Washington demonstrating its eagerness to build coalitions with European allies and other techno-democracies to counter the rise of authoritarian China.

Most concretely, the Biden administration has been supportive of the EU-U.S. Trade and Technology Council (TTC), which had its inaugural meeting in September 2021 and serves as a forum for the EU and United States to coordinate their trade and technology policy approaches based on shared democratic values. The TTC offers a significant opportunity to make progress in aligning transatlantic interests in artificial intelligence regulation, technological standards setting, security of supply chains, screening foreign direct investments and exports, and increasing cybersecurity resilience.

The TTC was launched in the shadow of the transatlantic drama over AUKUS, so it is too early to tell whether it can successfully address present and future tech challenges and renew the transatlantic bond. The AUKUS incident shows that for all the talk of revived transatlanticism, the United States will act, as it always has, in its own strategic interests. AUKUS further confirms that China takes center stage in U.S. geopolitical calculations, with the EU risking to become an afterthought.

There are also long-standing tensions between Brussels and Washington regarding technology regulation. The United States has in the past accused the EU of targeting U.S. tech companies with its stringent antitrust and data protection rules. And it is now watching closely how the EU’s proposed Digital Markets Act and Digital Services Act will affect U.S. interests. Transatlantic data flows also remain precarious after the European Court of Justice has twice invalidated the agreement that governed EU-U.S. data transfers.

However, the U.S. policy conversation is now shifting closer to the EU, with an increasing recognition in the country that big tech has become too powerful. The Biden administration is looking to revive antitrust enforcement against certain companies, while Congress is debating more interventionist technology regulations targeting market competition, privacy, and content moderation. These policy developments suggest that the transatlantic gap may be gradually closing, even though it remains unclear whether this new rhetoric will translate into actual policy change in the United States.

Building on these developments, the EU should actively engage on its own terms with the United States and other democratic countries around shared values and norms regarding responsible technological innovation, the preservation of an open and safe cyberspace, and the development of human-centric disruptive technologies. Beyond leveraging regulation, the EU should also aim to operationalize its digital and technological sovereignty in critical areas and build its open strategic autonomy in the face of the growing tech rivalry between the United States and China. This also means the creation of a more cohesive EU external tech policy agenda to deal collectively with contested policy choices, such as whether to welcome the Chinese tech company Huawei to build 5G networks across Europe.

Yet the EU’s pursuit to boost its homegrown technological and digital capacity and to reduce dependencies on others, including the United States, might raise concerns about growing protectionism and further deepen the transatlantic rift. The EU may similarly be concerned that the United States has engaged in protectionist actions in support of its own high-tech industries, while publicly advocating the techno-globalism promoted by big tech. To avoid shifts to techno-nationalism, both the EU and United States should reject this emerging global norm and recommit to open markets. To mitigate and counter the negative effects of techno-nationalist policies, the EU should promote both new policy instruments for critical infrastructure protections in the case of key strategic technologies and at the same time boost the competitiveness of the European innovation ecosystem.

Neither the EU nor the United States can safeguard their democratic, economic, technological, and strategic interests alone. Instead, they need to seize the opportunity the TTC presents to deepen EU-U.S. ties and shape the global trade and technology policy toward their shared values. There is no better path for preserving the liberal democratic foundations of the global internet.

#### The EU needs internal change to shore up cyber-defenses – establishing formal cooperation mechanisms bolsters its influence

de Liedekerke 22 (Arthur de Liedekerke is a Project Manager at political advisory Rasmussen Global and a non-resident fellow at the Institute for Security Policy at Kiel University (ISPK), Germany, 3-30-2022, Russia’s Cyber War: What’s Next and What the European Union Should Do, Council on Foreign Relations, https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do)

What should the European Union do in the immediate term?

The EU has adopted new frameworks, including its much vaunted Strategic Compass, which, in the long term, will improve cybersecurity in the bloc, and potentially reduce the risk of catastrophic Russian cyberattacks. However, the EU needs to take more steps in the short term to shore up cyber defenses and mitigate the threat of Russian cyber operations.

First, **the EU should get its own house in order**. The revised Network and Information Security (NIS) Directive–better known in Brussels circles as NIS 2–should be finalized in the coming months and will aim to further strengthen the security of supply chains, streamline incident reporting obligations, and introduce more stringent supervisory measures for a large number of operators of essential services and enterprises across the EU. While NIS 2 represents a step in the right direction, the EU still has some way to go in implementing harmonized cybersecurity rules across the bloc’s own institutions.

Second, the EU and its Member States have a role to play in discouraging and deterring cyberattacks by demonstrating a willingness to act and impose costs on perpetrators. The first-ever operational deployment of the EU’s Cyber Rapid Response Team to Ukraine, alongside similar teams from the United States, was a welcome signal in this respect. One way to impose further costs would be by pushing for coordinated attribution of cyberattacks at the EU-level. On the offensive and deterrent side, the EU should adopt a pooling of capabilities on a voluntary basis. Similar programs already exist among other groups, such as NATO’s Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) program, which the EU could use as a model for its own programs.

Third, the EU should ensure it is better prepared by leveraging the tools it already has at its disposal. Intelligence sharing and situational awareness have proven vital before and during the war in Ukraine, but the future effectiveness of these strategies in deterring and mitigating cyberattacks will be reliant on Member States willingness to contribute with timely and actionable intelligence. In the short term, the Cyber Crisis Liaison Organisation Network (CyCLONe), a recently created group bringing together the executives of the EU’s twenty seven national cybersecurity authorities, should be used to its full capability and integrated with the rest of the EU cyber ecosystem. CyCLONe, with their wealth of operational-level expertise, should be able to brief political decision-makers in the Council more frequently. On the military side, the EU still lacks a fully fleshed-out cooperation mechanism for military cybersecurity alerts, despite this being an objective since the 2014 EU Cyber Defence Policy Framework. Ensuring cooperation among both civilian and military groups is vital given the specter of Russian cyberattacks.

#### EU can solve—already engages in effective cybercrime operational coop

Ilves et al., Estonian Counselor at EU, ‘16

[Luukas K. Ilves, Counselor for Digital Affairs, Permanent Represnetation of Estonia to the EU, Timothy J. Evans, Senior Advisor, Cyber Strategy and Policy, Johns Hopkins University Applied Physics Laboratory, Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington Univesity, and Alec A. Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM v. 6 n. 2, 2016, p. 134]

Operational cooperation among European governments has improved, with EU structures playing a growing role. The EU’s best performance has been in the area of cyber crime, where cooperation among national cyber crime units and prosecutors has become frequent and close. The legal framework for cooperation on cyber crime is comparatively robust. The 2013 Directive on attacks against information systems includes a requirement for member states to respond to urgent requests within 8 hours. In 2013, EU member states also agreed to use an existing mutual evaluation mechanism to conduct thorough peer reviews of national cyber crime units.44 Europol, Eurojust (the EU’s agency for cooperation on prosecutions), and ENISA all have roles in cooperation with national authorities.

### EU S: Cyber—Resilience

#### EU has demonstrated effectiveness in addressing resiliency concerns

Roepke & Thankey, NATO’s Defence Policy & Planning Division ‘19

[Wolf-Diether Roepke and Hasit Thankey, Resilience and Civil Preparedness staff, Defence Policy and Planning Division, NATO, “Resilience: The First Line of Defence,” NATO REVIEW, 2—27—19, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>, accessed 6-3-22]

National authorities have legislative and regulatory powers but little few direct controls to influence or steer supply in the private/commercial sector, other than in an emergency situation. As the system seems to work efficiently, there has been little incentive for national authorities to engage directly. Instead, it has been left mainly to industry to resolve any supply shortfalls. For government, the focus has been on ensuring safety and quality levels of goods and services, particularly of food and other consumables.

The European Union (EU) plays a very strong role in the public administration architecture for these sectors. EU directives and regulation have substantially shaped the planning by its member states, as well as by the commercial sector. Contingency planning, which seeks to ensure the functioning and maintenance of operations, has focused predominantly on the ability to deal with the most probable disruptive incidents in the short term. The commercial sector has mainly focused on minimising their own costs given such a disruption, rather than preparing for larger-scale contingencies with cascading effects across sectors and society itself.

# CP – EU/U.S. Cooperation

### 1NC – Shell

#### The United States federal government should increase its security cooperation with the European Union and its Member States by: encouraging Member States to incorporate resilience as a core concept; supporting cyber coordination; supporting expansion of industry partnerships to appropriate non-members; supporting foresight analysis; supporting the development of a cyber code of conduct.

