# EU-NATO Cooperation CP

### Notes:

Simple “Agent CP.” It tests the “US Key” warrants of the affirmative and is an easy way to solve the affirmative without linking to US action. The China DA is a clean net-benefit as well as the forthcoming Midterms DA.

There’s also an internal net-benefit, but the perm might solve it and we only found one card. It just says EU leadership is good and that the CP might raise their profile and encourage more cooperation beyond the plan. You could use some of the “European Defence Good” cards from the NATO Bad/Withdrawal file.

The solvency evidence is pretty good. The EU has resources, expertise, and organizations to cooperation and there is a lot of ev about the need for the EU to lay the groundwork for a more integrated European defense network. Remember, you don’t need to solve the entire aff, but could win with “sufficient” solvency.

Final neg note is that you should consider making the CP texts more strategic by adding specific planks describing what the EU would do. Like the Diplomacy CP, the EU can’t do everything the DOD can, BUT it can take a number of actions to address the same harms (coordination, capacity building, data sharing, and development).

The aff has some perm options, not only because you can “do both” but also because NATO includes US as a member already, so “Perm - Do the CP” is an argument. The aff should rely on their US key cards from case and point out that a lot of the neg evidence says that the EU should cooperate more, but that they haven’t and aren’t really prepared to on that scale (the ev is prescriptive, not descriptive).

Thanks Maya & Hope and the rest of the GHS Lab!

## 1NCs

### 1nc – Generic

#### Text: The European Union should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of

#### < insert the plan area or mechanism >

#### The CP solves coordination, capacity building, data sharing, and development on emerging tech issues – EU-NATO coop reinforces existing programs to create better security.

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

POLICY RECOMMENDATIONS In a world marked by COVID-19, deeper social divisions, more vulnerable supply chains, and increased competition in the international arena, the roles of NATO and the EU and their ability to tackle global challenges are constantly being questioned. Moreover, with the proliferation of ad hoc coalitions to tackle specific challenges, the two organizations are constantly fighting for relevance and space to operate. In this context, as this paper has shown, both NATO and the EU have more to gain through joining forces rather than competing with one another. In light of the arguments developed so far, some broad policy recommendations appear relevant: 1. NATO and EU member states should leverage their policy fora to discuss joint initiatives and better employ their assets — NATO’s military capabilities and logistical systems and the EU’s capacity building and financial assistance. This would enable a more coordinated approach to crises based on a division of labor agreed to on a case-by-case basis. Learning from past experiences, the two organizations should work to avoid another “Afghanistan scenario” in areas like the Sahel region. 2. NATO and the EU should increase information sharing and establish protocols in crucial sectors from anti-terrorism cooperation to cybersecurity. The periodic joint exercises performed so far are important steps toward building confidence and fostering regular updates and the sharing of best practices. Yet insufficient information sharing and the lack of protocols in case of a crisis hinder the utility of the exercises conducted. While this recommendation ultimately depends on political will, some smaller channels could be created to streamline limited but vital information, especially in the event of a cyberattack. 3. Regarding disinformation, NATO should take advantage of the EU’s apparatus and support it with its own solid structure for intelligence gathering — instead of having NATO’s Public Diplomacy Division duplicate the work of the EU StratCom task force. Alternatively, because countering disinformation is not the main job of the division, NATO could create a separate disinformation unit to work closely with the EU’s task force. Coordinating efforts to tackle different outlets of disinformation could help reduce the overall burden. In both scenarios, the two organizations should not just seek to counter disinformation but also prevent it as much as possible. 4. NATO and the EU should increase their dialogue on regulations and impediments to military mobility and interoperability. NATO’s deeper expertise on strategic airlifting and military operations could help the EU improve regulations to facilitate military mobility. More broadly, NATO should leverage EU regulatory power in conjunction with its objectives when it comes to capacity building as well as in countering China’s multifaceted influence. 5. To reinforce NATO’s posture in Europe and elsewhere, the EU should boost its military capability (as member states’ militaries contribute to NATO’s single set of forces). Enhanced military capabilities would also enable the EU to intervene independently from the United States in theaters that are no longer security priorities for Washington. European countries will need to assess their defense spending for greater efficiency and assess the advantages of a more integrated procurement system. While doing so, Europeans should consider mechanisms to enable the U.S. defense industry to participate; this could minimize the economic losses, foster technological development and cooperation on a trans-Atlantic level, and reduce dependence on geopolitically risky supplies. 6. NATO and the EU should foster cooperation in procurement and capability development to increase interoperability, including through the establishment of similar standards. This would enhance military mobility and interoperability across Europe and other theaters like the Indo-Pacific, where the engagement of the U.S. and Europe is growing.

### 1nc – Cybersecurity

#### CP text: The European Union should substantially increase its cybersecurity cooperation with the North Atlantic Treaty Organization by

* establishing a joint taskforce for cyber crisis responses coordination
* intensifying joint cyber exercises
* creating an information hub to share data
* creating a common cyber trust fund

#### The CP creates an effective European cybersecurity network – solves the aff

Lete ’19 [Bruno Lété currently serves as a transatlantic fellow, security and defense at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international security and defense policy. “THE EU AND NATO: the Essential Partners”. 2019. European Union Institute for Security Studies. https://drive.google.com/file/d/18Um8tOva0YQLiUGAjjzkkuUnIIXx-TGZ/view?usp=sharing. Accessed 6-22-2022; MJen]

~ Evolving to a joint model The priority for the EU and NATO is to now find agreement on how to mitigate cyber- security threats which are becoming more frequent and more sophisticated. EU-NATO : cooperation is essential to allow European and transatlantic governments to become better at preventing, detecting, and deterring cyberattacks, as well as to hold those that engage in malicious cyber activities accountable. As such, both organisations must continue to seek new ways of cooperation that deepen and broaden their engagement. The following recommendations are achievable, some immediately and others in the long term. But given the scale of the threat, it is necessary to think ambitiously. Create an EU-NATO cyber threat information hub Joint structures that combine EU and NATO resources or expertise are nothing new. The European Centre of Excellence for Countering Hybrid Threats in Helsinki is a good example of how, with the necessary good will, the EU and NATO can work together un- der the same roof. The creation of an EU-NATO Cyber Threat Information Hub could be another step in this vein. The mission of such a hub would simply be to improve information sharing by building relations and networks between the EU, NATO, mem- ber states and partners. It could do so first of all by advising technical and operation- al level Standard Operating Procedures (SOP) for information exchange between the EU and NATO entities, and identifying how to enable secure lines of communication to share confidential cyber intelligence. In addition, it could assist the EU and NATO in defining what type of information needs to be shared, who needs to receive it, when the information needs to be shared, and making sure the information is released in a timely and appropriate manner. In this regard, the hub could make active recommendations concerning the growing role of automated information sharing in identifying rele- vant information more quickly, but also in automating threat mitigation in real time. Automated sharing of security and threat information could also help the EU and NATO to standardise their threat intelligence. The hub could identify adequate informa- tion-sharing platforms or information-storage clouds that can withstand increasingly complex attacks, based on open industry specifications. Such platforms bring several benefits. They enable rapid communication and peer-based sharing, they reduce cost, and increase the speed of cyber defences by substituting manual responses for auto- mated processes. In this regard, the hub could make active proposals on how to use the EU’s Permanent Structured Cooperation (PESCO) or the European Defence Fund (EDF) to develop this type of technological capacity. The recent proposal of eight EU member states to develop a ‘Cyber Threats and Incident Response Information Sharing Platform’ under PESCO encourages more thinking in this direction. The success of EU- NATO cooperation in preventing, detecting and deterring cyberattacks will ultimately be defined by the ability of the two organisations to share information more effectively. Cautious steps in this direction have already been taken; for instance the EU was grant- ed access to the NATO Malware Information Sharing Platform. But both organisations will need to continue to explore bold initiatives if they are to address today’s informa- tion-sharing gap. Establish an EU-NATO Taskforce for cyber crisis response coordination To efficiently synchronise their cyber crisis response mechanisms the EU and NATO : will need to create additional capacity. The existing structures that allow the EU and - NATO to come together are still limited, ranging from formal and informal meetings ~ between the North Atlantic Council (NAC) and the EU Political and Security Committee (PSC), exchanges at ministerial meetings, cross briefings to respective Committees and i - Councils, and informal staff-to-staff interaction, for instance between the European External Action Service and NATO’s International Staff. These interactions are valu- : able, but they do not represent a solid basis for guaranteeing an efficient and smooth | ~ collective response in the event of a real cyber crisis. A roadmap for collective response is therefore needed. An immediate way to achieve this would be to create a structure — like a joint taskforce — that brings together the EU Cyber Crisis Response Framework ~ and NATO’s Crisis Response System. This taskforce would be convened when a ma- jor cyber incident strikes multiple EU member states and NATO Allies or EU/NATO institutions. To prepare this taskforce for operational duties, in a first stage, its task would be | to map the full spectrum of EU and NATO competencies for cyber defence, to clari- fy responsibilities at national and supranational levels for issues like attribution and countermeasures, and based on this information to create a common template of cyber crisis management phases. Once such a common template is created, in a second stage,% ~ the taskforce could then be convened to respond to cyber incidents. This taskforce! could also be useful in many other ways. For instance, it could make recommenda ~ tions on how to synchronise joint strategic communication among EU and NATO in- stitutions, or make proposals on how to use EU PESCO and NATO structures to supporti countries before, during and after crises. It could also look at creating linkages betweeni the EU ‘Cyber Rapid Response Teams’ currently being developed under PESCO and the! existing NATO Rapid Reaction Team to Fight Cyber Attacks. Finally the taskforce couldi also make suggestions on how to include NATO into the EU Commission ‘Blueprint toi respond to large-scale cybersecurity incidents and crises’. The EU and NATO have a§ wide array of crisis management tools at their disposal, but they are disconnected. An% ambitious, but much needed step, would now be to align those different instruments and to create an EU-NATO ‘playbook’ on how to react to cyber incidents and crises. Develop EU-NATO triggers for a collective response to cyberattacks Talking openly about active and reactive responses in cyberspace is no longer taboo fori EU or NATO member states. And the policy instruments to conduct an offensive strategy or to sanction adversaries are steadily increasing. NATO for instance has already ~ recognised that a serious cyberattack on a member state could be a potential triggeri for Article 5. At its November 2017 defence ministerial the Alliance also agreed to cre ate a Cyber Operations Centre that will facilitate the integration of cyber capabilities with conventional military capabilities. The EU for its part created in 2017 its Cyber Diplomacy Toolbox, a framework for a joint EU diplomatic response to malicious cyber activities. In May 2019, EU countries also agreed that individuals and groups conducting cyberattacks from outside the bloc may be hit with potential sanctions, including travel bans and asset freezes. These measures have boosted the EU’s and NATO’s individual capacity to hit back at cyber adversaries. But there is today no template on how to synchronise these different EU and NATO tools, nor is there agreement on the conditions that would trig- ger the collective use of these tools. In other words, the circumstances in which the EU and NATO would work together to adopt a responsive or offensive posture are still éambiguous. While NATO and the EU have to an extent consciously embraced ambigu- éity for its strategic value, the absence of a clearer definition of an offensive posture, : and of the circumstances, degree, and manner in which counter-measures can or should be taken if member states perceive a cyber threat or suffer a cyberattack, make 1t more difficult for the EU and NATO to respond collectively. The conditions to use Ethe EU Cyber Diplomacy Toolbox or the trigger for NATO to launch an offensive cyber : campaign may be clear if a member state faces a large-scale, devastating cyber cri- ésis. However, most cyberattacks fall below the threshold of being perceived as a clear act of aggression. Formulating a proportionate response in this grey zone constitutes the biggest problem. Russian ‘active measures’ in Europe are for instance clearly de- ésigned to exploit these grey zones, and the Kremlin has acquired some sophistication i in avoiding red lines that would trigger a common response from EU or NATO member Estates. Russia is also not the only potential adversary capable of similar tactics. There is thus an acute need to define when and how the EU and NATO must respond against i day-to-day cyber intrusions. The development of a set of EU-NATO basic principles, or (non-binding) guidelines that would trigger a joint response would be a good first step. The Tallinn Manual® published by the NATO Cyber Defence Centre of Excellence could offer inspiration on how the EU and NATO can define these principles while respecting the application of international law. Currently the EU and NATO need to assess each individual cyber threat or cyberattack on a case-by-case basis without the support of standard measurement tools and indicators that can help them formulate a swift and proportionate response. This considerably slows down the decision-making process. However, if the EU and NATO were to dispose of a set of pre-agreed principles, it would significantly improve their joint reactiveness and resilience. Intensify joint cyber exercises, foster a culture of mutual trust Exercising, training and learning together is key to better understand each other’s institutional processes, to develop common responses, and to cultivate a culture of trust. In their history, the EU and NATO have found it difficult to adopt such a mind- ~ set. They held only one joint crisis management exercise in 2003, which prioritised politico-military priorities and did not include cyber assets. The EU and NATO also planned, but failed, to implement more exercises in 2007, 2010, and 2014. The Joint ~ Declarations of 2016 and 2018 have nevertheless turned the tide and today both organi- sations exercise, train and learn together more than ever before. But the rapprochement is in many cases still cautious. A key example are the EU and NATO ‘coordinated and parallel’ crisis management exercises — EU PACE and NATO CMX. Synchronising EU and NATO flagship exercises is a commendable step to develop more interaction but : working in parallel is still a very different concept than a ‘joint exercise’. De facto, EU | PACE and NATO CMX remain independent initiatives, they constitute only one signif- icant occasion per year where the EU and NATO exercise together, and they are not conducted at the same moment in time which represents an important disconnect with a joint crisis response in reality. A more realistic approach to creating a fully-fledged - EU-NATO joint exercise is perhaps to think small-scale. A useful angle in this respect would be to have EU-NATO staffs exercise how to align specific technical cyber inci- i dent information (from computer security incident response teams — CSIRTs) with ~ military intelligence threat assessments. Moreover, exercises must also go hand-in- ~ hand with joint training and education opportunities. The EU and NATO have already opened up their cyber courses to each other’s staffs. As a next step, they could further explore how to integrate NATO cyber defence courses with the recently launched EU - Cyber Education, Training and Exercise platform - an initiative from the European Security and Defence College to harmonise and standardise cyber defence education for - EU member states. Coherent training and joint exercises will be key to create a mutual ~ culture of trust and understanding. Create a common Cyber Trust Fund for partner countries Today the EU and NATO work individually with their partner nations on cybersecuri- ty and defence programmes. But EU and NATO programmes could become more effi- cient if both institutions coordinate their assistance in order to create more synergy and avoid duplication. The EU and NATO could coordinate their assistance for partners around issues like technical cyber capabilities, information networks, and standards. A coordinated approach would also enable partners to more efficiently share with the EU and NATO their firsthand information, expertise, and experience. To complement or bundle the efforts of various EU or NATO assistance providers, an independent Cyber Trust Fund, supported by the EU and NATO, could be created. Access to the Trust Fund could be granted to EU Associated Countries or partner countries of the NATO Euro- Atlantic Partnership, Mediterranean Dialogue, Istanbul Cooperation Initiative and Global Partnerships. The management of EU-NATO donations and screening of project proposals could be managed by an independent private law foundation — for instance based on the model of the European Endowment for Democracy. The Trust Fund could address an important gap by focusing on the buildup of local and grassroot cyber skills and enable various stakeholders in partner nations to attend EU or NATO cyber courses, seminars, training sessions and conferences, or to organise similar types of activities in their homeland. The Trust Fund could adopt new approaches towards the develop- ment of local skills (government, corporate or civil society), for instance by requiring local partners to be involved in the project, and avoid situations where European or American contractors simply export their technology or knowhow to the partner na- tions. In this light, the Trust Fund could only support projects proposed by the partner nations, rather than copying the EU and NATO approach of pre-defining specifics for trust fund projects. The EU and NATO have worked together on financial assistance programmes in the past, such as the regular EU contributions to NATO trust funds for the disposal of unexploded ordnances, and anticorruption initiatives. In this light, the development of an independent EU-NATO Cyber Trust fund may not be such a far- fetched idea after all. Shape global norms around state behaviour in cyberspace To sustain global peace and security, much capacity to prevent irresponsible state be- haviour already exists in traditional domains such as nuclear, chemical or biological warfare. But the legal tools to stop governments across the world from engaging in malicious cyber activities are still limited. The lack of international agreement on rules regulating state behaviour in cyberspace or triggers for ‘digital self-defence’ com- plicates efforts to manage cross-border cyberthreats. As such, the EU and NATO, as two rather like-minded bodies with overlapping memberships, have the opportunity to shape their own common vision for responsible nation state behaviour in cyber- space and project it to the world stage. Today, the most significant platform to clarify the application of legal frameworks in cyberspace probably remains the UN General Assembly’s First Committee, which deals with disarmament and international security. In this context the EU and NATO should have a common dialogue on how they can assist the work done by the United Nations Group of Governmental Experts on Information Security (UNGGE) — a UN platform designed to debate the applicability of internation- al law in cyberspace. EU-NATO cooperation could also be used to advance ideas about transparency and accountability in cyberspace in other international platforms, from the G20 to the OECD or OSCE.” The current volatile geopolitical relations on cyber- ~ security between major powers such as Russia, China, the US or the EU, means that | finding global compromise around the rules of state behaviour in cyberspace remains : very much an open question. The EU and NATO have an opportunity here to lead the way and use their combined political weight to promote their ideas on this issue on the global stage.Adapting together The accelerating change of the digital age, and the challenges it brings, is placing new pressures on the traditional structures of intergovernmental organisations like the EU or NATO. It also highlights how these traditional structures can find it difficult to co- : ordinate with each other, even if the political will to do so is there. However, both the EU and NATO will continue to face threats emerging from cyberspace. For a long time, : ~ both found themselves ill-adapted to deal with this new reality, but change is on the horizon. And common responses are slowly but surely being developed to assert EU and NATO credibility in cyberspace in the eyes of their members, partners — and, in- deed, adversaries. Clearly, bold initiatives are needed. The EU and NATO must transit : from an agenda that strengthens their coordination, exchange and consultation mech- anisms, to initiatives that improve their joint force-multiplying functions, their cyber | ~ capabilities, their communication and decision-making structures in cyber exercises, crises and conflicts, and their interoperability with partners in cyberspace. EU-NATO : cooperation in cyberspace has taken its first small steps, but it will take a bigger leap ~ forward to adapt to a digital age that is constantly, and rapidly, evolving.