#### Solves by harmonizing cyber policy and positioning the EU for more control

Selga 2021 (Ēriks Selga is a Non-Resident Fellow with the Digital Innovation Initiative and Transatlantic Leadership program at the Center for European Policy Analysis (CEPA), 8-27-2021, "Building Common Ground in Transatlantic Cybersecurity – A Baltic Approach," CEPA, https://cepa.org/building-common-ground-in-transatlantic-cybersecurity-a-baltic-approach/)

The diverging data governance approaches of the United States and the EU require a flexible approach to cybersecurity that can react quickly, and across policy levels, to best incorporate and exchange security practices, build trust, and ultimately bolster resilience across the transatlantic space. The Baltic approach offers a model that can help form a dynamic cross-sectoral threat information sharing feedback loop. In Latvia, for example, the Digital Transformation Guidelines establish an Information Society Council that meets with stakeholders from the private, public, military, and civilian sectors at the highest executive level to directly exchange digital threat information.35 As sectors become more dependent on data flows, the Information Society Council can dynamically react to changes in threats. The following recommendations draw on the Baltic experience to expand channels for the United States and the EU to find common ground for realignment across divergent data governance and cybersecurity regimes. These channels may be helpful in lessening divergences in practical cyber threat aversion, and may aid in normative alignment.

**I. Establish and Advance National Cybersecurity Councils for Critical Functions**

National cybersecurity councils are common across the Baltic states. Generally, these function as informal or formal councils that convene representatives of military and civilian, private and public sector participants from critical sectors, and increasingly — critical functions that underpin the aforementioned. These councils collect holistic information on the state of cybersecurity across sectors, and are the only funnel of such information. (In the United States, the equivalent is the U.S. Department of Homeland Security’s Critical Infrastructure Partnership Advisory Council (CIPAC), which has authorities from 16 critical infrastructure sectors.)36 The findings of these cross-sectoral councils are increasingly critical to the development of transatlantic cybersecurity. A similar council should be established at the international level, between the United States and the EU, dedicating a channel to negotiate the security regimes of shared transatlantic critical functions, like ensuring the smooth operation of international finance or even maintaining internet infrastructure.

**II. Advance Threat Information Sharing Channels Under the U.S.-EU Trade and Technology Council**

President Biden’s administration and EU leaders have both signaled commitments to renew the transatlantic partnership, especially in the digital arena, as highlighted by the recent formation of the U.S.-EU Trade and Technology Council.37 Of the 10 working groups within the council, four are working in the ambit of cybersecurity.38 These working groups should be used as a platform to advance cyber threat information sharing, providing a direct forum to channel the information from ENISA, NIST, and other national sectoral stakeholders. The aim of such a channel should be to triangulate the highest cybersecurity priorities, which should then branch off into more subsidiary cooperation channels with a feedback loop to higher, more senior executive levels.

**III. Conflate Civilian and Military Cybersecurity Experience via the EU’s Joint Cyber Unit**

U.S.-EU cybersecurity experience sharing is segmented between civilian and military sectors. However, the type of cyber threats both sectors share are increasingly similar and costly. The recent proposal to create an EU Joint Cyber Unit that will coordinate, share knowledge, and provide advanced warnings will draw together operational groups’ national cybersecurity authorities (CERTS), national defense authorities (military CERTs), and EU structures (ENISA and the Permanent Structured Cooperation; PESCO), among others.39 This Joint Cyber Unit can act as the mirror partner to the United States, which already has military and civilian sectors sharing risks via the Cyber Unified Coordination Group. The partnership between the United States and the EU in this capacity can take place via the U.S.-EU Trade and Technology Council, or a separate channel.

#### EU leadership and cooperation with the U.S. regulates dominant platforms and preserves digital markets.

Wheeler 22 (Tom Wheeler, Visiting Fellow at Brookings - Governance Studies, Center for Technology Innovation, 3-29-2022, "U.S. regulatory inaction opened the doors for the EU to step up on internet," Brookings, https://www.brookings.edu/blog/techtank/2022/03/29/u-s-regulatory-inaction-opened-the-doors-for-the-eu-to-step-up-on-internet/)

WANTED: A WESTERN DIGITAL ALLIANCE

The linear nature of the industrial economy has been replaced with an exponential economy based on the build-once nature of digital products coupled with the deliver-everywhere capability of the internet. If nation-specific, or region-specific rules were to disassemble that economic phenomenon, it would not only be a step back in time, but also a blow to the economies of the world, including the dominant digital platforms based in the United States. At the very time when the wisdom of the mid-20th century leaders to create Western alliances is being reinforced, the digital policy actions by the Europeans – both the EU and UK – create an opportunity for similar 21st century leadership. A few weeks after D-Day, while the Second World War was still raging, Western democracies came together to determine their collective economic future. At the foot of New Hampshire’s Mt. Washington, they established the Bretton Woods Agreement and set the rules for the commercial and financial relations of the post-war world. The United Nations Monetary and Financial Conference, the gathering’s official name, convened amidst transatlantic economic divisions not dissimilar to those of today. The United States’ stronger trade position—a position not unlike the strength of its digital economy today—encouraged the U.S. to prioritize free trade and fixed exchange rates. The other nations, with the UK in the lead, wanted policies to reflect their trade deficits and the need for rate flexibility. The result was a compromise of fixed-but-adjustable exchange rates. The conference also created two important international institutions, the International Monetary Fund (IMF) and what would become the World Bank. This is where the flood that started in Brussels will inundate Washington. Western democracies must seize the moment and form a similar alliance to oversee the commercial relations of the post-industrial world. That the United States has lost its leadership position through inaction will place it in an unusual position of not bringing the strongest hand to the bidding. Yet, for the dominant digital platforms domiciled in the U.S., the priority must be to protect the “build once, sell everywhere” economics of the internet. The dominant digital platforms lobbied the EU as actively as they have the U.S. Congress to avoid regulatory oversight. As a result of the EU’s decision, however, the fight has been redefined. The opposition to regulation must now transform from the protection of companies into the protection of the interconnected market.

In other words, that there will be rules has been established. What is important now is to make those rules work to protect consumers, competition, and the connected market. It is time for a Western Digital Alliance that harmonizes the rules that will govern the internet on both sides of the Atlantic. Such harmonization does not mean the policies must be identical, but that they are compatible. Herein lies the art of the possible for the U.S. government, American platform companies, and Western democracies. Just as the digital companies must be expected to consider the effects of their actions on the public interest, so must the actions of sovereign nations be expected to consider the effects of those actions on the interest of maintaining the exponential economics of the internet. To harm those economics in the name of sovereignty would be to harm the economics for all. Internet policy compatibility, as opposed to identicality, should underpin the new Western Digital Alliance. At the same time, taking another clue from the leaders who built the back half of the 20th century at Bretton Woods, perhaps the time has come for an ongoing as opposed to occasional transatlantic structure to keep pace with the rapid changes of connected digital technologies and how to protect both the public interest and a pervasive internet.

#### Digital authoritarianism causes global info-wars – extinction.

Manstead ’20 [Katherine; Non-Resident Fellow @ Alliance for Securing Democracy and Senior Adviser for Public Policy @ Australian National University’s National Security College; “Strong Yet Brittle: The Risks of Digital Authoritarianism”; https://securingdemocracy.gmfus.org/wp-content/uploads/2020/05/Strong-Yet-Brittle-The-Risks-of-Digital-Authoritarianism.pdf]

While digital authoritarianism can enhance regime durability and national power, it also introduces deep-seated vulnerabilities, eight of which are considered below. Significantly, digital authoritarians may find themselves in a state of constant contest with other regime types, trapped in cycles of overreach and backlash, and prone to strategic miscalculations that pull them into interstate conflict. The current turn to digital authoritarianism therefore also has broader implications for international peace and stability.

Brittle Legitimacy

Reliance on information control makes authoritarians brittle. Small chinks in their information control armor could have existential consequences, particularly during political or economic crises (i.e. when the regime needs to rely on control for legitimacy because it is not delivering for citizens). The information and ideas most dangerous to authoritarians include:

• the identity of opposition groups and leaders and their levels of support; 17

• technical means for subverting control of communications and surveillance technologies;18

• ideas about values that transcend state sovereignty, such as liberalism and human rights;19

• evidence that the central government is not delivering efficient outcomes;20 and

• ideas that undermine the myths and narratives used to legitimize authoritarian rule or the power of the ruling elite.21

Constant Contest

Since technologies and ideas are dynamic, the battle for information control is a constant struggle. It can never be ‘won.’ Authoritarians are therefore in a perpetual state of information warfare, inside and outside their regime, and feel perpetually insecure. This dynamic may lead authoritarian governments to assess that it is worth engaging in information or cyberattacks to discredit liberal ideas at their foreign source or to shape or disable systems that jeopardize their information control—despite real risks of conflict escalation and global pushback.

Overreach and Backlash

The fundamental importance of information control to authoritarians increases the likelihood of overreach, leading to cycles of backlash and reprisal. Many perceive China’s heavy-handed narrative warfare in Hong Kong and confrontational efforts to control narratives about coronavirus to be strategic missteps. For example, CCP efforts to stifle dissent by punishing online gaming company Blizzard and the National Basketball Association (NBA) arguably aided Hong Kong protester narratives;22 while CCP obfuscation about coronavirus has prompted unprecedented diplomatic rebukes from world leaders.23 Despite rising international awareness and condemnation of China’s sharp power tactics,24 China is accelerating, not muting, these behaviors.25 One explanation for this is that the CCP calculates that the risks of international backlash (and occasional overreach by its officials) are acceptable, compared with the risk of letting domestic information control falter.

Impaired Feedback Mechanisms

Authoritarians embrace technology to increase the legibility of their societies. But legibility requires cooperation from society. It is facilitated by an open information ecosystem, robust civil society, mechanisms of transparency, and protections for political speech.26 Conversely, information control and technology-enabled systems of surveillance and enforcement discourage accurate reporting and punish whistleblowing, while incentivizing officials to conceal failures and exaggerate successes.27 In 2007, Le Keqiang (before he became China’s premier) described China’s national income figures as “man-made” and unreliable, and noted that more objectively verifiable proxies should be preferred to official statistics collected by provinces.28 Without elections, authoritarians can also struggle to understand public sentiment, a problem highlighted by the Chinese government’s mismanagement of massive ongoing protests in Hong Kong. Party leaders wrongly assessed that the protestors’ grievances were primarily economic rather than political and that they did not enjoy broader public support.29 As Zeynep Tufekci has observed, the costs of China’s “authoritarian blindness” have been immense: a solvable issue (demands to withdraw a relatively unimportant extradition treaty) became “a bigger, durable crisis” with ongoing political consequences.30

China’s delayed reaction to coronavirus is a stark example of the authoritarian legibility and feedback problem. Local officials and hospital administrators in Wuhan suppressed information about the outbreak and punished doctor whistleblowers—depriving other provinces and the central government (not to mention international authorities) of vital signals that would have allowed swifter action to control the pandemic.31 Once authorities acknowledged the pandemic, China deployed the full weight of its digital surveillance capabilities. It was able to implement top-down lockdowns quickly; marshal its tech sector to build health apps; force citizens to download these apps; and access vast commercial holdings of personal data to cross-check compliance. However, it lacked critical bottom-up feedback systems that may have obviated the need for such draconian measures in the first place.32 Indeed, controlling for income and population size, authoritarian regimes appear to be more lethal than democracies during epidemics, arguably because of their closed information ecosystems.33

Overreliance on Technological Systems which ‘Fail Hard’

Many authoritarian governments are embracing AI-driven surveillance and control methods—from ‘smart cities’ to digital currencies, e-payment platforms and social apps. However, when AI systems fail, they tend to fail in unpredictable, often catastrophic ways. While citizens in democracies lament slow adoption of digital governance, authoritarians’ speed comes with the risk that authorities roll out unsafe or vulnerable systems.34 Imagine a critical failure of China’s social credit system—whether by accident or sabotage—which affected the integrity of records. The implications for regime stability could be significant.

AI systems do not need to fail to produce problematic results. They draw insights and make predictions based on correlations in vast datasets but are not good at identifying causal mechanisms. This means that AI systems often produce outcomes which humans cannot reverse engineer or routinely evaluate. Like using asbestos to build a city, AI governance systems might produce good results in the short-term, but inconsistencies or oversights in their approaches could lead to cascading failures that humans struggle to identify, let alone rectify.35

Unintended Consequences from High-Tech Modernism

Fixation by central governments on achieving targets or deploying certain technologies creates incentives for local officials to deploy “technology placebos” that do little to address underlying economic and social concerns. For example, many so-called smart city projects in authoritarian societies have failed to meet development and economic goals. They are fraught with issues such as “unclear strategic goals” (e.g. they often optimize for surveillance, not development) and “inadequate implementation.”36 This problem may be particularly pronounced for less-developed authoritarian governments which have been persuaded, for strategic reasons, to buy Chinese-exported digital surveillance tools that are not customized to local circumstances. These cities may also become locked into unstable or insecure technical architectures37 and economic dependence on China.38

Commitments to targets, and ideological fervor about technology, can also distort commercial decisions and raise unrealistic public expectations. Analysis of China’s AI industry, for example, suggests that companies are eschewing investment in basic research and focusing on quick wins in applied research.39 Additionally, China is already behind on meeting a number of its technology targets40—a lag that will likely be exacerbated by the global economic downturn following the coronavirus pandemic, and rising security fears in foreign markets about the security of Chinese technology and IP theft by its companies.

From a strategic perspective, there are risks that authoritarian governments’ fixation on technology-centric strategies will lead them to overestimate what technology can in fact achieve. For example, Chinese military strategists have posited that AI could lift the ‘fog’ of war and eliminate uncertainty and confusion on the battlefield. This is an ahistorical and unlikely prediction that could inspire miscalculation.41 Russian strategists theorize about how psychological operations might subdue adversaries without a shot being fired—an approach that may overestimate what cognitive warfare can achieve, at least without being combined with other elements of national power.42

Challenges to Social Cohesion

The medium- and long-term social consequences of digital authoritarianism are yet untested. Overreliance on surveillance and enforcement systems could attenuate relationships within a society, exacerbating authoritarians’ underlying low trust problems. Since they tend to reduce citizens to data inputs, these systems may deny citizens’ intrinsic desire for dignity and identity—with unexpected results.43 Information control tactics—such as flooding—can repress opposition, but long-term may exacerbate public uncertainty and decrease business confidence and trust in official information, with implications for social cohesion and economic progress.44

Dysfunctional Innovation Ecosystems

Information control and state-led pushes for technology dominance risk hampering innovation. For example, to achieve Xi Jinping’s ‘Made in China 2025’ goals, the CCP is supporting high-tech monopolies, restricting international collaboration, and yoking the state and market together.45 However, monopolies are notoriously inefficient and cross-border collaboration is an important driver of innovation. Further, innovation works best under free market conditions and in open societies.46 Some analysts argue that China’s success in deploying AI applications is an exception to this rule. However, there is a risk that Chinese companies are prioritizing shortterm breakthroughs (e.g. analyzing existing datasets to find new insights) at the expense of long-term investment in basic research.47 While authoritarians may excel at developing and deploying AI applications, conceptual research is arguably the real engine of AI advancement—and something that will continue to thrive in open societies.

Summary and Further Research

All states face risks in the information age, but the extent to which regime type affects the relative likelihood of these risks materializing, and their magnitude, is understudied. For example, much has been written about liberal democracies’ vulnerabilities to propaganda and foreign interference via social media.48 But while information warfare against open societies is more likely, arguably it is a higher magnitude threat for authoritarians, where control of information is core to regime survival. Similarly, analysts often lament that democratic governments have been slow to digitize governance systems and craft forward-looking technology policy.49 But while digital authoritarians might outcompete democracies in the roll-out of advanced technologies, this creates new vulnerabilities and risks. Inappropriate safeguards and accidents may result in cascading failures, while heavily digitized governance systems may be susceptible to foreign attack. Regime type may also affect the relative ability of authoritarians and democracies to mitigate their information age risks. For example, a democracy can build resilience to cyber and information threats through a variety of civil society and market-based interventions. Digital authoritarians must rely on a more limited set of top-down policy tools. Ultimately, a more systematic effort to map the comparative strengths and vulnerabilities of authoritarians and democracies in the information age could help both to better understand the other’s threat perceptions and manage escalation risks. It might also highlight ways in which democracies can hold digital authoritarians’ core interests at risk, in order to deter authoritarian interference in their own digital environments.