### 1nc – NB

#### The CP sets the framework for broader EU-NATO cooperation – the spills over into cooperation over a laundry list of impacts. Outweighs and turns case.

Drozdiak ’15 [William Drozdiak was a nonresident senior fellow in the Center on the United States and Europe at The Brookings Institution, and is a senior advisor for Europe with McLarty Associates, an international strategic consultancy firm based in Washington. “Why can’t NATO and the EU just get along?”. 9-28-2015. Brookings. https://www.brookings.edu/blog/order-from-chaos/2015/09/28/why-cant-nato-and-the-eu-just-get-along/. Accessed 6-23-2022; MJen]

For anybody who spends time in Brussels, one of the more baffling mysteries in the self-styled “capital of Europe” is the lack of communication between the North Atlantic Treaty Organization and the European Union. Even though these vital Western institutions are located just a few miles from each other, there is a striking absence of policy coordination between them. This, at a time when the European continent is confronting multiple crises whose solutions will require ingenuity, innovative thinking, and smarter use of resources. HAPPIER TOGETHER The need for closer collaboration between the EU and NATO makes sense for several reasons. There is now greater overlap in membership than ever before—22 out of 28 NATO countries also belong to the EU. European allies are worried about an American retreat and want to see a reinvigorated U.S. commitment to their security. In fortifying ties between the two organizations, Europe could be reassured by an abiding American involvement on their continent. And deeper bonds between NATO and the EU could have tangible political benefits, perhaps even to help persuade Britain to stay in the EU. For the United States, this kind of initiative could revitalize the transatlantic alliance as the foundation of our political, security, and economic relations with the rest of the world. It could also demonstrate that the community of Western democracies still remains our front line in defending common values and interests in the 21st century. A new approach to Western security cooperation—starting by creating a joint policy planning council linking the EU and NATO—should extend beyond military thinking and pursue more imaginative responses to current threats. Those include hybrid warfare by Russia, surging waves of refugees from North Africa and the Middle East, pandemic disease, climate change, and economic instability on Europe’s periphery. Future security challenges will demand more pluralistic policy responses that could be best accomplished by combining NATO and EU assets and capabilities. In the fight against terrorism, NATO could work directly with the EU to connect national criminal databases and use the EU’s special powers to seize financial assets of suspected criminals. The EU and NATO should also collaborate to avoid conflict with Russia over the control of energy resources and shipping lanes through the Arctic region. The melting polar icecap will transform global shipping routes by shaving thousands of nautical miles and up to seven days of travel time off current itineraries through the Suez and Panama canals. For those reasons alone, it is imperative for the West to prevent Russian domination in the Arctic. Other regional challenges will require closer NATO and EU cooperation. The United Nations predicts the world will need 70 percent more food to feed a global population of 9.6 billion by 2050; some experts say at least three dozen countries could be desperately short of crops or fresh water within the next 10 years. The Intergovernmental Panel on Climate Change predicts that by 2020, between 75 and 250 million Africans could face starvation or drought—which could trigger new wars that might require EU and NATO intervention.

## Solvency

### S – Generic

#### NATO and EU cooperation can successfully build long-term defence against Russia and China without relying on the US – the CP ensures lasting European autonomy.

Simón ’19 [Luis Simón is a Director of the Research Centre for Security, Diplomacy and Strategy and a Research Professor in International Security at the Brussels School of Governance. “EU-NATO Cooperation In An Era Of Great-Power Competition”. 11-26-2019. GMFUS. [https://www.gmfus.org/news/eu-nato-cooperation-era-great-power-competition. Accessed 6-23-2022](https://www.gmfus.org/news/eu-nato-cooperation-era-great-power-competition.%20Accessed%206-23-2022); MJen]