## Solvency

### 2NC – CP Solvency Block

#### CP sufficiently solves the case – coordination with the European Union revitalizes U.S.-EU cooperation across areas

#### Solves the China advantage – threat information sharing makes it easier and quicker to detect attacks – that’s Selga

#### Solves the cyber advantage – coordinating via the lens of the Joint Cyber Unit strengthens both U.S. and EU cyber posture and ability to respond to attacks

#### It solves in place of NATO – European unity creates cohesion around hybrid threats and attacks from Russia and China

### Solvency – Baltic Model

#### The U.S. and EU should adopt a Baltic-style information sharing system—will bolster resilience

Selga, Center for European Policy Analysis fellow, ‘21

[Eriks Selga, Non-Resident Fellow, Innovation Initiative and Transatlantic Leadership program, Center for European Policy Analysis (CEPA), “Building Common Ground in Transatlantic Cybersecurity – A Baltic Approach,” Center for European Policy Analysis, 8—28—21, <https://cepa.org/building-common-ground-in-transatlantic-cybersecurity-a-baltic-approach/>, accessed 6-9-22]

RECOMMENDATIONS

The diverging data governance approaches of the United States and the EU require a flexible approach to cybersecurity that can react quickly, and across policy levels, to best incorporate and exchange security practices, build trust, and ultimately bolster resilience across the transatlantic space. The Baltic approach offers a model that can help form a dynamic cross-sectoral threat information sharing feedback loop. In Latvia, for example, the Digital Transformation Guidelines establish an Information Society Council that meets with stakeholders from the private, public, military, and civilian sectors at the highest executive level to directly exchange digital threat information.35 As sectors become more dependent on data flows, the Information Society Council can dynamically react to changes in threats. The following recommendations draw on the Baltic experience to expand channels for the United States and the EU to find common ground for realignment across divergent data governance and cybersecurity regimes. These channels may be helpful in lessening divergences in practical cyber threat aversion, and may aid in normative alignment.

I. Establish and Advance National Cybersecurity Councils for Critical Functions

National cybersecurity councils are common across the Baltic states. Generally, these function as informal or formal councils that convene representatives of military and civilian, private and public sector participants from critical sectors, and increasingly — critical functions that underpin the aforementioned. These councils collect holistic information on the state of cybersecurity across sectors, and are the only funnel of such information. (In the United States, the equivalent is the U.S. Department of Homeland Security’s Critical Infrastructure Partnership Advisory Council (CIPAC), which has authorities from 16 critical infrastructure sectors.)36 The findings of these cross-sectoral councils are increasingly critical to the development of transatlantic cybersecurity. A similar council should be established at the international level, between the United States and the EU, dedicating a channel to negotiate the security regimes of shared transatlantic critical functions, like ensuring the smooth operation of international finance or even maintaining internet infrastructure.

II. Advance Threat Information Sharing Channels Under the U.S.-EU Trade and Technology Council

President Biden’s administration and EU leaders have both signaled commitments to renew the transatlantic partnership, especially in the digital arena, as highlighted by the recent formation of the U.S.-EU Trade and Technology Council.37 Of the 10 working groups within the council, four are working in the ambit of cybersecurity.38 These working groups should be used as a platform to advance cyber threat information sharing, providing a direct forum to channel the information from ENISA, NIST, and other national sectoral stakeholders. The aim of such a channel should be to triangulate the highest cybersecurity priorities, which should then branch off into more subsidiary cooperation channels with a feedback loop to higher, more senior executive levels.

III. Conflate Civilian and Military Cybersecurity Experience via the EU’s Joint Cyber Unit

U.S.-EU cybersecurity experience sharing is segmented between civilian and military sectors. However, the type of cyber threats both sectors share are increasingly similar and costly. The recent proposal to create an EU Joint Cyber Unit that will coordinate, share knowledge, and provide advanced warnings will draw together operational groups’ national cybersecurity authorities (CERTS), national defense authorities (military CERTs), and EU structures (ENISA and the Permanent Structured Cooperation; PESCO), among others.39 This Joint Cyber Unit can act as the mirror partner to the United States, which already has military and civilian sectors sharing risks via the Cyber Unified Coordination Group. The partnership between the United States and the EU in this capacity can take place via the U.S.-EU Trade and Technology Council, or a separate channel.

### Solvency – Cyber/Hybrid Threats

#### Strong European security policies and cooperation strengthen U.S. security

Borrell 19 (Josep Borrell, High Representative of the Union for Foreign Affairs and Security Policy, 1/12/2019, A stronger European Union within a better, greener and safer world - key principles that will be guiding my mandate, European Union External Action, https://www.eeas.europa.eu/eeas/stronger-european-union-within-better-greener-and-safer-world-key-principles-will-be-guiding-0\_en)

There can be no doubt that the US plays an essential role in the maintenance of peace and security, and also in European security. Indeed, in many places on our continent and at our borders, we need to work together to get sustainable results, from the Western Balkans, to the Eastern Mediterranean to Ukraine and beyond. As global partners, we will have to deepen our dialogue and cooperation in all areas, including on reviving the Iran nuclear deal and the broader area of non-proliferation and arms control. In addition, we will soon begin a dialogue to discuss the full range of issues related to China. We will also look at opportunities for cooperation across the globe where our interests coincide.

Many US administrations have insisted that Europe increases its defence efforts to take better care of its own security and act as a security provider. So it matters that we are already actively working to strengthen EU defence policies, capacities and operations. Our flagship defence initiatives now include the Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF) and military mobility. Indeed, a strong and capable Europe is not a rival to the trans-Atlantic alliance but a precondition for it.

Reinforcing defence capabilities of EU member states strengthen the Alliance and contribute to transatlantic burden-sharing. A more assertive, more capable and resilient Europe is the best partner for the US. Enhancing Europe’s security role will allow for a better cooperation with the US when it comes to the security risks of today and those of the future. It is clear that we have much to gain from close cooperation with the US to address pressing security challenges, from cyber security to hybrid threats, protecting our critical infrastructure and the security implications of climate change. We should certainly be ambitious in this area.

While we step up cooperation, we should be mindful that the experience of the last four year have left their toll on European public opinion. Indeed a clear majority of Europeans, as explained in a recent ECFR report, now believe that even under President Biden, the US will be mostly consumed with healing internal divisions and will have little capacity or will to help solve global problems. And there are underlying reasons—demographic, economic, and political—why the historical trajectory of the United States and Europe could well diverge. However, we appreciate that at least for the next four years there will be a US President who believes in partnership with democratic allies. And we don’t just feel appreciation for this restoration, but we recognize its necessity.

### Solvency – Misinformation

#### EU-U.S. cooperation can help combat misinformation

Clüver Ashbrook & Sanger, Harvard Kennedy School researchers, ‘20

[Cathryn Clüver Ashbrook, Director, Project on Europe and the Transatlantic Relationship and the Future of Diplomacy Project, Harvard Kennedy School and David Sanger, Adjucnt Lecturer, Public Policy, Harvard Kennedy School, “Technology,” STRONGER TOGETHER: A STRATEGY TO REVITALIZE TRANSATLANTIC POWER, Harvard Kennedy School & German Council on Foreign Relations, 12—20, p. 77-78]

Formalize transatlantic operational coordination to counter disinformation and election interference

Countering the spread of mass disinformation (including deep fakes, cheapfakes and other next-generation disinformation technology), particularly from China and Russia, must be at the core of the joint transatlantic project to defend the integrity of democracies. Europe and the United States were equally the target of strategically launched disinformation campaigns by Russia and China at the height of the spring COVID outbreak.

As part of the Tech Forum’s work, the U.S. State Department’s Global Engagement Center and the EEAS detection and early-warning systems must be closely aligned. The 2018 G-7 summit Charlevoix agreed to build transatlantic data competence to identify dual-use tech and tech-powered human rights violations so that powerful nations can coordinate sanctions design. Transatlantic nations need to expedite the implementation of this decision.

Both sides have a vested interest in protecting election infrastructure from technological interference by malign actors. This includes a tighter control on election advertising, bots, deep fakes, inauthentic behavior, and hate speech. But there must also be a recognition that these efforts cannot be used to give governments greater power to restrict real political speech— including unpopular opinions.

The December 2020 European Democracy Action Plan (EDAP) signals the EU could be willing to make a joint effort with U.S. agencies and lawmakers to focus on the twin challenges of increasing transparency and accountability of platforms. A joint EU–U.S. ‘code of conduct’ on removal of hate speech, illegal and illiberal and blatantly harmful content could create a ‘race to the top’ when coupled with a credible threat of regulatory action—all while safeguarding provisions of transparency and free speech. A transatlantic audit mechanism of ‘black box’ algorithms could also force changes in business models. Joint EU–U.S. standards around identifying and marking disinformation could give platforms greater credibility and accountability.

The Tech Forum could also work to correct the information asymmetry on technology that exists among EU, member state and American lawmakers devising platform regulation. And it could coordinate joint research funding by American and European foundations and academic institutions into the impact of disinformation on society and democratic integrity to better anticipate, educate and counter its spread.

### 2NC – Permutation Block

#### Links to the net benefit – any inclusion of NATO forces redirection of its priorities and reallocation of its resources – that’s Moller

#### The permutation causes operational redundancy – decks any increased cybersecurity measures

Atlamazoglou and Moyer 22 (Constantine Atlamazoglou, European Security Analyst/Journalist; Jason C. Moyer, Program Associate, Global Europe Program, 6/1/22, A Strategic Compass: The European Union expands its toolbox, Wilson Center, https://www.wilsoncenter.org/article/strategic-compass-european-union-expands-its-toolbox)

Nevertheless, the EU needs to ensure that its mechanisms contribute effectively to transatlantic unity.

Perhaps the most striking stipulation of the Strategic Compass is the creation of a 5,000-strong force able to swiftly deploy to non-permissive environments. The force is to include air, land, and maritime components along with strategic enablers. It will be enabled through the substantial modification of the EU Battlegroups and the member-states that will participate with troops and capabilities will be pre-identified.

However, NATO currently has the NATO Response Force (NRF) which can start deploying globally within one to four weeks and a Very High Readiness Joint Task Force (VJTF) that can start deploying within two days. EU member-states that are also part of NATO are major contributors to the NRF and VJTF. Therefore, there is risk of **operational redundancy between the EU and NATO**’s components.

Additionally, due to the high number of initiatives put forth by the Strategic Compass the risk of some of them falling behind schedule or underdelivering is present. Nevertheless, besides the obstacles ahead, the importance of the document for the geopolitical future of the EU should not be underestimated.

#### No solvency -- the EU Treaty has broader scopes of protection and collective cyber-defense – NATO acting would trade off.

Zandee et al. 2021 (Dick Zandee, Senior Research Fellow and Head of the Security Unit of the Research department of the Clingendael Institute, Adája Stoetman is a Research Fellow at the Security Unit, and Bob Deen is at the Clingendael Institute as Senior Research Fellow and team leader on Security and Defence, The EU’s Strategic Compass for security and defence, Clingendael Institute, https://www.jstor.org/stable/resrep32154.9)

The EU Treaty acknowledges that the Alliance is the main forum for the collective defence of its members as defined in Article 5 of the NATO Treaty. However, there has been considerable debate on how this affects the EU, considering that the EU has its own mutual defence clause: Article 42.7 TEU (see chapter 3). Despite the degree of ambiguity surrounding Article 42.7, EU member states agree that the Alliance should remain the principal organisation for safeguarding collective defence.89 Not only is there a widely held view that the EU lacks the necessary means and capabilities to autonomously defend its territory, but a majority also believe that deterrence and collective defence are only credible because of the pivotal role of the US.90 87 The concrete proposals can be found here: proposals dating from December 2016 & proposals dating from December 2017.

However, Article 42.7 TEU has already been invoked in response to a terrorist attack in the past and could also be called upon in the nearby future, for example when an EU member state is under attack, which is in particular relevant for the cyber domain. This applies specifically to non-NATO EU member states such as Finland and Sweden. Even though these countries work closely with NATO, Article 5 would not apply if they were to be attacked. Thus, it is important to clarify what the EU’s responsibilities could be. As stated in chapter 3, when cyberattacks hit non-military infrastructure and other targets, it seems preferable that the EU acts instead of NATO in case international assistance is needed. In other words, what is already the case for activating Article 42.7 TEU when an EU member state is under a terrorist attack should equally apply to cyberattacks targeted at the civilian infrastructure. In order to clarify what sort of cyberattacks would fall under the Article 42.7 TEU or under NATO’s Article 5 clause, both organisations should discus scenario-planning and attend each other’s relevant exercises. Furthermore, the case of an armed attack against an EU member state can raise questions for which the answer is not to refer to NATO’s collective defence task because the EU member state under an armed attack is not a NATO Ally or the Alliance is not capable of responding collectively. What will happen if an EU member state invokes Article 42.7 in such cases? In sum, while the principle holds that NATO is the primary organisation responsible for collective defence, as part of the Strategic Compass process the EU should not overlook the importance of operationalising and clarifying the applicability of Article 42.7 TEU.

### 2NC – Solvency

#### The stage is set for expanded cooperation – cyber doctrine is key

Muncaster 22 (Phil Muncaster -- UK / EMEA News Reporter, Infosecurity Magazine, 5-17-2022, "US and EU Move Closer on Cyber in New Trade Pact," Infosecurity Magazine, https://www.infosecurity-magazine.com/news/us-eu-move-closer-cyber-new-trade/)

Representatives from the European Union (EU) and US government have jointly announced a range of new initiatives in areas such as SMB and supply chain security, tackling disinformation, sanctions evasion and the development of trustworthy AI and privacy-enhancing technologies. The outcomes were announced after a second ministerial meeting of the US-EU Trade and Technology Council (TTC) in Paris on May 15-16. Many of the announcements were given extra urgency by current Russian aggression in Ukraine. On that note, there’s a new Cooperation Framework on issues related to information integrity in crises, particularly concerning the Kremlin’s attempt to “manipulate and censor” information. There will also be closer information exchange between the two parties on critical tech exports, with an initial focus on Russia and other sanctions-evading countries. On a more positive note, the TTC agreed to produce a cybersecurity best practice guide for SMBs, which it said were “disproportionately” impacted by cyber-threats. There were also commitments to “promote secure, resilient, diverse, competitive, transparent, and sustainable digital, telecommunications, and ICTS infrastructure supply chains.” Regarding emerging technologies, the EU and US agreed to develop a joint roadmap to evaluate tools for “trustworthy AI and risk management,” alongside a project on privacy-enhancing technologies. Perhaps with one eye on China’s increasing presence in the international standards community, the TTC also announced the creation of a “US-EU Strategic Standardization Information (SSI) mechanism” to facilitate information sharing on international standards development. John Dickson, VP at advisory firm Coalfire, described the agreement as significant. “Supply chain disruption from Russian and Ukrainian suppliers most certainly affects European manufacturers compared to their US counterparts,” he added. “This reality will also drive deeper cooperation with the European Union on a variety of fronts, including cybersecurity. If there are any Russian attempts by to expand the conflict outside Ukraine in the cybersecurity realm, closer cooperation on that front will be an imperative.”

### 2NC - Avoids the DA

#### Cooperation with the U.S. avoids mechanisms for circumvention embedded in NATO

Zandee et al. 21 (Dick Zandee is Head of the Security Unit and Senior Research Fellow at the Clingendael Institute. Sico van der Meer is a Research Fellow at the Clingendael Institute. Adája Stoetman is Junior Researcher at the Security Unit of the Clingendael Institute, October 2021, Countering hybrid threats: Steps for improving EU-NATO cooperation, https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/#international-cooperation-outside-the-eu-nato-framework)

EU-US

Besides cooperation within a variety of European formats, one could think of increasing cooperation between the EU and the US. At the latest EU-US Summit on 15 June 2021, the topic of security and defence was explicitly added to the agenda. Therefore, this offers a second possibility for transatlantic cooperation outside the EU-NATO framework in the field of countering hybrid threats. **By cooperating with the US directly,** some of the political obstacles in the NATO context may be circumvented (especially political tensions around Turkey, Greece and Cyprus). Therefore, it could be worthwhile to start some more relatively small test projects in this specific cooperation framework.