Over the past two decades, discussions on EU-NATO relations have been closely associated with crisis-management operations and transnational threats. But that is yesterday’s world. The return of great-power competition is eliciting a shift in European security and transatlantic relations toward deterrence and defense. As such the conceptual framework that has so far underpinned debates on EU-NATO relations has been, by and large, rendered obsolete. The return of great-power competition and growing uncertainty about the United States' commitment to Europe have led to renewed calls to turn the EU into an autonomous pole in global politics. Some even toy with the notion of European equidistance in a global context that is increasingly defined by Sino-American competition. At the same time, the EU’s need to give its global role security and a transatlantic anchor underlines the potential of a more structured EU-NATO dialogue. Great-power competition also has important implications for capability development. A key challenge is to ensure that the EU’s new defense initiatives help reinforce NATO’s ongoing efforts in deterrence and defense. One way to do that would be to give the EU’s High Representative for Foreign Affairs and Security Policy the authority to bring together the industrial and politico-strategic aspects of the union’s defense policy and thus act as an effective bridge between the EU and NATO. The last three years have witnessed a steady flow of self-congratulatory remarks about unprecedented progress in the relationship between the European Union and NATO. Their joint statements in 2016 and 2018 provided a compass for greater cooperation between them. But it is important to put this in perspective and ensure that the relationship keeps apace with a rapidly changing— and worsening—geostrategic environment. Discussions on EU-NATO cooperation remain stuck on a 1990s wavelength, taking crisis management and transnational challenges as their key referents. As NATO leaders meet in London and the EU undergoes a leadership transition, they should revamp their dialogue around the increasingly important theme of great-power competition. Crisis-Management Cooperation Ever since the EU stepped into the realm of security and defense in 1999, discussions on EU-NATO relations have been intimately linked with the notion of European strategic autonomy. See, for example, Jolyon Howorth, European integration and defense: the ultimate challenge? European Union Institute for Security Studies, 2000. Whereas European countries tend to see the EU’s Common Security and Defense Policy (CSDP) as a useful means to curb over-reliance on the United States in security matters, the latter has traditionally perceived the EU’s ventures in this domain as both an opportunity and a challenge. This equivocal attitude on the part of NATO’s leading member has also reflected on the EU-NATO relationship, which has always displayed a mix of competition and cooperation. From the outset, the United States warned that any attempt by Europeans to pursue security cooperation in the EU framework should avoid duplicating existing NATO structures, discriminating against non-EU NATO members, or decoupling the EU from the transatlantic security architecture. Yet, it also recognized that there was a growing political demand for European strategic autonomy. More importantly, perhaps, this demand came at a time when the United States was adopting a less direct and engaged approach to European security affairs, as it sought to shift its attention to other regions. For this shift to be successful, Europeans would have to do more in the security sphere. European integration and defense. From a U.S. viewpoint, there was a way to square the European security circle: CSDP would be welcome as long as it helped overcome Europe’s strategic introspection and generate the capabilities needed for expeditionary operations while being firmly embedded in the NATO framework. Key EU member states like the United Kingdom and Germany were sympathetic to this vision. Thus, a sort of balance emerged, with the EU explicitly acknowledging NATO’s monopoly in collective defense and confining its venture into security policy to the realm of external crisis management, and more particularly to those contingencies where NATO as a whole was not engaged. This arrangement would still work for those countries, like France, eager to underscore the EU’s autonomy vis-à-vis NATO and the United States. The absence of great-power competitors and the salience of transnational challenges meant that collective defense and deterrence were not really on Europe’s politico-strategic radar. In this vein, the 2003 European Security Strategy noted that “ large-scale aggression against any Member States” had become “improbable” and that Europe was facing “new threats” such as terrorism, the proliferation of weapons of mass destruction, regional conflicts in the European periphery, “failed states,” or organized crime. The focus was not so much on high-end warfare against peer-adversaries, but rather on external crisis management in militarily semi-permissive environments. When it comes to external crisis management, the EU and NATO have been cooperating and competing at the same time. On the one hand, the 2002 Berlin Plus agreements granted the EU access to NATO assets for the planning and conduct of such operations, while efforts to coordinate capability-development processes in the EU and NATO outlined the complementarity between them. On the other hand, the EU’s efforts to set up its own command arrangements as well as to launch operations in Africa—often at France’s behest—underlined the principle of political and operational autonomy from NATO and the United States. Enter Great-Power Competition For almost two decades, the concept of European strategic autonomy and discussions on the EU-NATO relationship were closely associated with external crisis-management operations—but that is yesterday’s world. Neither the EU nor NATO have given up on this field, which remains particularly relevant in Europe’s extended southern neighborhood. However, the return of great-power competition is eliciting a conceptual shift in U.S. and European thinking, away from crisis management and transnational threats and toward deterrence and defense. The return of great-power competition is increasingly recognized in NATO and EU circles. For the alliance, Russia’s annexation of Crimea marked a turning point. The 2014 and 2016 NATO summits in Wales and Warsaw ushered in rebalancing to the core business of deterrence and defense in a context of Russian revisionism, even as crisis management would still remain part of NATO’s remit. More recently, the question of how to deal with China has also found its way into NATO debates, partly as a result of repeated U.S. references to the country as a “long-term strategic competitor” and “the greatest threat to the West,” but also partly spurred by European worries about Beijing’s recent military exercises in the Mediterranean and Baltic seas, and its military modernization. Against this backdrop, NATO launched an internal strategic reflection on China earlier this year. For its part, the EU already referred to Russia as a strategic challenge in its 2016 global strategy, and it has more recently defined China as a systemic rival. In his confirmation hearing, High Representative for Foreign Affairs and Security Policy Josep Borrell alluded to the existence of an increasingly competitive world and argued that the EU should learn to “use the language of power.” This theme resonates with European Commission President Ursula von der Leyen’s call for a more “geopolitical Commission.”‘A commission to stand up for Europe’s interests’, A New Framework for EU-NATO Relations? The shift from a world dominated by transnational security challenges to one increasingly defined by great-power competition will have a pervasive impact on discussions on EU-NATO relations. Over the last three years, the Trump administration has expressed disdain for the multilateral, rules-based order Europeans hold so dear, and instead emphasized great-power competition with China and, to a lesser extent, Russia. While the EU is also concerned about Russian revisionism and China’s rise, Trump’s repeated swipes at it have also provided much political impetus in support of greater European political and strategic autonomy. There seems to be growing political support in EU circles around the need to reject a binary choice between the United States and China, and instead, invest in the development of the union as an autonomous pole in great-power politics. Yet, the existence of deeply rooted shared values within the West, the United States’ ongoing role in European security, and the fact that many European countries (especially in Central and Eastern Europe) have a closer political allegiance to Washington than Brussels underscores the limits to the notion of EU strategic autonomy and geopolitical equidistance between the United States and China. Great-power competition bears important implications for capability development. It is one thing for European countries to be operationally autonomous in the context of relatively modest out-of-area operations conducted against non-peer adversaries and another for them to deter or defend themselves against a great power such as Russia. The EU—and more particularly the European Defence Agency—has in recent years insisted that its work on capability cannot be restricted to crisis management and must incorporate capabilities required for defense and deterrence, regardless of whether they will be used directly by the EU itself or simply to boost the capabilities of its member states. This principle is meant to inform three key EU initiatives: the Capability Development Plan (CDP), the Coordinated Annual Review on Defence (CARD), and Permanent Structured Cooperation (PESCO). The CDP identifies those capabilities that the EU should collectively prioritize on the basis of evolving strategic and technological trends, thus providing a reference for CARD, which surveys existing defense capabilities and identifies opportunities for cooperation, and PESCO, which provides a framework to develop key 4 capabilities collaboratively. Yet, while the EU has the potential to develop the capabilities needed for defense and deterrence (nuclear weapons excepted), its current efforts (including through PESCO) are still primarily focused on the lower end of the military spectrum. The conceptual leap from crisis management to full-spectrum defense capabilities in EU circles opens up opportunities for cooperation with NATO in this field, not least given the renewed importance that European armed forces attach to deterrence, which NATO excels at and has much more experience in than the EU. This underscores the relevance of the NATO Defense Planning Process (NDPP), “a framework to harmonize national and NATO defense planning activities to enable Allies to provide the necessary forces and capabilities in the most effective way.” Notably, the CDP is meant to take into consideration NDPP requirements. Likewise, CARD aspires to develop in coherence with the NDPP wherever requirements overlap while acknowledging the different nature of the two organizations. In that same vein, the 25 EU member states that signed on to PESCO declared that it is complementary with NATO and insisted that the alliance “will continue to be the cornerstone of collective defense for its members.”Yet it remains unclear to what extent the CDP, PESCO, and CARD will actually feed into the NDPP process or provide an alternative framework. The key political challenge for the three EU initiatives is to make themselves relevant in the context of the newly launched European Defense Fund (EDF), which puts their relationship with NATO and the NDPP on the back burner. This leads to a critical sticking point in the EU-NATO relationship. In 2017, the European Commission launched the EDF as a vehicle to provide financial incentives to member states to advance toward a more efficient and competitive European defense-industrial base. In 2020, the European Defense Industrial Development Program will devote around €500 million to collaborative defense capability endeavors and some €90 million are already being invested in defense research projects. In 2021-2027, the EDF will invest €13 billion (about €1.8 billion per year). The United States has raised concerns about the difficulties for third-party participation in the EDF (as in PESCO), arguing that such barriers could undermine the integrity of the transatlantic defense market. The broader question, however, is to what extent the European Commission’s efforts on the defense-industrial front are grounded in a common political-strategic vision about the future of European defense. This is problematic within the EU framework, not least as the failure to give the high representative for foreign affairs and security policy a pivotal role in the EDF decision-making progress will only serve to aggravate the decoupling between the industrial aspects of European defense and the politico-strategic ones. Some measures have been adopted to ensure some interface between the two, such as placing the European Defense Agency at the center of the CDP, CARD, and PESCO processes, allowing it to act as a transmission belt to ensure that the EU’s industrial and technological priorities are capability-based, and thus strategy-based. Yet, as long as the European Commission remains in control of allocating the EDF’s money, there is no guarantee that funding decisions will be made on the basis of strategic considerations. The problem of an industrial-strategic gap in European defense transcends intra-EU bureaucratic rivalries, and even the EU itself. To the extent that the key challenge is great-power competition and deterrence, the real decoupling between the industrial and strategic aspects of European defense is the one between the EU and NATO. Since the growing importance of deterrence and defense underline NATO’s centrality to European security, strengthening the connection between the EDF, the CDP, and the NDP is critical to redressing the existing gap between the technological-industrial and strategic aspects of European defense.

#### EU has a comparative advantage in all emerging tech.

De Maio ’21 (Giovanna was a nonresident fellow in the Center on the United States and Europe at Brookings. She is currently a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. She holds a doctorate in international studies from the University of Naples, “OPPORTUNITIES TO DEEPEN NATO-EU COOPERATION”, December 2021, Brookings Institute, <https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf>)

In this regard, the EU appears to have a comparative advantage given the role of the European Defense Agency to go beyond specific operational requirements and its ability to consider long-term trends and ways member states can cooperate on the development of new capabilities. In particular, the EU defense procurement benefits from strong support from EU-led research and development programs, as well as from considerable financial resources from the European Defense Fund. As European defense capabilities advance, there will be overlap between the EU Capability Development Priorities and the NATO Defense Planning Process; this gives the EU and NATO an opportunity to foster greater cooperation and build up a more efficient and competitive trans-atlantic defense.73 A recent study from the French Institute of International Relations identifies areas where defense requirements could be harmonized and where the EU and NATO could work on joint research projects: from cyberdefense, air superiority, logistics, and medical support capabilities to science and technology, arms control, and intelligence.74 A more synchronized approach in these areas — that would also entail a joint assessment of member state performances — will undoubtedly reinforce both NATO- and EU-led operations as well as deterrence.

#### A balance between bolstering EU autonomy and multilateral cooperation is possible---they’re compliments.

Puglierin ‘21, Dr Jana Puglierin is Head of the Alfred von Oppenheim Center for European Policy Studies. From September 2013 to December 2015 she was a program officer at the DGAP’s Future Forum Berlin, “Strategic Partnerships and EU Security and Defence” in “Achieving Strategic Sovereignty for the EU”, European Parliament, <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653634/EXPO_STU(2021)653634_EN.pdf>)

However, the next four years of the Biden presidency should not be wasted on meta-debates. They present a window of opportunity for both sides of the Atlantic. It is up to the Europeans to prove that the European quest for greater strategic sovereignty can at the same time be positive for the transatlantic partnership and that a strong and self-reliant Europe is in America’s interest. And it is up to the Americans to show that they are interested in real partnership on greater eye-level, instead of curating vassals. The starting conditions are good: President Biden wants to repair the shattered relationship with the Europeans and make the transatlantic partnership the cornerstone of a unified Western approach toward great power competition. The recent US request to join a PESCO project on military mobility as a third country represents an initial test case – and a big opportunity - for a constructive future EU-US cooperation. For the Europeans, this also means that they must contribute greater added value to the transatlantic partnership through measures that simultaneously strengthen their own strategic sovereignty. First of all, this would be the development and procurement of more effective European capabilities, including high-end spectrum capabilities and strategic enablers. Very few PESCO initiatives currently address these capability gaps. Even if the issue of transatlantic industrial cooperation will remain difficult – Biden will be tough when it comes to buying and selling American – a basic willingness to support credible efforts to strengthen European defence capabilities is there. But the EU will need to demonstrate that its efforts go beyond subsidizing European defence industries and lead to a tangible boost in Europe’s operational equipment that would be available also within a NATO framework. Second, the EU needs to take some military load off the United States. They should assume greater regional responsibility in its Southern and Eastern neighbourhood and also increase their operational readiness for operations abroad. Third, Europeans should spell out what the European pillar of NATO is supposed to be and how it relates to CSDP. Cooperation between the EU and NATO has made much progress in recent years, but there is clearly still unused potential. Capability development and defence planning could be even better coordinated and further aligned. The ongoing Strategic Compass process should be closely linked to the NATO review process, especially in the areas of countering cyber and hybrid threats as well as fighting terrorism and disinformation campaigns, cooperation between the two institutions should be strengthened. The EU needs to reemphasise its effort to strengthen European military mobility and provide adequate funding.

#### EU-NATO summits allow the EU to take the lead on emerging tech.

Soare 21, Simona R. Soare was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest, “Innovation as Adaptation: NATO and Emerging Technologies”, German Marshall Fund, https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies)

As the allies meet with the EU High Representative for Foreign Affairs and Security Policy Josep Borrell at this month’s NATO summit, the two organizations need a more ambition agenda for cooperation. In particular, the EU and NATO need to consider a joint task force on fostering defense innovation and EDTs, with renewable two-year mandates. This instrument would provide political impetus for closer cooperation on EDTs, it would give coherence, regularity, and structure to the efforts of the two sides, and ensure commonality of purpose and synergy of output. In addition, allies could consider meeting regularly in EU-NATO digital summit formats. The EU could take the lead in this regard given its considerable financial capacity for investing in EDTs and its regulatory powers. EU-NATO digital summits would allow the transatlantic partners to regularly review progress, provide strategic guidance on legal, ethical and adoption challenges related to innovation and EDTs, and enhance their tech diplomacy by inviting like-minded global partners to attend.