More concretely, one could think of the development of a ’strong collaborative relationship’ between the EU and the US in the digital and information domain. This would contribute to **countering hybrid threats** stemming from China and Russia. If this partnership is explicitly embedded in policies on both sides of the Atlantic, this will help to form a unified stance towards adversaries such as China and Russia.﻿[101] Despite the potential advantages that this may bring, one should also take into consideration the downsides that this format might bring about. Existing initiatives for direct EU-US (military) cooperation show that political and bureaucratic obstacles may still exist. A good example is the recent EU-US cooperation on military mobility, which is being hindered by bureaucratic red tape after the initial decision was taken to allow the three non-EU states to join the related PRSCO project.﻿[102] Moreover, care should be taken not to alienate the few NATO countries that are not EU members and might feel left out by increasing EU-US (military) cooperation.

#### The U.S. needs to be on board with EU security policies – NATO has too much on its plate

López-Aranda 22 (Ambassador Ricardo López-Aranda, Resident Distinguished Fellow at the German Marshall Fund, 6-13-2022, "A Renewed Sense of Purpose: Europe and the Transatlantic Relationship on the 75th Anniversary of the Marshall Plan," GMFUS, https://www.gmfus.org/news/renewed-sense-purpose-europe-and-transatlantic-relationship-75th-anniversary-marshall-plan)

Another traditionally vexing issue is the respective role of NATO and the EU in European security. The EU can and, as the new Strategic Compass reflects, is willing to do more in crisis management and the development of military capabilities, thus helping to lighten the US security burden in Europe and the neighboring area. **But if the US signals reluctance to this, as has been the case in the past, this will generate resistance in some EU member states**. More burden sharing requires the United States to be supportive of European efforts in developing its security dimension. As High Representative Borrell has stated, to increase the military capabilities of the European Union is a way of increasing and reinforcing the global security, the transatlantic link in complementarity with NATO.

That said, there is no denying that the Trump administration has left a sense of concern in Europe about the solidity of the US commitment to European security. The development of strategic autonomy within the EU is a reflection of this concern. But the Ukraine crisis has shown how efficiently the transatlantic relation can work when addressing together a common challenge. On both sides of the Atlantic, this common purpose means a renewal of mutual trust and hence of the solidity of the alliance.

Ultimately, the Russian aggression against Ukraine also profoundly affects the debate on NATO’s role, as it brings to the fore its traditional character as an instrument of collective security in the European area. Europe and the United States will no doubt continue working together in facing international challenges, including the consequences for the international order of China’s growing assertiveness. But arguably NATO will have to concentrate on its core task of dealing with the challenges coming from Europe’s eastern and southern neighborhoods.

The Madrid NATO summit, which will take place June 29-30, will be an historic moment. The Madrid Strategic Concept will have to outline an agenda to make our military better prepared for the challenges coming from the East and from the South, as well as establish processes to make our societies to be more resilient against cyberattacks and disinformation. For Spain, it will be an occasion to celebrate the 40th anniversary of its accession to NATO, a reminder that freedom and democracy that cannot be taken for granted.

# Permutation

### DA: Article V

#### The EU Treaty has broader scopes of protection and collective cyber-defense – NATO acting would trade off.

Zandee et al. 2021 (Dick Zandee, Senior Research Fellow and Head of the Security Unit of the Research department of the Clingendael Institute, Adája Stoetman is a Research Fellow at the Security Unit, and Bob Deen is at the Clingendael Institute as Senior Research Fellow and team leader on Security and Defence, The EU’s Strategic Compass for security and defence, Clingendael Institute, https://www.jstor.org/stable/resrep32154.9)

The EU Treaty acknowledges that the Alliance is the main forum for the collective defence of its members as defined in Article 5 of the NATO Treaty. However, there has been considerable debate on how this affects the EU, considering that the EU has its own mutual defence clause: Article 42.7 TEU (see chapter 3). Despite the degree of ambiguity surrounding Article 42.7, EU member states agree that the Alliance should remain the principal organisation for safeguarding collective defence.89 Not only is there a widely held view that the EU lacks the necessary means and capabilities to autonomously defend its territory, but a majority also believe that deterrence and collective defence are only credible because of the pivotal role of the US.90 87 The concrete proposals can be found here: proposals dating from December 2016 & proposals dating from December 2017.

However, Article 42.7 TEU has already been invoked in response to a terrorist attack in the past and could also be called upon in the nearby future, for example when an EU member state is under attack, which is in particular relevant for the cyber domain. This applies specifically to non-NATO EU member states such as Finland and Sweden. Even though these countries work closely with NATO, Article 5 would not apply if they were to be attacked. Thus, it is important to clarify what the EU’s responsibilities could be. As stated in chapter 3, when cyberattacks hit non-military infrastructure and other targets, it seems preferable that the EU acts instead of NATO in case international assistance is needed. In other words, what is already the case for activating Article 42.7 TEU when an EU member state is under a terrorist attack should equally apply to cyberattacks targeted at the civilian infrastructure. In order to clarify what sort of cyberattacks would fall under the Article 42.7 TEU or under NATO’s Article 5 clause, both organisations should discus scenario-planning and attend each other’s relevant exercises. Furthermore, the case of an armed attack against an EU member state can raise questions for which the answer is not to refer to NATO’s collective defence task because the EU member state under an armed attack is not a NATO Ally or the Alliance is not capable of responding collectively. What will happen if an EU member state invokes Article 42.7 in such cases? In sum, while the principle holds that NATO is the primary organisation responsible for collective defence, as part of the Strategic Compass process the EU should not overlook the importance of operationalising and clarifying the applicability of Article 42.7 TEU.

### DA: European Security

#### Reliance on NATO precludes development of united European collective defense measures

He 19 (Wendy, Research Analyst with the Military Studies Programme, RSIS, 11-21-19, “‘NATO is Brain-Dead’: Time For EU Military Force?,” *RSIS Commentary,* <https://www.rsis.edu.sg/rsis-publication/rsis/nato-is-brain-dead-time-for-eu-military-force>, accessed 8-6-2020)

In an interview with The Economist on 21 October 2019, French President Emmanuel Macron painted a distinctively bleak picture of the state of security affairs in Europe. Candidly, he urged for a rethinking of the North Atlantic Treaty Organisation (NATO) and its traditional role as a long-standing cornerstone of Europe’s defence, going so far as to assert that Europe is experiencing the “brain death of NATO”. He warned that if Europe continues to meander along, choosing to ignore the reality of an increasingly unreliable American partner in fulfilling NATO’s commitment to the freedom and security of its members, it would cease to be in control of its own destiny. Underpinning this “apocalyptic vision” is a familiar rhetoric he has used before. Europe needs to have a military force of its own and start thinking of itself as a strategic power. Is he right? An independent European Union (EU) military force that would protect Europeans is familiar rhetoric and the idea that EU might eventually deviate from NATO has been discussed long before Macron’s appearance. For the first time, the EU signalled in its 2016 EU Global Strategy a qualitative shift in its strategic outlook; it put forth the idea of attaining “a certain level of strategic autonomy” and being able to “act independently if and when it is needed”. This rhetoric picked up steam when German Chancellor Angela Merkel endorsed Macron’s call for the creation of a EU army in November 2018, reiterating the stand that Europe needs to be able to defend itself. At the same time, EU President Donald Tusk alluded to a new era in which American and European relations are at an inflection point due to differences in worldviews and actions. Tusk echoed the rhetoric of having a European army in the face of an American administration (under President Donald Trump) that seems intent on breaking down the post-World War II order. Increased calls for the creation of an independent EU military force have been recurring and the potential onset of an uncertain multi-polar world has pushed this familiar rhetoric further. This is not to say that there have been no attempts at enhancing EU’s military capabilities and defence structure. The EU has taken steps to bolster its military capabilities through the establishment of the Permanent Structured Cooperation (PESCO) and battle groups. Such initiatives provide platforms for EU member states to work together in planning, investing and developing projects that heighten the functional integration of the military forces. However, the voluntary nature of such projects means that the member states can remain elusive about defence collaboration. Moreover, by leaving participation in PESCO to the willingness of member states, there is little alignment and agreement on how member states are going to contribute to these projects. Similarly, the creation of the battle groups in 2004, with an aim to compensate for EU’s lack in permanent military forces, was promising in its inception, but has not been deployed since it became operational in 2007. The lack of political resolve by the EU in these attempts at strengthening the EU’s military capabilities provides a glimpse of the challenges Macron will face if he tries to push for the development of a permanent, independent and unified EU military force. Underlying these half-hearted attempts at enhancing the military capabilities of EU is the member states’ reliance on NATO. The 2002 NATO-EU Declaration on a European Security and Defence Policy (ESDP) and the subsequent 2003 “Berlin Plus” essentially cemented EU reliance on NATO. This dependence can be seen from the current presence of 4,500 US troops stationed in Poland and the added confirmation that more troops will be sent to the region. Departure from NATO would mean being cut off from access to NATO’s military planning capabilities and resources − essential support that the EU has grown accustomed to and would need much time to build up on its own. Will Macron’s assertive choice of words take root this time? Europe finds itself facing an increasingly uncertain geopolitical climate. Recent developments such as America’s troop withdrawal from Syria, which effectively led to a hasty invasion into Kurdish territory in north-eastern Syria by Turkey (another NATO-member), undoubtedly contributed to Macron’s bold criticism of NATO. Earlier episodes of Russian aggression in Ukraine, Georgia and Moldova likewise spurred the Chairman of the Munich Security Conference, Wolfgang Ischinger to affirm that “the creation of a European army is inevitable”. However, such push for an independent European collective defence demands a level of unity and commitment that the EU currently does not seem capable of. As a whole, the EU is still embroiled in tackling Brexit while contending with the rise of populism and the ongoing migration crisis. The chances that EU member states would rally around brash rhetoric and pull attention away from their respective domestic issues are slim. As such, Macron’s warning words may end up being symbolic rhetoric at best, noted for its audacity, but soon to be relinquished to the back of people’s mind until such “familiar rhetoric” starts up again.

### DA: Redundancy

#### The permutation causes operational redundancy – decks any increased cybersecurity measures

Atlamazoglou and Moyer 22 (Constantine Atlamazoglou, European Security Analyst/Journalist; Jason C. Moyer, Program Associate, Global Europe Program, 6/1/22, A Strategic Compass: The European Union expands its toolbox, Wilson Center, https://www.wilsoncenter.org/article/strategic-compass-european-union-expands-its-toolbox)

Nevertheless, the EU needs to ensure that its mechanisms contribute effectively to transatlantic unity.

Perhaps the most striking stipulation of the Strategic Compass is the creation of a 5,000-strong force able to swiftly deploy to non-permissive environments. The force is to include air, land, and maritime components along with strategic enablers. It will be enabled through the substantial modification of the EU Battlegroups and the member-states that will participate with troops and capabilities will be pre-identified.

However, NATO currently has the NATO Response Force (NRF) which can start deploying globally within one to four weeks and a Very High Readiness Joint Task Force (VJTF) that can start deploying within two days. EU member-states that are also part of NATO are major contributors to the NRF and VJTF. Therefore, there is risk of **operational redundancy between the EU and NATO**’s components.

Additionally, due to the high number of initiatives put forth by the Strategic Compass the risk of some of them falling behind schedule or underdelivering is present. Nevertheless, besides the obstacles ahead, the importance of the document for the geopolitical future of the EU should not be underestimated.

### A2 Perm: NATO-EU Disputes

#### NATO-EU cooperation is formally blocked by Turkey – cooperation that does happen is stalled by this dispute

Smith 19 (Simon J. Smith, Associate Professor of Security and International Relations at Staffordshire University, 12-3-19, A short history of the EU and NATO’s uneasy relationship, Quartz, https://qz.com/1759575/a-short-history-of-the-eu-and-natos-uneasy-relationship/)

The American NATO expert David Yost set out the problems at the heart of the EU-NATO relationship in a 2007 book. As he put it: “Difficulties include institutional and national rivalries, the participation problem, and disagreements about the proper scope and purpose of NATO-EU cooperation.”

The “participation problem” is a central impediment to formal EU-NATO relations that stems from the ongoing dispute between Turkey (a NATO-only member) and Cyprus (an EU-only member). This **led to Turkey directly blocking formal EU-NATO cooperation in 2004** beyond that of Operation ALTHEA. Formal meetings between the PSC and NAC were suspended as Turkey objected, and still does, to Cyprus sitting in on such meetings without a NATO security agreement—which Turkey refuses to allow.

Informal meetings do take place but these have been described to me by both PSC and NAC ambassadors during my research as “dull,” “highly scripted,” and “uninspiring”. As a result, there has been a move towards enhancing cooperation at the inter-organizational level to compensate for deficiencies at the formal political level.

# Internal Net Benefit

### L: NATO Bad EU Good

#### NATO decks any chance at European peace because of divisive U.S. military strength – EU military buildup is key

Merritt 22 (Giles Merritt is the Founder and Secretary General of Friends of Europe, the Brussels-based think-tank that focuses on high-level EU policy proposals, 5-24-2022, "Europe mustn't put all its eggs in the NATO security basket," Friends of Europe, https://www.friendsofeurope.org/insights/europe-mustnt-put-all-its-eggs-in-the-nato-security-basket/)

The eyes of the West are on NATO and its swift response to Russia’s invasion of Ukraine. But we should also focus our thinking on the European Union, **for only the EU and not the US-led military alliance can be the basis of a peaceful long-term outcome to this crisis.**

So far, the EU’s political input has centred on sanctions to dissuade Russia from continuing its war against Ukraine. Henceforth, though, it must play a wider role. That was the message France’s President Emmanuel Macron strove to impart when he proposed a wider European political framework open to non-EU members such as Ukraine and the United Kingdom.

NATO’s importance is indisputable. Although its ill-considered enlargement may very well have contributed to the crisis by feeding Russia’s ‘encirclement’ paranoia, the alliance now stands as the only credible deterrent of further incursions. **However, US military strength can never be key to a lasting peace settlement in Europe**.

The US must back an eventual ceasefire leading to peace discussions between Kyiv and Moscow. But the greater burden of establishing a new European order capable of reassuring Russians while punishing Putin will fall on the EU’s shoulders. Washington’s financial and material support is crucial to Ukraine’s gallant counter-attacks, but it also rules out US leadership in whatever post-war reconciliation and re-balancing process may emerge.

The US not only leads NATO but dominates it, so the alliance’s future is potentially clouded by America’s domestic politics. When Moscow launched its blitzkrieg attack on Kyiv, worldwide condemnation was tinged with relief that Donald Trump is no longer in the White House. Now his strengthening grip on the Republican Party is ringing alarm bells warning of a possible return. Much of the damage he did to the transatlantic alliance has been repaired, yet that doesn’t quell fears of how NATO would fare in a second Trump presidency.

The crux of the problem is the military inadequacy of all the EU’s member states. The eastern deployment of European troops has been getting much play in media reporting of the Ukraine crisis, but the reality is far less reassuring. The legacy of three decades of free-riding and reliance on the US is Europe’s lack of firepower, limited cooperation between national armed forces and the proliferation of incompatible weapons systems.

The EU has for years been trying to boost member governments’ defence spending, but with little success. The European national average is 1.6 per cent of GDP, far short of the 2 per cent targets of both NATO and the Union. Most governments still ignore the requirements of PESCO, the EU’s permanent structured cooperation pact of 2018.

When in 2020 Brussels published a long-awaited Defence Review, it observed that only 60 per cent of the troops notionally available for Europe’s protection can be activated operationally. This year, that concern has become a fact; less than a third of the forces hurriedly deployed to strengthen NATO’s eastern frontiers are European. American units flown in from the US make up the majority.

Despite these manifest weaknesses, Charles Michel, President of the European Council which groups EU leaders, declared last December that 2022 was to be “the year of European defence.” Security policy veterans recalled the embarrassment of 1999 when Luxembourg’s foreign minister Jacques Poos boasted that attempts to avert war in the Balkans were “the hour of Europe, not America.”

The recent flurry of national boosts to defence spending is encouraging, but it’s no more than the first step down a long road. Germany’s €100 billion plan to reinvigorate its armed forces, for instance, will probably take about 15 years to bear fruit. Recruitment and rearmament are not the only priorities, because the EU’s most daunting challenge is to parallel NATO’s ‘command and control’ structures.

The EU has been trying for almost 20 years to develop its own defence identity, but in the area of security it still lacks the Atlantic alliance’s diplomatic and operational mechanisms. Without them, Europe will remain unable to project force to any substantial degree.

Thanks to Putin’s war, the EU must brace to take on the leadership of a far-reaching post-war project to reorder and rebuild relationships across Europe. Once Washington’s focus returns to East Asia, Brussels must have developed a much fiercer bite to reinforce its bark.