### S – Cyber

#### Increased EU-NATO cooperation over cybersecurity is vital and likely to happen- recent developments prove.

Lété and Pernik ’17 (Bruno Lété currently serves as a senior fellow at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international affairs. He focuses primarily on NATO, transatlantic defense cooperation, developments in Eastern Europe and the Black Sea region, and cybersecurity. Piret Pernik is a researcher at NATO Cooperative Cyber Defence Centre of Excellence, “EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions,” The German Marshall Fund of the United States, No. 28, December 2017, <https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf)-> HL

Cybersecurity and defense have long been part of EU and NATO calculus but have only recently moved to the top of their agendas. The game first changed for Europe in 2007, when cyber-attacks in Estonia forced both institutions to think more seriously about this type of threat. As a result NATO developed in 2008 its very first Cyber Defense Policy.1 Five years later, the EU followed suit by adopting its first Cybersecurity Strategy. The 2014 crisis in Ukraine was Europe’s next big shock. Russia’s annexation of Crimea and semiclandestine military actions returned new urgency to European defense and deterrence, but also to cyberdefense and readiness as Russia’s hybrid aggressions against Ukraine included cyber-attacks.3 Since then, NATO and the EU have intensified their initiatives in the cyber sphere. NATO endorsed an enhanced cyber defense policy and action plan in 2011, and it decided to operationalize cyberspace as a domain of defense policy and planning in 2016. That same year all Allies also made a Cyber Defense Pledge to enhance their cyber resilience as a matter of priority.4 The EU for its part made the fight against cybercrime one of the three pillars of the European Agenda on Security, and recognized cybersecurity as one of the priorities for the Global Strategy for the European Union’s Foreign and Security Policy. In 2017 the EU adopted a “Cybersecurity Package” including the revised Cybersecurity Strategy.5 In this climate of urgency the EU and NATO have started to see each other as complementary partners to build up their cyber resilience. In order to foster operational level information sharing, NATO and the EU signed a Technical Arrangement on Cyber Defense in February 2016 between NATO’s Computer Incident Response Capability and the EU’s Computer Emergency Response Team. The most significant step was made with the signing of the EU–NATO Joint Declaration of July 2016 that creates a concrete framework for cooperation in security and defense. With regard to cyber, the implementation plan of the EU–NATO Joint Declaration recognizes four areas of cooperation: integration of cyber defense into missions and operations; training and education; exercises; and standards. EU–NATO cooperation in times of crisis is increasingly becoming a must. And in the field of cybersecurity and defense the past years have indeed been pivotal.

#### EU-NATO coop needed now – squo cyber relations are not enough.

Lete 19 [Bruno Lété currently serves as a transatlantic fellow, security and defense at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international security and defense policy. “THE EU AND NATO: the Essential Partners”. 2019. European Union Institute for Security Studies. https://drive.google.com/file/d/18Um8tOva0YQLiUGAjjzkkuUnIIXx-TGZ/view?usp=sharing. Accessed 6-22-2022; MJ]

The EU and NATO are targeted by the same cyber threat vectors that undermine all levels of society in member states, threatening civil, political, econom- ic and military security. The vast increase in the number of cyberattacks and the emergence of cyberspace as a new battlefield has motivated the EU and NATO to launch initiatives to strengthen their cyber resilience, and to increase their mutual consultations and coordination in the cyber domain. While the recent progress in EU- NATO cyber relations is commendable, this chapter nevertheless argues that the EU and NATO will eventually need to evolve from today’s coordinated approach to a more ambitious and integrated joint model of cooperation if they are to respond adequately to the security threats that shape today’s digital age. The first part of this chapter out- lines the history of EU-NATO cooperation in cyberspace. The second part highlights the present-day challenges that prevent a more ambitious EU-NATO cooperation agenda. The third part formulates concrete recommendations on how to move from a coordi- nated approach to a joint model for EU-NATO cooperation in cyberspace. EU and NATO responses to cyber insecurity Cybersecurity and defence have long been part of the EU and NATO calculus but it is only gradually that the issue moved to the top of their policy agendas.! The first game-changer for Europe came in 2007, when a series of coordinated cyberattacks on Estonia forced both institutions to think more seriously about this type of threat. With the aftermath of Estonia in mind, in 2008 NATO developed its very first Cyber Defence Policy. Five years later, in 2013, the EU followed suit by adopting its first ~ Cybersecurity Strategy. Another wake-up call for Europe came with the 2014 crisis in Ukraine. Russia’s an- | nexation of Crimea and semi-clandestine military actions in Donbass lent new urgency ~ to cyber defence and readiness because Russia’s hybrid aggression against Ukraine also - included sophisticated cyberattacks.? Since then, cybersecurity has loomed increasing- ly large in NATO and EU priorities and both institutions’ initiatives in the cyber domain ~ have increased exponentially. NATO endorsed an enhanced cyber defence policy and action plan in 2011, and it decided to operationalise cyberspace as a domain of defence policy and planning in 2016. That same year all Allies also made a Cyber Defence Pledge to enhance their cyber resilience as a matter of priority. At its last Brussels Summit in July 2018, the Alliance - also announced the creation of a new Cyberspace Operations Centre as part of NATO’s strengthened Command Structure. The EU for its part made the fight against cyber- crime one of the three pillars of the European Agenda on Security, and recognised cy- bersecurity as a priority for the 2016 Global Strategy for the European Union’s Foreign - and Security Policy. The same year the EU Directive on the Security of Network and ~ Information Systems introduced important legal measures to boost the overall lev- : el of cybersecurity in the EU. In addition, in 2017 Brussels adopted a ‘Cybersecurity - ~ Package’ including the revised Cybersecurity Strategy and the introduction of a Cyber : ~ Diplomacy Toolbox.> In November 2018 the EU also updated its 2014 Cyber Defence Policy Framework to strengthen European strategic autonomy in cyberspace. Finally, ' in May 2019, member states adopted a list of ‘EU cyber sanctions’ targeting individuals ~ or groups that engage in cyberattacks against the bloc. In this climate of urgency, the EU and NATO have started to see each other as com- plementary partners in the endeavour to build up their cyber resilience. In order to foster operational-level information sharing, NATO and the EU signed a Technical Arrangement on Cyber Defence in February 2016 between NATO’s Computer Incident Response Capability (NCIRC) and the EU’s Computer Emergency Response Team (CERT). The most significant step was made with the signing of two EU-NATO Joint Declarations, in July 2016 and in July 2018, that create a concrete framework for coop- eration in the sphere of security and defence. With regard to cyber, the implementation plan of the EU-NATO Joint Declarations recognises four areas of cooperation: integra- tion of cyber defence into missions and operations; training and education; exercises; and standards. A common set of new proposals was added in 2017 to foster exchange between staffs’ relevant good practices concerning the cyber aspects and implications of crisis management and response, as well as operational aspects of cyber defence, with a view to improving understanding and synergies between the EU and NATO.\* Since neither organisation possesses the full range of capabilities to tackle contem- porary security challenges, there is a serious incentive for the EU and NATO to cooperate in times of crisis. And in the field of cybersecurity and defence the past few years have indeed brought significant change. The EU and NATO share many of the same priorities in cyberspace, their policies are largely identical — based on the principles of resilience, deterrence and defence — and their tools are becoming increasingly complementary. Active interaction in the field of cyber has significantly improved with exchanges be- tween staffs on concepts and doctrines, information on training and education courses, ad-hoc exchanges on threat assessments, cross-briefings, including on the cyber as- pects of crisis management and regular meetings, and featuring an annual high-level EU-NATO staff-to-staff dialogue.® Another concrete achievement is the fact that since 2017 the EU and NATO flagship crisis management exercises — respectively called EU PACE and NATO CMX - are being coordinated and held in parallel with options for mu- tual participation of EU and NATO staffs. Coordinating EU PACE and NATO CMX reflects the overall desire to develop more interaction between both organisations.

#### The CP maximizes resources, fills defense gaps, and avoids article 5 activation

Deschaux-Dutard ’21 – Delphine, Associate Professor in Political Science at the University Grenoble Alpes, France. She is also a researcher at CESICE and Vice-Dean for International Relations at the Faculty of law at the same institution., (“Is NATO ready for cyber war?”, pp.1-3, 8/30/21, <https://www.frstrategie.org/en/publications/nato-briefs-series/nato-ready-cyber-war-2021>) – sel

In a more and more connected world cyberspace has become the fifth battlespace. The latest Pegasus case, refereeing to a spying hardware which affected many European heads of states and government in the Summer of 2021, shows how much cyber threats are now part of the international security arena. NATO has tackled the cyber topic for over a decade. NATO’s awareness towards cyber threats started raising in the late 1990s, following cyberattacks by Serbian hackers against NATO Supreme Command’s (SHAPE) website during the air bombing campaign on Serbian positions in the frame of the Kosovo war. The cyberattacks against Estonia in 2007 and in the context of the conflict in Georgia in 2008 urged the Alliance to take this new threats seriously. NATO is today the most advanced international organisation regarding cyber defence. With a cyber command structure set up in 2008, its 2010 Strategic Concept has enabled it to lay the foundations of its vision for cyber defence. Indeed NATO frames cyber threats as a direct challenge for transatlantic and national security as stated in the 2010 Strategic Concept. The Alliance approved its first Policy on Cyber Defence in 2008 (revised in 2011 and 2014) and established a Cyber Defence Management Authority (CDMA) in 2008 and even a Cybersecurity Operations Centre within NATO Command Structure in 2018. The Strategic Concept adopted in November 2010 in Lisbon fully acknowledges cyber defence capabilities as a necessity for the Alliance. NATO also created tools to prevent cyber-attacks and cyber offensive capabilities with a central objective: to defend the Alliance’s own communications and information systems and to arouse its member states’ awareness on the need to protect critical infrastructures implied in contemporary military operations. At the NATO Summit in Wales in September 2014, the organisation crossed a new important threshold by recognizing cyber defence as part of the Alliance’s core task of collective defence and therefore included cyber threats as relevant article V material. This concretely means that NATO could trigger the article V of the Washington Treaty in case of a massive cyber attack with lethal implications against one of its members. Yet such a case would raise the difficult question of the attribution of the cyberattack. Such an attribution to a specific state or state-sponsored hacker would necessitate a consensus among the member states within the North Atlantic Council, which would probably make it difficult as it tackles diplomatic strings and strategic priorities which keep diverging among the EU member states. Indeed attribution continues to be a competence of member states until now, and not of NATO as such. Since 2014 NATO regularly reaffirms the importance of cyber defence as one of the core tasks of the Alliance, as it has been done during the Alliance’s summit in Brussels in June 2021: NATO endorsed a new Comprehensive Cyber Defence Policy supporting the three main priorities of the Alliance (collective defence, crisis management and cooperative security). The member states also agreed to commit to making use of the full range of capabilities to actively deter, defend against and counter the full spectrum of cyber threats at all times. Aside from these policy aspects, NATO also develops a wide range of tools and capabilities in the area of cyber defence, with the aim of being able to provide assistance to its member states in case of cyber-attack. It should also be acknowledged that NATO owns its information and computer networks used in NATO military missions, whereas in the case the EU for instance, the EU depends on the members states ICT infrastructures for CSDP missions. NATO set up a specific agency dedicated to cyber defence in 2012 at its SHAPE headquarters: the NATO Communications and Information Agency (NCI Agency), which hosts since 2016 a Cyber Security Operations Center (CyOC) dealing with around 500 cyber incidents each month and responsible for the cyber defence of NATO’s information and computer infrastructures in the world and on military theatres (like in Afghanistan until August 2021 for instance). This Cyber Operation Center should be fully operational in 2023. In addition to these tools the Alliance created a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which is a research and training facility dealing with cyber defence education, research and development. The main task of the Centre is to provide expertise on cyber defence, and organise cyber exercises involving both NATO Allies and partners. These tools are completed with NATO’s smart defence initiatives entailing cyber defence aspects and aiming at bringing member states to cooperate to develop and maintain capabilities they could not afford to develop or alone. The Alliance develops yearly exercises under the label Cyber Coalition. The development of NATO cyber capabilities over the last 15 years clearly shows that NATO started developing its own cyber defence culture. The organization therefore issued a Cyber Defense Pledge at the Warsaw summit in 2019 to facilitate cyber cooperation among its member states. As a follow up, France decided to host the first international conference in Paris in 2018 gathering the 29 NATO member states and the Secretary General of the Alliance to urge its allies to keep developing strategic thinking on cyber issues. Last but not least, NATO also develops an important cooperation with the EU on cyber defence. Both organizations have enhanced their cooperation in cyber defence since their joint declaration at the Alliance summit in Warsaw in 2016. They regularly organize common training and exercises and develop information sharing in order to raise mutual. Cooperation is even more needed in a context of limited financial resources: some experts suggest using the Berlin Plus agreements in cyber defence. The EU and NATO have also concluded a technical agreement between their response teams for cyber incidents (NCIRC and CERT-EU) in February 2016 to intensify their cooperation on cyber defence. This agreement has been enforced to discuss cyber threats in the context of 2019 European elections for instance. NATO also started a partnership with industry through the NATO Industry Cyber Partnership (NICP). More precisely the Alliance develops links with computer firms such as Microsoft, Atos, Thales, Cisco or Apple. The panorama of NATO’s cyberdefence assets shows therefore that the Alliance takes cyber threats seriously and dedicates resources and reflection to the topic. Even though NATO could not decide itself to trigger article V against a cyber aggressor, its member states have the common framework enabling them to act, should they manifest the political will to do so.

#### EU-NATO cooperation is key to cyber security.

Shea 19 (Jamie Shea, Senior Fellow at Friends of Europe and former Deputy Assistant Secretary General for Emerging Security Challenges, “EU-NATO COOPERATION A SECURE VISION FOR EUROPE,” Spring 2019, https://www.friendsofeurope.org/wp/wp-content/uploads/2019/06/dp\_2018\_web.pdf)//JRD

To **strengthen** inter-organisational **cyber** **security** and **cyber** **defence** **cooperation**, the **EU** and **NATO** should solve the political blockage, develop **joint** **action** plans to be implemented by member states and do away with technical issues such as the lack of **formal** **agreements** between **institutions**. The work done at staff-to-staff level must now be replicated at the national level by launching and investing in joint activities and projects that will increase member states’ capabilities. While top representatives spoke of ‘prioritising strengthened cooperation’ at the 2016 and 2018 NATO summits, more should be done to generate investments from the capitals. The following **policy** **proposals** aim to **designate** a number of **joint** **activities** with an aim to create more **substantial** **cooperation** among the member states of both organisations. A **strong** **political** support and **prioritisation** is **necessary** also from the **key** **capitals**. First and foremost, an EU-NATO working group on cyber security and defence issues must be established. These topics must also be regular agenda items in other joint working and high political level meetings, such as the EUNATO capability development group and the NAC-PSC meetings. This new working group should discuss policy themes where closer cooperation can create **synergy** (synchronising **crisis** **response** mechanisms, speeding **political** **decision-making**, developing **joint** **response** options to **cyberattacks**, etc). Joint working groups at the subject matter expert level should explore possibilities to **develop** **joint** **research** and **innovation** **programmes** and coordinate **national** and **union-level** **activities** in the area of **emerging technologies** (including 5G and artificial intelligence). Joint education and training courses should be created with the first step of opening all existing courses to each other’s officials and member states. The EU must be granted observer status at the Steering Committee of NATO’s Cooperative Cyber Defence Centre of Excellence (**CCD COE**), as suggested by the Allied Command Transformation. Formal cooperation – including technical arrangements for **information sharing** – must also be established with ENISA and other relevant EU bodies (such as the Cybersecurity Research and Competence Centre and EU-CERT) in order to facilitate participating in each other’s exercises. Closer cooperation between **research and competence** centres is needed to **jointly develop** doctrine and concepts, and launch **common research** projects in areas such as **cyber activities** in the grey space, **supply chain security**, **military dependencies** on civilian **critical infrastructure** (such as energy, transport and finance), including how do develop common methodology to assess inter-dependencies. The NATO Cyber Defence Pledge could also be applied to **non-NATO EU countries** and possibly in third countries. The resiliency requirements and cyber security standards of the EU and NATO should be complementary and ensure the minimum common level of protection in all countries. Information sharing between the organisations has been improved but more should be done to create joint threat assessments and intelligence sharing for attribution of cyberattacks. The EU and NATO should continue synchronising their hybrid threats playbooks with a view to creating joint responses. They must also synchronise cyber defence capabilities development **roadmaps and experiences** on improving civilmilitary information sharing. One way forward is through joint EU-NATO joint exercises, be they technical, crisis management or table-top style. The table-top exercises at the subject matter expert and ambassadors, foreign and defence ministers level should explore the application of EU’s cyber diplomacy toolbox and joint response options. More joint action is also needed to promote the **application of international law**, confidence building measures, and state responsible behaviour in cyberspace. Both organisations should create common cyber capability **building programmes**, including **joint trust funds**, for the third countries. In the area of cyber defence, the EU and NATO should explore options on how to use the sovereign effects of the NATO Cyberspace Operations Centre with a view to support future EU missions and operations. PESCO’s recent ‘Cyber Rapid Response Team’ initiative – comprised of nine participating EU member states – could be deployed to assist non-EU NATO countries and third countries to prevent, detect and respond to cyber incidents.

### S – AI

#### **The CP strengthens NATO deterrence and defense in AI.**

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

NATO and the EU address capability development in markedly different ways. NATO focuses more on procuring a given item from a given state to meet a specific need of the alliance, whereas the EU focuses more on filling capability gaps and encouraging member states to cooperate to develop new assets. In this regard, the EU appears to have a comparative advantage given the role of the European Defense Agency to go beyond specific operational requirements and its ability to consider long-term trends and ways member states can cooperate on the development of new capabilities. In particular, the EU defense procurement benefits from strong support from EU-led research and development programs, as well as from considerable financial resources from the European Defense Fund. As European defense capabilities advance, there will be overlap between the EU Capability Development Priorities and the NATO Defense Planning Process; this gives the EU and NATO an opportunity to foster greater cooperation and build up a more efficient and competitive trans-atlantic defense.73 A recent study from the French Institute of International Relations identifies areas where defense requirements could be harmonized and where the EU and NATO could work on joint research projects: from cyberdefense, air superiority, logistics, and medical support capabilities to science and technology, arms control, and intelligence.74 A more synchronized approach in these areas — that would also entail a joint assessment of member state performances — will undoubtedly reinforce both NATO- and EU-led operations as well as deterrence. Such an approach to procurement could prove particularly helpful given the rising threats coming from vulnerabilities in the global supply chain. The COVID-19 pandemic has unveiled Western countries’ strong dependency on Chinese supplies, both in the medical and technological fields (though the supply issues around personal protective equipment were addressed relatively rapidly).75 A recent study by the Mercator Institute for China Studies identifies 103 categories of electronics, chemical, mineral/metal, and pharmaceutical products in which the EU is critically dependent on imports from China.76 At the same time, as economies worldwide have started to recover from the pandemic and embark on ambitious investment plans to boost innovation in their national industries, the demand for semiconductors — crucial for building microchips, which are essential in any modern technology — has increased and become one of the central issues of the U.S.-China competition. This issue is further complicated by geopolitical concerns; a large proportion of semiconductor manufacturing occurs in Taiwan.77 The U.S. and the EU have recently begun initiatives to increase the domestic production of microchips. In June, the U.S. Senate passed the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act, which allocates $52 billion toward the effort.78 And the EU followed suit with European Commission President Ursula von der Leyen committing to a similar amount.79 The U.S. and EU discussed the issue during their inaugural Trade and Technology Council (TTC) meeting in Pittsburg, Pennsylvania, in September 2021.80 These discussions represent a first step toward breaking the ice on trans-Atlantic cooperation, particularly related to developing new technologies that are vital for enhancing geopolitical and economic security. But the main takeaways are that the U.S. and the EU are facing the same challenges and that the EU has increased its geopolitical ambition and range of interests. So far, there is no similar dialogue platform between NATO and the EU — a fact that hinders inter-institutional cooperation in the procurement domain. In fact, if NATO and the EU develop different standards, it could lead to duplication and hinder logistical and strategic interoperability across the trans-Atlantic space. For this reason, it is especially important for NATO and the EU to establish deeper communication on procurement and the definition of common standards. Increasing connections and synergies between industrial clusters within the trans-Atlantic space, particularly for materials such as semiconductors and microchips, would decrease dependence on geopolitically risky supply chains. Moreover, developing common standards when it comes to procurement, data privacy, and weaponry components would facilitate technological exchanges as well as the interoperability of equipment (be it artificial intelligence or more traditional military supplies) across the NATO-EU space. Given the increasing importance of new technologies for economic development, industrial advancement, and innovation, the only alternative to a shared approach in the trans-Atlantic space would be increased competition among allies and reduced interoperability — which would inevitably create more advantages for competitors to exploit.

### S – Biotech

#### Transatlantic cooperation on biotech solves

Giddings ’22 – Val, Senior fellow at the Information Technology and Innovation Foundation, (“Prospects for Transatlantic Cooperation in Biotech Policy—A US Perspective”, 3/11/22, <https://itif.org/publications/2022/03/11/prospects-transatlantic-cooperation-biotech-policy-us-perspective/>) – sel

A WORLD OF BIOLOGICAL POSSIBILITIES Mutual self-interest provides a strong basis for transatlantic cooperation in biotechnology based on shared recognition of its vast potential to provide solutions to some of civilization’s most pressing problems. Thanks to explosive advances in our understanding of the many ways in which promiscuous nature has been manipulating DNA and RNA for the past billion years, it is widely anticipated that the 21st century will belong to biology.1 We are now at the point where our ability to innovate is constrained less by technical capability than by the limits of our imaginations. Multiple laboratories and companies on both sides of the Atlantic (and throughout the world) are pursuing promising applications, and experience confirms progress would be accelerated by cooperative approaches. But there are some considerable challenges, especially in agricultural and industrial contexts. The most important rate-limiting factor in our ability to harness biological innovations to the challenges of feeding the world, sustaining human and environmental health, and addressing climate change, is the burden imposed by ill-considered regulations. Unless this bottleneck can be unblocked, the enormous potential for transatlantic scientific cooperation will not yield the necessary fruits. DIVERGENT REGULATORY PATHS: PRECAUTION VS. OPENNESS TO INNOVATION Existing policies, legislation, and regulations do little or nothing to advance human or environmental safety.2 Born out of understandable caution at the dawn of recombinant DNA technologies, today their most obvious impact is to obstruct and discourage research, development, and deployment of innovative solutions to various challenges.3 This is so despite an abundant record of production and consumption of new biotech products with enviable records of improved safety, superior sustainability, and widespread beneficial economic impacts.4 The benefits are so substantial that a pattern has emerged of farmers breaking the law to acquire and plant improved seeds in countries where governments have lagged in allowing access.5 It is one thing to implement policies and regulations ostensibly designed to ensure safety; it is quite another to ignore vast data and decades of experience around the world to maintain obsolete policies and regulations that add nothing to safety or sustainability, but only impede our ability to use the most innovative, precise, and safest tools to address our gravest challenges.6 In terms of regulatory policy and openness to biological innovations, the width of the Atlantic might be measured better in light years than miles or kilometers. As imperfect as regulations for the products of biotechnology are in North America, they are simply indefensible in Europe.7 The United States decided in 1986, after years of study and consultation, that no new laws were required to ensure the safety of crops and foods improved through biotechnology. This was based on the finding that they present no novel hazards, and foreseeable risks of their development and use fall into categories with which humans have considerable experience from millennia of conventional plant and animal breeding.8 The United States therefore decided to regulate these novel products under existing authorities administered by the Department of Agriculture, the Food and Drug Administration, and Environmental Protection Agency.9 While implementation of this policy, the “Coordinated Framework,” has been far from perfect, it has been sufficiently predictable and science-based to enable an explosion of innovation, new product development, and commercial activity. Consequently, the United States has led the world to the present day wherein crops improved through biotechnology are now the global standard for quality seeds, delivering improved yields, safety, sustainability, and economic productivity around the world, with the lion’s share of benefits accruing on behalf of small farmers in developing countries.10 Europe took a different approach. It is one thing to implement policies and regulations ostensibly designed to ensure safety; it is quite another to ignore vast data and decades of experience around the world to maintain obsolete policies and regulations that add nothing to safety or sustainability. The European Union decided to regulate seeds improved through biotechnology as a novel class governed under new regulations specifically focused on an arbitrary category known as “GMOs” (for “genetically modified organisms”). The conceit was that because they represented gene combinations produced by mechanisms supposedly “not found in nature” (but actually ubiquitous) they must present novel hazards, even though none has ever been identified. These putatively novel hazards, despite the lack of any concrete manifestations, allegedly required dedicated, specific, “precautionary” regulations. The resulting regulatory regime proved so burdensome it led to the general collapse of agricultural biotechnology in Europe, which had played a leading role in its discovery and invention. Permissions for field trials proved almost impossible to obtain, products could not be developed and brought to market, academic labs abandoned the field, and the industry relocated most of its assets and activities to the Americas. And Europe became the world’s largest importer of commodity foods improved through biotechnology, only recently surpassed by China. OPPORTUNITY FOR TRANSATLANTIC COOPERATION Many scientists in the EU (and around the world) knew from the beginning that this was the wrong approach, yet the EU pushed its model internationally, with aggressive diplomacy, leading to emulation by many countries in the developing world, with equally unhappy results to those seen in Europe.11 But a growing number of scientists, policymakers, and even “green” NGOs that had originally opposed GMOs, now recognize the counterproductive results of this approach and are working to avoid repeating the same mistakes with gene editing. This shines a spotlight on the most important and potentially fruitful opportunity for transatlantic cooperation in biotechnology: the revival of science-based regulatory regimes in which the degree of regulatory oversight is proportional to the hazards involved, and regulation that enables, rather than discourages the safe development of innovative products. A return to and reaffirmation of these first principles would provide fertile ground for cooperation and coordination globally. Regulatory reform (everywhere, not just in the EU and its emulators, though the need is greatest there) provides fertile ground for transatlantic cooperation and coordination. We have robust models of proven approaches.12 Without such cooperation, other progress in developing and deploying innovative solutions through biotechnology will be impeded or foregone. As to national security risks, just as with other risks, novelty attributable to biotechnology is elusive. One can do very nasty things with conventional bioweapons, and they are easily magnified with recombinant DNA techniques. At the same time, defensive capacities are also buttressed by biotechnology, as demonstrated by the rapid development of mRNA vaccines against SARS-CoV-2. There has been some good work done in this area, but this topic is worth exploring at greater depth. The OECD has a track record of thoughtful analyses with such topics. One possibility would be to build on that foundation by establishing a joint OECD/NATO working group to serve as a forum.