### L: US Focus

#### EU strategic autonomy benefits NATO and frees up US resources

**Keil,** Senior Fellow, Security and Defense Policy GMF**, 2022**

[Steven, German Marshall Fund - non-partisan policy organization studying transatlantic interests “NATO Core Tasks in a Contested Global Landscape” German Marshall Fund February 11, 2022 [https://www.gmfus.org/news/nato-core-tasks-contested-global-landscape GDI-TM 6.16.2022](https://www.gmfus.org/news/nato-core-tasks-contested-global-landscape%20GDI-TM%206.16.2022)]

Beyond the need for added capability, at a strategic level, it is also critical to understand what kind of actor Europe sees itself as in this new geopolitical era. Conversations around strategic autonomy have often been fraught for this very reason. At times, certain expressions or interpretations of the concept have created fears in the United States of geopolitical hedging or strategic ambivalence. But rather than lamenting a worst-case scenario, it is more useful for both sides of the Atlantic to jointly seize the current moment in a constructive way. Traditional US fears should be put aside and replaced with a proactive agenda that encourages a clearer European pillar in the alliance, that, for European purposes, could also be used more ad hoc in non-NATO contingencies. This should be done through new planning and thinking around burden-sharing metrics, including a more holistic reevaluation, reinvestment, and planning of Europe-wide contributions to the alliance. Ultimately, such efforts should fill gaps in European crisis-management capabilities and contribute to European defense within the NATO context. Such an approach “could also lead to a new division of labor within the alliance. That need not divide the alliance. It would just create greater clarity as to who would lead certain missions and what they need to do to succeed.”

The EU Council concluded in November 2016 that strategic autonomy is the “capacity to act autonomously when and where necessary and with partners wherever possible.” In this sense, an EU-based strategic autonomy, as argued above, that aligns and coordinates with NATO’s defense planning and could operate formally within or informally below the consensus NATO or EU level would certainly be welcomed, particularly at a time when the United States will likely be increasingly preoccupied elsewhere. Europe’s ability to respond robustly in resolving regional crises, while complementing—and, if possible, supplanting—certain collective defense efforts traditionally borne by the United States would be a hugely welcome development for US policymakers and put NATO on a more sustainable footing.

### NB: Soft Power

#### EU modelling is key to its soft power

Bradford 20, the Henry L. Moses Distinguished Professor of Law and International Organization at the Columbia Law School. (Anu, The Brussels Effect: How the European Union Rules the World, pp. 24 )

Finally, being able to set norms globally allows the EU to prove to its critics that it remains relevant as a global economic power. Embracing the role of a regulatory hegemon reinforces the EU’s identity and enhances the EU’s global standing even in the times of crises where its effectiveness and relevance are constantly being questioned. If the EU wants to exert influence, it must do so with the means available to it. Lacking traditional means of power, the EU’s greatest global influence is accomplished through the norms that it has the competence to promulgate. In the absence of military power or unconstrained economic power, the EU can exercise genuine unilateral power most effectively by fixing the standards of behavior for the rest of the world.80 In the world where the United States projects hard power through its military and engagement engagement in trade wars, and China economic power through its loans and investments, the EU exerts power through the most potent tool for global influence it has—regulation.

### NB: A2 “Strong EU Undermines NATO”

#### Stronger EU defense / autonomy does not cause delinking with NATO

Credi et al., IAI researcher, ‘20

[Ottavia Credi, Junior Researcher, Security and Defence Programmes, Istituto Affari Internazionali (IAI),Alessandro Marrone, Head, Defence Programme, IAI, and Roberto Menotti, Editor-in-Chief, Aspenia Online“NATO Toward 2030: A Resilient Alliance and Its Main Priorities,” Digital International Seminar, Second Meeting, The New American Administration and Translatlantic Relations: A Renewed NATO?” 11—25—20, p. 6, <https://www.iai.it/sites/default/files/2020_aspen_iai.pdf>, accessed 5-17-22]

Because of the pressure of an aggressive multipolar system, whereby China’s influence is on the rise and the US increasingly focuses on the Pacific, NATO is bound to demand a higher level of burdensharing from its European members. In the worse-case scenario, the Alliance needs to be able to potentially fight a conflict in which American and European forces are to a certain degree interchangeable, and Europeans are able to hold NATO’s eastern flank with limited American support while a simultaneous crisis is attractingmost US forces in the Pacific. At the same time, by reaching an appropriate degree of strategic autonomy in the midterm, the EU will be able to operate with NATO on the high level of the conflict spectrum and contribute to Europe’s defense and deterrence. Still, European strategic autonomy should also cover non-military issues such as emerging technologies, just like the EU-NATO collaboration should concern the whole security spectrum.

At the same time, European strategic autonomy should not be seen as a potential cause for a de-linking between Europe and the US, the EU and NATO. Rather, it should complement NATO’s collective defense, which remains a cornerstone of the conventional nuclear continuum (to which the cyber domain should be added). As a matter of fact, by investing in its own defense and security, also through the EU, the Europeans will also demonstrate their willingness to take up greater responsibilities in NATO.

# NATO Focus Net Benefit

### NATO Focus NB: 2NC

#### Offloading to the EU strengthens NATO

Moller & Rynning, Seton Hall & University of Southern Denmark Professors, ‘21

[Sara Fjerg Moller, Assistant Professor, School of Diplomacy and International Relations, Seton Hall University and Sten Rynning, Professor, Center for War Studies, University of Southern Denmark, “Revitalizing Transatlantic Relations: NATO 2030 and Beyond,” WASHINGTON QUARTERLY v. 44 n. 1, Spring 2021, p. 193]

NATO’s continued transformation in the coming years seems all but certain; less certain is what it will transform into. The alliance has survived this long by adapting. But unlike during previous rounds of adaptation that involved the alliance taking on more responsibilities and tasks, the coming decades—whose defining feature will be the continued rise of China—will require a much more narrowly focused alliance. For nigh on three decades, NATO had the luxury of pondering what kind of alliance it wanted to be as it searched for a new raison d’etre in the reduced threat environment following the end of the Cold War. But the contrast between the 1990s and today’s deluge of challenges and threats is stark, and NATO no longer has the luxury of time.

To ensure the alliance’s future operational utility, the alliance must embrace its original collective defense identity and look for ways to streamline, and where possible reduce, its existing collective security and crisis management activities. In addition to offloading existing responsibilities to the EU and UN, NATO should think twice before taking on new mandates and avoid elevating new tasks like resiliency or counterterrorism missions and assigning them equal importance to Article 5. The alternative to the vision outlined here is an alliance increasingly weighed down by a myriad of tasks, unable to prioritize among them, and lacking both the political will and financial resources to perform its main function. An overburdened NATO risks being unable to fulfill its chief purpose of collective defense, thereby increasing the risk of further fracturing within the alliance. The proposed course of action will by no means be an easy one. But it provides the best chance to guarantee that the transatlantic alliance will have the capabilities and assets needed to meet the challenges posed by China’s rise.

#### U.S. cooperation with EU can also help counter China

Moller & Rynning, Seton Hall & University of Southern Denmark Professors, ‘21

[Sara Fjerg Moller, Assistant Professor, School of Diplomacy and International Relations, Seton Hall University and Sten Rynning, Professor, Center for War Studies, University of Southern Denmark, “Revitalizing Transatlantic Relations: NATO 2030 and Beyond,” WASHINGTON QUARTERLY v. 44 n. 1, Spring 2021, p. 185]

Second, the Biden presidency should embrace the global agenda Europeans are now developing in order to relaunch Euro-Atlantic cooperation. EU governments and authorities are pursuing an agenda (though still under negotiation and confidential) centered on health cooperation, economic recovery, climate policy, security cooperation, and the upholding of shared values.23 In effect, it is an invitation to craft a comprehensive Western response to the challenge posed by China’s economic rise and increasing political assertiveness.

In December 2019, the Trump presidency made some headway in this respect by gaining NATO’s acceptance to develop a China policy, but the transatlantic dialogue remains anchored in a debate over the role of technology and societal resilience.24 The EU— which, in March 2019, labeled China a “systemic rival”—was unsure of the leadership the United States was offering and whether the Trump administration would endorse the move or continue to treat the Brussels organization antagonistically.25 The EU is offering a reset to the United States and a new beginning to the Western response to China. The Biden presidency could exploit this to craft a new foundation for common policy initiatives especially on investment screening and technology policy, two of the areas where, given their implications for societal and military resilience, it is vital that Washington and Brussels come to an agreement.