### S – Deterrence

#### Building defense capabilities through EU-NATO cooperation strengthens a weak NATO for future China/Russia warfare.

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

IMPORTANCE OF COOPERATING IN EMERGING THEATERS As the pressure from China and Russia rises and amplifies the threats posed by traditional challenges, the EU and NATO’s partners have little to gain from division and a lack of coordination. The time has come to identify new and better ways to fill security gaps and effectively allocate resources to ensure readiness on a variety of fronts. Moreover, to enhance coordination, each organization should consider how to add value to the other organization in both the military and non-military domains. At least four dimensions of the current security debate are crucial to strengthening the NATO-EU partnership: increasing European military capability, improving military mobility and interoperability, sharpening cooperation in the cyber and disinformation space, and finding synergies in procurement through the securitization of technology and supply chains. A stronger European defense to strengthen NATO’s posture While the EU has made significant progress in countering hybrid warfare since Russia’s annexation of Crimea, the same cannot be said with regard to developing more effective traditional deterrence capabilities. Such capabilities are increasingly necessary, not just because of Russia’s aggressive posture — expanding its area of operations beyond the post-Soviet space to Syria and Africa — but also because of the growing geopolitical and security alignment between Beijing and Moscow. Since 2014, cooperation between China and Russia has expanded beyond the domain of arm sales. The two countries have supported each other’s development of strategic weapons (such as for missile defense) and artificial intelligence, as well as each other’s political positions in the United Nations Security Council.41 Beijing and Moscow have deepened their interactions in Africa, where Russian Wagner Group mercenaries patrol Chinese facilities,42 and conducted military exercises including a shared air patrol in the Asia-Pacific region.43 They also have been seeking common ground on Afghanistan since the departure of U.S. troops.44 Such alignment is increasingly resembling a partnership that is reflected at the military level too. After the past year’s military drills in the Mediterranean, the Baltic Sea, and the Indo-Pacific, China and Russia recently conducted a joint military exercise called Zapad/Interaction-2021 in China’s northwestern region of Ningxia, where for the first time they used a joint command and control system and shared equipment — mimicking the way NATO forces work with each other.45 Meanwhile, the United States has begun to shift its security focus toward the IndoPacific region and South China Sea where Beijing is threatening Taiwan. Consequently, should a direct confrontation with China occur in the medium to long term, Russia could take advantage of the situation and potentially target Europe while U.S. forces and attentions are directed elsewhere. For this reason, it is crucial for European allies to have the military capabilities to push back against Russia with little support from the United States, at least in the initial phases. With more defense capabilities, European allies would also have the resources to respond to crises that arise in the Mediterranean region. After four years of strained trans-Atlantic relations — where the defense spending issue has intoxicated the broader debate on trans-Atlantic security — a stronger European defense would help Washington recognize the increased geopolitical cohesion and security concerns of the bloc. Unfortunately, as described earlier, such capability has yet to be achieved. A RAND Corporation wargaming simulation exercise assessed that in the case of a conventional attack by the Russian Federation, Moscow’s forces would be able to reach the outskirts of either the Estonian or Latvian capital in around 60 hours, and the NATO allies would not be able to defend these territories because of a (totally fillable) shortage of military capabilities.46 Similarly, a scenario analysis by the International Institute for Strategic Studies argued that without the help of the United States, conventional forces from European NATO countries would not be able to push back against the hypothetical conquest of Lithuania and part of Poland by the Russian Federation.47 To ensure that they can successfully respond to a land attack from Russia, or a coordinated Russia-China operation, Europeans need to increase the quality and readiness of their defense apparatus. A policy brief by the NATO Defense College calls for multinational battlegroups in Poland and in the Baltics to increase their readiness in terms of support capabilities, such as artillery and air defense, and for European allies to fulfill their NATO 2018 Readiness commitment of providing several land combat brigades and maritime task groups.48 The authors also point out that to increase deterrence, European allies need sufficient and effective air and missile defense capabilities to protect critical infrastructure, as well as long-range conventional precision-strike weapons to limit Russia’s options for regional conventional attacks. All these analyses indicate that expanded capabilities on the European side are crucial for a stronger NATO posture. Political tensions around the branding of European strategic autonomy have unfortunately poisoned this debate and complicated a very simple issue: European forces must be able to take effective action with or without the United States in the theaters that are crucial for European security.

### S – Interoperability

#### EU-NATO coordination reduces dependencies and coordinates assets to solve for interoperability.

De Maio ’21 (Giovanna was a nonresident fellow in the Center on the United States and Europe at Brookings. She is currently a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. She holds a doctorate in international studies from the University of Naples, “OPPORTUNITIES TO DEEPEN NATO-EU COOPERATION”, December 2021, Brookings Institute, <https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf>)

So far, there is no similar dialogue platform between NATO and the EU — a fact that hinders inter-institutional cooperation in the procurement domain. In fact, if NATO and the EU develop different standards, it could lead to duplication and hinder logistical and strategic interoperability across the trans-Atlantic space. For this reason, it is especially important for NATO and the EU to establish deeper communication on procurement and the definition of common standards. Increasing connections and synergies between industrial clusters within the trans-Atlantic space, particularly for materials such as semiconductors and microchips, would decrease dependence on geopolitically risky supply chains. Moreover, developing common standards when it comes to procurement, data privacy, and weaponry components would facilitate technological exchanges as well as the interoperability of equipment (be it artificial intelligence or more traditional military supplies) across the NATO-EU space. Given the increasing importance of new technologies for economic development, industrial advancement, and innovation, the only alternative to a shared approach in the trans-Atlantic space would be increased competition among allies and reduced interoperability — which would inevitably create more advantages for competitors to exploit.

### S – Disinformation

#### EU-NATO cooperation is key to stopping disinformation – turns the populism and democracy impact scenarios.

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

Leveraged EU advantages in the hybrid domain Although progress has been slow on the traditional military side, the European Union has proved to be a versatile asset for other aspects of security, specifically in the political and hybrid domains. Diplomatic and regulatory approaches are primary political tools to push back against autocracies. Despite its members having different strategic foreign policy priorities, the European Union has established a solid diplomatic posture in defense of European values and interests. For example, learning from its reaction to the Russo-Georgian War in 2008, the EU was able to create a united front following Russia’s incursions in Ukraine in 2014 and has imposed sanctions still in place today — for example, in response to the annexation of Crimea, the downing of Malaysian Airlines Flight 17 in eastern Ukraine, and more recently the poisoning of Russian opposition leader Alexey Navalny. On China, the European Union has acted consistently, based on its labeling of the country as both an economic competitor and a strategic rival. The EU has pursued commercial deals while also heavily regulating Chinese foreign direct investment in sensitive sectors of European interest. More meaningfully, the EU has repeatedly condemned China for its human rights abuses in Xinjiang, Hong Kong, and Taiwan and has announced a ban on products made with forced labor.57 While NATO is reinventing itself in the face of pressing challenges like China and climate change,58 the EU has advanced in tackling cybersecurity, regulating and exploring new technologies and developing its Indo-Pacific strategy.59 The EU’s advantages over NATO in the diplomatic and economic domains, especially when it comes to crisis management and political pressure, should be taken into account in broader discussion of NATO-EU coordination. Sharpened cooperation on disinformation and cyber The countering of disinformation is one key area where the European Union offers added value to international security. Since 2014 — and particularly following the disinformation operations carried out by Russia-sponsored media during the Brexit referendum and the U.S. presidential elections in 2016 as well as the French presidential elections in 2017 — the EU has set up a solid structure to monitor, detect, and counter disinformation. The EU was the first to establish a dedicated task force, the EU StratCom, within the European External Action Service (EEAS) to combat disinformation in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine). Subsequently, the European Commission established ground rules for online platforms and the advertising and social media industries, including a Code of Practice on Disinformation and guidelines on accountability obligations.60 The EU also has set up important monitoring activities, such as the Digital Media Observatory and the COVID-19 monitoring and reporting program, to function as a European hub for fact-checkers. A crucial part of these efforts is included in the Action Plan Against Disinformation that sets up a Rapid Alert System to facilitate information sharing and a unified response across the European institutions.61 Compared to the EU, NATO’s approach to combatting disinformation is less robust and limited in scope. NATO has set up tracking and monitoring activities — which offer fact-checking findings and counternarratives, including in the Russian language — but it has mostly relied on its Public Diplomacy Division which only monitors NATO-related material. For example, during the first few months after the outbreak of COVID-19, the division set up a section on its website called “NATO-Russia: Setting the record straight”; the website addresses the top five myths circulated by Russian propaganda regarding NATO’s connection with and reaction to the spread of COVID-19.62 Also established by NATO — but operationally independent — the StratCom Center of Excellence (COE) in Riga, Latvia brings together civilian and military stakeholders to conduct research on the use of modern technologies and to develop virtual tools for analyses, research, and decisionmaking. Hence, the center has produced valuable material for NATO’s Public Diplomacy Division. In addition, the StratCom COE has worked with the EEAS StratCom task force to train EU staff on how to respond to simulated disinformation attacks and responses. More recently, in 2019, the EU and NATO started exchanging information through the inclusion of NATO’s international staff in the EU Rapid Alert System, as well as through dialogues, staff and information exchanges and training exercises, including briefings between the EEAS StratCom and NATO Public Diplomacy Division.63 These are important efforts that highlight NATO and the EU’s openness to dialogue and mutual learning experiences. But they are nowhere near enough to keep up with the network of disinformation, where techniques are rapidly evolving and taking advantage of artificial intelligence. While China and Russia are reinforcing each other’s narratives through multiple channels, the effects of malign foreign influence in the disinformation domain are now being compounded by homegrown disinformation networks using the same pattern of exploiting people’s fear and vulnerability. Evidence of this occurring includes the spread of anti-vaccination propaganda as well as antidemocratic propaganda (which helped spur the assault on the U.S. Capitol in January 2021).64 Given the growing vulnerabilities in the trans-Atlantic space, NATO and the EU should join forces and expand their activity from countering disinformation to a preventing effort. The EU can add value in increasing the involvement of the private sector, and NATO can add value in using its intelligence capabilities in the counterterrorism domain to identify troll factories and disinformation sources. More broadly on cyber, despite advancements in their own jurisdictions, the paths of NATO and the EU have not crossed much yet. The two organizations have a different approach to cyber issues: While the EU aims to develop resilience against cyber threats, NATO has a broader and forward-looking approach that aims to prevent cyberattacks and to use cyber as an offensive tool to tackle threats and create deterrence.65 For example, the EU is seeking to strengthen its cyber posture through an EU Cybersecurity Strategy. The first piece of corresponding legislation, the EU Network and Information Security Directive (EU 2016/1148), established substantial cybersecurity standards that member states must adopt to protect critical sectors.66 Meanwhile, in its latest summit communiqué, NATO stated that “a decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis,” thus highlighting the increased awareness of the security implication of cyberattacks on critical infrastructure.67 Despite their different approaches, both NATO and the EU included cyber in their 2016 cooperation frameworks and started a series of joint exercises between the EU’s 2017 Parallel and Coordinated Exercise and NATO’s 2017 Crisis Management Exercise, as well as more recent exercises like those conducted through the CYBERSEC 2019 forum.68 However, while incredibly valuable, such exercises have not gone much beyond staffto-staff interactions and joint workshops. Understandably, cybersecurity cooperation implies a significant amount of intelligence sharing, which is ultimately impeded by a lack of trust stemming from political tensions and by the national security concerns of individual member states. In addition to establishing a more substantial channel for intelligence sharing to immediately warn allies about a cyberattack and prevent domino effects, other smaller steps could help increase cooperation and strengthen resilience in the trans-Atlantic space. For instance, the establishment of common standards related to threat and resilience capabilities could, in the event of a cyberattack, facilitate talks between allies and improve the interoperability of infrastructure. Within the United Nations, there are already two working groups trying to advance international legislation and standards covering the cybersecurity space.69 In line with these efforts, NATO and the EU could adopt similar standards that also help integrate and reinforce their complementary cybersecurity strategies. In particular, NATO could look at the existing EU regulatory framework and adopt similar strategies and resilience practices across the alliance, and the EU could benefit from NATO’s vast military experience and capabilities that are relevant to the cyber domain in order to bolster the security aspect of the EU’s cybersecurity strategy.

### A2: EU Fails

#### EU solves better and can act as a force multiplier given their solidarity and diverse country membership.

Belin ’19 — Célia; visiting fellow in the Center on the United States and Europe at Brookings. Her areas of expertise include trans-Atlantic relations, U.S. foreign policy toward Europe, French politics and foreign policy, domestic determinants of foreign policy, and the politics of travel under COVID. She holds a doctorate in political science (University Paris 2), a master's degree in international relations (University Paris 2), and a bachelor’s degree in Modern Languages/Business (University of Burgundy). April 2, 2019; “NATO matters, but the EU matters more”; *Brookings*; <https://www.brookings.edu/blog/order-from-chaos/2019/04/02/nato-matters-but-the-eu-matters-more/>; //CYang

Americans who are truly committed to the idea of a Europe “whole and free” should realize that NATO is no longer the main spinal cord of the European project; the European Union is. When George H. W. Bush coined the phrase in 1989, the level of intra-European integration was arguably on par with the defense alliance as providing stability and prosperity to the continent, and Americans were still heavily involved in both. Remember, this was pre-Maastricht Treaty, before the EU itself. Three decades of political, economic, and monetary integration later — and 16 new members later — the European Union is deeply entrenched in the lives of Europeans. Today, 28 European democracies, which used to compete among themselves and sometimes fight to their ultimate demise, now choose to pool sovereignty and have their interests communally discussed and collectively defended. The EU is a power multiplier: Every one of the 28 has a stronger individual voice because they stand together in the European Union. Small European countries, whose geography and demography would force them to cave to stronger neighbors, can now count on the solidarity of the group — as illustrated by the unwavering support for Ireland by the other 26 member states and the Brussels institutions in the Brexit negotiations. The neighbors of the European Union are no fools. Those who seek prosperity and stability hope to join the EU club. Those who reject the model set by the West and liberal democracies feel threatened by the European Union — it is the prospect of Ukraine moving into the EU’s orbit through an Association Agreement that triggered Russia’s hostility and ultimate aggression, not NATO. The power of attraction of the European Union, at least as much as the security guarantees of NATO, has helped stabilize Eastern Europe. Despite these realities, Americans often indulge in a scornful disregard for the EU. Recently, benign contempt has taken an ugly turn. Since taking office, President Trump and his administration have attacked the European Union and individual member states repeatedly, with near impunity. At first sight, American complaints appear to be centered on the issue of Europe’s trading power, which rivals that of the United States. For Donald Trump, the EU was created to “take advantage of” the United States and it is “worse than China.” Early in his mandate, the American president pushed for tariffs on steel and aluminum and threatened to go after automobiles, until a meeting with EU Commission President Juncker put a brake on the downward spiral. However, a deeper look reveals a fundamental ideological contention: The brand of nationalism and populism that defines this administration stands in direct contradiction with the very existence of a liberal, supra-national body such as the European Union. As laid out by the State Department’s Director of Policy Planning Kiron Skinner in December 2018, the administration holds the view that “international institutions have steadily encroached on the rights of sovereign nations” and that “nothing can replace the nation-state as the guarantor of democratic freedoms and national interests” — an indictment of the EU’s very existence. The ideological clash is reminiscent of older times. Addressing a crowd in Warsaw in July 2017, President Trump likened the European Union to the Soviet Union, criticizing a similar “steady creep of government bureaucracy that drains the vitality and wealth of the people,” an equivalency popular in conservative circles. Similarly, Secretary of State Mike Pompeo suggested in a December 2018 speech in Brussels that EU bureaucrats were not really working for the interests of European citizens. By making no secret of his personal support for euroskeptic forces, Donald Trump has become an active political opponent of the European Union in its existing form. He celebrated the Brexit vote, expressed support for far-right candidate Marine Le Pen ahead of the French presidential elections, disparaged Angela Merkel repeatedly, and appeared to rejoice at the Yellow Vests protest movement. He criticized Theresa May for negotiating a “soft” Brexit, and even recommended to Emmanuel Macron that France leave the EU. The American president has nominated ambassadors famously critical of the EU, and his administration demoted the EU ambassador’s status without notification, before reversing under criticism. As Donald Trump torments both the Atlantic alliance and the European Union, all rush to NATO’s bedside, and few worry about the EU. Truthfully, Atlanticists love to love NATO. It stands for values, valor, unity, solidarity. NATO won the Cold War. Celebrating NATO is celebrating the military. It is much harder to love the EU, the bureaucracy, the politics, the regulations. The EU lacks democratic appeal, and its slow-moving decisionmaking process create many frustrations. Unlike in NATO, the United States sits on the sidelines, it does not control who enters, or who stays in. The EU is also an economic peer competitor, a tough trading partner, and a sovereign international actor, at times non-compliant with American demands. Yet, the prospect of an implosion of the European Union should be as unbearable and intolerable to an American audience as the dissolution of NATO — or more so, as no one wants to see the demons of nationalism back on the European continent, along with a global economic catastrophe. Benign neglect is counterproductive; but a policy openly hostile to the European Union is a grave mistake. In a world where the strongmen are striking back, Americans should not forget that the European Union stands with the United States when it matters most. The NATO summit in Washington this week should be the occasion to recall not only the utmost importance of the Atlantic alliance to trans-Atlantic security, but also the crucial contribution of the European Union to peace, unity, and ultimately security for Europe and beyond.

### A2: Hurts NATO

#### The CP facilitates necessary autonomy for Europe

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

In the summer and early fall of 2021, two incidents cast doubt on the United States’ future commitment to European security. The first was the withdrawal of U.S. forces from Afghanistan despite the objections of NATO allies. The second was United States’ negotiation of the AUKUS nuclear submarine deal with Australia and the United Kingdom without informing France. (France had an agreement with the Australian government to build diesel-propelled submarines.)1 Europeans were furious. Charles Michel, president of the European Council, said, “What does it mean America is back? Is America back in America or somewhere else? We don’t know… We are observing a clear lack of transparency and loyalty.”2 European Commissioner Thierry Breton, who is French, spoke of “a growing feeling in Europe… that something is broken in our transatlantic relations” and called for a “pause and a reset.”3 These twin shocks created a new demand for what is intermittently called European strategic autonomy — the notion that the European Union should be more capable of acting on its own in pursuit of Europe’s interests. While France champions this idea, other European nations are more reluctant, especially those physically closer to Russia who see the United States as the key security provider. France argues that a greater role for the European Union is compatible with a continuing vital role for NATO in European security, but this begs the question of how the two organizations — NATO and the EU — relate to each other.

### A2: No Money

#### **CP saves money -Lack of EU-NATO cooperation wastes 100 billion euros annually.**

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

As with the cyber domain, NATO and the EU could respond to outside pressure by increasing and improving procurement and technological cooperation. The COVID-19 pandemic has triggered shortages and vulnerabilities in the supply chain, and the competition for rare earth material and high-technology products (such as microchips) has increased. Meanwhile, breakthrough technological achievements are opening new frontiers for competition in the security domain. First, European allies could better coordinate their defense spending within the framework of the European Union; the absence of an integrated defense structure inevitably leads to duplications and wasted resources. Moreover, the armed forces of different European countries may encounter difficulties in operating with one another, given that there are 138 defense systems in Europe (compared to only 30 in the United States).70 As stated in a European Commission report, the lack of cooperation in the European defense industry produces a loss of 25 billion to 100 billion euros per year, while 30% of the costs could be saved if a joint procurement was in place.71

## Competition

### A2: Perm DB

#### Perm links to the NBs because it requires US action and leadership. The CP doesn’t mandate US resources or focus and certainly wouldn’t be perceived as US action.

#### Perm doesn’t solve European autonomy benefits – US and European interests are mutually exclusive.

Franke 21, Dr. Ulrike Franke is a senior policy fellow at the European Council on Foreign Relations (ECFR), “Artificial divide: How Europe and America could clash over AI”, European Council on Foreign Relations, <https://ecfr.eu/publication/artificial-divide-how-europe-and-america-could-clash-over-ai/#why-work-together-disagreements-and-shared-goals>)

The transatlantic alliance has had a bad four years. The Trump administration’s criticism of the United Nations and the World Trade Organization, the president’s threats to leave NATO, and his active criticism of the EU all made Europeans wonder whether they had lost their most important partner. Moreover, in light of the conflict over 5G, in the minds of many Europeans, technology in particular has become an area that creates conflict in the transatlantic relationship rather than fostering cooperation. Although transatlantic relations are likely to improve under Biden, substantial damage has been done, and it will take some time to mend these ties. But, even if relations improve, it is becoming increasingly obvious that US has a diminishing interest in Europe as a geopolitically important part of the world. This trend was already visible under Trump’s predecessor, Barack Obama. It is, therefore, unsurprising that, on technology cooperation, both sides emphasise the importance of working with other actors as well as each other. The US National Security Commission on AI, for example, recommends that the US Departments of State and Defense “should negotiate formal AI cooperation agreements with Australia, India, Japan, New Zealand, South Korea, and Vietnam”. Its March 2020 report emphasises on several occasions the importance of the Five Eyes intelligence alliance. Meanwhile, Europeans are pursuing the idea of an alliance for multilateralism. And, on technology and AI more specifically, they have also begun to reach out to other democratic allies. European digital autonomy The most important aspect of transatlantic estrangement, however, is not the loss of trust between the US and Europe – which they will eventually reverse. Rather, during the four years of the Trump administration, and partly in response to isolationist tendencies in the US, Europeans have become much more comfortable talking about European strategic autonomy or sovereignty. Without encouraging the narrative that these efforts are directed against the US, or were primarily an answer to Trump, Europeans aim to empower Europe as an actor in its own right. In the technological realm, this led to the idea of European digital sovereignty, the aim of which is to build up European technological capabilities. Although European digital sovereignty is not specifically targeted at the US, it has led, among other things, to efforts such as the possible regulation of American technology companies and concerns over American firms acquiring European start-ups. European campaigners and some policymakers believe US tech giants such as Google, Apple, Facebook, and Amazon are forces to protect against. European thinking on technology partly developed in opposition to the US and US companies. Thus, European efforts to build up digital sovereignty may impede transatlantic cooperation.

#### The perm will just result in EU dependence and the US will crowd them out – means no defense autonomy and worse cooperation.

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

A weak European military European defense spending, specifically related to nations falling short of the NATO 2% of GDP target, has been a major issue in U.S.-EU relations. While Barack Obama’s administration exerted diplomatic pressure, Donald Trump’s engaged in open confrontation on this issue. Neither administration obtained significant results, however; and as Afghanistan has shown, Europe is still far too reliant on the military protection of the United States — an issue that weakens NATO’s posture. Over the past few years, the EU has strengthened both its legal and financial mechanisms to be more competitive on the security side. In December 2017, under articles 42.6 and 46 of the Lisbon Treaty, the European Council established a Permanent Structured Cooperation mechanism to deepen cooperation between willing member states. These states have agreed to binding commitments on investment, planning and management to advance their defense capabilities in the service of both national and multinational operations (including those of NATO and the UN). PESCO currently has 46 projects in several domains, from training to maritime and land exercises to cyber and military mobility.33 Through the European Defense Fund, the EU also has allocated 7.9 billion euros (roughly $9 billion) for the 2021-2027 period to research innovative defense products and technologies through collaborate development projects.34 But while these initiatives represent a step toward better European coordination on defense issues, they are completely reliant on political will and inter-governmental coordination — as security is not a competence of the EU but an inalienable prerogative of its member states. In fact, many of the PESCO projects appear to be severely delayed.35 U.S. experts interviewed for this research also point out the bad shape of European defense and more broadly its dependence on the United States for even more reachable defense objectives. A report from the Center for American Progress mentions the example of France’s anti-terrorism operation in the Sahel, where the U.S. ended up supporting basic air-refueling and surveillance flights.36 A detailed study by the Clingendael Institute points out that if the EU wants to be a credible actor in crisis management, primarily in its neighborhood, then it should be able to operate crossspectrum in the air, land, sea, cyberspace, and space domains — which cannot be done without more serious investments in European defense.37 The case of Afghanistan — where Europeans decided to leave after the U.S. withdrawal despite the predictable consequences on migration and political instability — offers a concrete example of such shortcomings.38 As Brookings expert Michael E. O’Hanlon points out, Afghanistan operations did not require high-tech equipment or massive resources; but the fact that European countries involved in NATO operations in Afghanistan did not step up to preserve a military presence in a crucial theater for European security speaks to their unpreparedness in terms of stockpiles of equipment and inability to conduct such operations without the help of the United States.39 Germany’s defense capabilities are also emblematic: Despite having more fiscal leeway and being at the forefront of European technological innovation, Berlin has not invested in its military, which still lacks critical equipment such as body armor, night vision gear, and helicopter spare parts.40 In this regard, evidence suggests that integrating and strengthening European defense would undoubtedly offer more openings for specialization, boost resource allocation and more broadly improve readiness. Yet such opportunities are highly contingent on building trust between allies and increasing political will, which will inevitably take time and be achieved in different ways. Recently, some inter-governmental initiatives outside of the EU and NATO frameworks were taken to tackle these shortcomings. In 2018, French President Emmanuel Macron launched the European Intervention Initiative (E2I) with the aim of deepening military cooperation between like-minded European governments sharing a strategic culture. Through intelligence sharing, scenario planning, joint planning and exercises, its 13 participants are working to strengthen their military cooperation so that they can offer rapid responses in case of a crisis. The E2I is particularly relevant because one of its members is the United Kingdom, which is not currently part of any PESCO projects. The U.K’s involvement signals the importance of the relationship and responsibilities that the it shares with European partners on security. While limited, the initiative is an example of how Europe and the U.K. can strengthen their security cooperation. As the U.K. has left the EU, stronger defense cooperation between the U.K. and the EU would also positively impact NATO through fostering synergies and interoperability. However, while relevant, these initiatives are insufficient for Europe to play a credible role as a security actor in its eastern and southern neighborhoods. And such weaknesses endanger the deterrence power of the NATO alliance against Russia and ultimately reduce the opportunities for the EU more broadly to defend its security interests.

### A2: Agent CPs Bad

#### Agent CP’s good

#### [C/I – Agent CP’s with a solvency advocate]

#### Logic – judge is a neutral policymaker who chooses the best policy. The CP tests the benefits of each. Key to cost-benefit analysis

#### Education – tests \_\_\_ key warrant of the aff

#### Neg flex – puts a structural constraint on the aff. No topic disads, infinite prep, 2ar flex proves Agent CP’s are good.

#### Reject arg not team

### A2: International Fiat Bad

#### I-Fiat’s good –

#### [Counter Interpretation – I-Fiat’s fair on foreign policy topics]

#### Info processing – test optimal actors – key to decisionmaking

#### Limits – limits affs to US key warrants – checks explosion

#### Education – key to learn about international actors and we have literature, so there is an incentive to research more.

#### Aff side bias – the topic is inherently biased against the neg – no good DAs or process counterplans.

#### Reject arg not team

# AFF ANSWERS

### Perm

#### **Perm do both -**

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

In the United States, several commentators point out that a more integrated procurement system at the European level will negatively impact U.S.-EU trade relations in the defense industry.72 Although some economic losses for the United States are indeed possible, there are ways to contain them and of course an EU with a stronger defense would make a more reliable partner for the United States. In fact, the U.S. and EU are currently discussing administrative agreements with the EDA to allow the United States to participate in PESCO projects. Through a franker dialogue, the two sides of the Atlantic could strengthen the defense market without resorting to protectionist stances on either side. This is particularly relevant considering the strong ties between the U.S. and EU defense industries; they both could benefit from deeper cooperation and exchanges on the technological level, and from free and fair competition in the trans-Atlantic defense market based on common rules and standards.

#### The perm shields the link to the China tradeoff DA

De Maio ’21 [Giovanna De Maio is a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. “Opportunities to deepen EU-NATO cooperation”. December 2021. Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2021/12/FP\_20211203\_nato\_eu\_cooperation\_demaio.pdf. Accessed 6-24-2022](https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.%20Accessed%206-24-2022); MJen]

First, the EU could be a valuable partner for the U.S. and NATO in this theater given its growing economic and regulatory power, especially related to fair-trade practices and human rights protection. Second, NATO could help promote standards and interoperability (for example, through procurement coordination between NATO and the EU as described earlier). Increased interoperability not just through NATO but also EU forces could help to quickly mobilize forces in case of conflict, as well as serve as a deterrent regarding China. The EU could also offer support through its European Peace Facility, designed to provide assistance to partner countries to increase their security and defense capabilities.83 However, regardless of the type of assistance provided, without clear rules for standardization and convergent strategies for procurement and military strengthening, the two organizations (and their member states) risk competing with one another for strategic and market advantages.

### NATO-EU Coop Fails

#### Technical impracticalities between EU states and ideological divergences mean EU-NATO cooperation fail.

Akturan et al 18, EUChicago, (Ozan Beran Akturan, Jordi Vasquez, Noah McLean, Aurore Tigerschiold, and Forrest Alonso Haydon, “”, The University of Chicago’s Chapter for European Horizons, <https://voices.uchicago.edu/euchicago/nato-eu-cooperation-transatlantic-perspectives-on-regional-security-issues/>) //CHC-DS 🐱‍👤

[Edited] for ableist langauge

However, the difference in how commitment to respective sets of values is executed in NATO and EU results with a wide portfolio of cooperational problems, ranging from bureaucratic to strategic, despite their intention to work together. Could there be comprehensive and mutually respectful cooperation between the two organizations on security issues? Would this cooperation be wearproof given the bilateral conflicts brought up by non-joint members, such as in the Cyprus dilemma? This article surveys how bilateral and regional conflicts challenge the international resolve for transatlantic security cooperation, in which NATO and EU share common milito-political interest. The European Common Security and Defense Policy: Boon or Bane The Common Security and Defense Policy (CSDP), known before 2009’s Lisbon Treaty as the European Security and Defence Policy, represented the apex of security cooperation among European Union member states and the EU’s undertaking of a heavier defence role along with NATO. The CSDP seeks to exercise European military independence from NATO within five areas: the self-assured security of the EU, a closer relationship between eastern and western Europe, structural improvement in European conflict management, cooperation between neighboring regions, and pioneering global governance of conflicts. To implement these priorities into pre-existing European structural mechanisms, the EU’s civilian-military status has undergone an updating process. For instance, the European External Action Service (EEAS) was created through the Lisbon Treaty, signed in 2007, which made the EU constitutional laws legally binding and further centralized the Union. The Lisbon Treaty also sought to address the independent methods in which the EU member states were answering international crises. When EEAS was launched in December 2010 as an EU department with the express function of consolidating EU responses to international security issues as an autonomous unit, it actualized CSDP’s vision for a new European crisis management strategy which technically compelled member states to cooperate in situations of security threats, in or out of the EU. Initiatives similar to EAAS make clear what the EU lacks has not been the incentive to incorporate an international security dimension to its agenda, but the technical practicality to implement decisions to that end in a unified manner. Although common goals had been set for NATO-EU cooperation through the Berlin Plus Agreements in 2003 before CSDP, creation of a unified transatlantic defence and security policy between the two entities has encountered ample executive difficulties. For instance, Cyprus – an EU but not NATO member- was excluded from joint EU-NATO meetings by Turkey – a NATO but not EU member- due to the decades long political antagonism over the Turkish invasion of Northern Cyprus in 1974. Even this seemingly inconsequential bilateral problem was enough to [halt]~~paralyze~~ the NATO-EU cooperation, making some organizational details of Berlin Plus Agreement impossible. Berlin Agreement’s decision to create a merged NATO-EU headquarters in Brussels to manage conflicts in which both the EU and NATO have common interests has not helped reduce the fracture between American and European politics. For instance, when France and Germany coordinated a joint gathering with Belgium and Luxembourg to protest the British-American invasion of Saddam Hussein’s Iraq, NATO and then American government denounced it as “Chocolate Summit,” betraying the spirit of cooperation aimed by CSDP. Joint NATO-EU missions for stabilization in Bosnia and Herzegovina in 2004, in Dafur, Sudan, as an assistance to African Union or in Somali to combat piracy are, however, some successful products of Berlin Plus Agreements. These joint undertakings are cases in which not all the EU or NATO members were interested in intervention, but they were made possible by sharing of military expertise and assets from either of the parties, mostly by NATO. However, post-colonial Africa and Western Balkans are regions over which NATO and EU do not have strong strategic disagreements. Despite Berlin Plus, EU has been critical of NATO’s call for joint missions in Afghanistan for instance and only supported the civilian projects of current Resolute Support Mission of NATO. Bilateral hurdles in front of NATO-EU cooperation such as Cyprus Dispute are hence not the actual root causes hindering the constructive attitude of Berlin Plus. As Europe’s disapproval of Iraqi invasion or reluctance of cooperation in Afghanistan demonstrates, the CSDP cannot overcome the strategic divergence of NATO and EU in issues of incompatible political interests. Ideological divergence of the two partners should be reconciled before the region specific problems are addressed by calls for joint military actions. The new and more NATO-conscious level of ambition for CSDP thus required European member states to invest more in security and defence, both politically and economic. Perhaps an important undertaking was revisiting Berlin Plus Agreement’s comfort in EU utilizing NATO asset and capabilities when necessary, instead initiating more EU-focused solutions like EAAS. With the attenuation of this cooperative ethos in both sides, there is a present risk that NATO and the EU will begin to compete for limited military resources, straying from the envisioned Berlin Plus Agreement. Lack of a coherent strategy among Western partners could prevent efficient response to crises, which does not bode well in a time of humanitarian atrocities — whether it be in Syria, Yemen, or South Sudan.

#### NATO-EU coop fails-- unresolved Cyprus-Turkey conflict and opposing institutional goals leave all projects in a deadlock.

Raik and Järvenpää ’17 (Dr Kristi Raik is the Director of the Estonian Foreign Policy Institute at ICDS since February 2018. She is also an Adjunct Professor at the University of Turku. Dr. Pauli Järvenpää, a former Finnish diplomat and a senior government official, joined International Centre for Defence and Security on 1 May 2013. As a Senior Research Fellow at ICDS, he focuses on the security of the Baltic Sea and Nordic region and on issues related to NATO, the EU and transatlantic cooperation, as well as on the security and development of Afghanistan. “A New Era of EU-NATO Cooperation How to Make the Best of a Marriage of Necessity,” International Centre for Defense and Security, May 2017, <https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf)-> HL

In spite of the promising start that created a solid framework for cooperation, by the early 2010s the EU-NATO relationship had produced very limited tangible results and was mired in structural obstacles. The main impediments, especially at the operational level, were created by the standoff between Cyprus and Turkey over the unresolved conflict on Cyprus. Furthermore, there was a tendency on both sides to see the relationship between NATO and the CSDP in terms of competition – even as a zero-sum game – which obviously did not encourage cooperation.21 Since its accession to the EU in 2004, Cyprus has put brakes on Turkey’s accession negotiations and blocked its participation in EUled missions, membership of the EDA and generally a more active role in CSDP. At the same time, Turkey has been able to block the use of NATO capabilities and assets by the EU and has not allowed the participation of the Republic of Cyprus, which it does not recognise, at formal EU-NATO meetings. Hence, meetings between the North Atlantic Council and the PSC have been held rarely (the latest took place in September 2015) and with a narrow agenda.22 This deadlock practically turned the Berlin Plus arrangements into a dead letter and 21. Drozdiak 2010. It should also be said that the Americans were not at that point particularly helpful. 22. In the 18 months to August 2015, four PSC-NAC meetings were organised: one formal meeting on EUFOR Operation Althea, two informal meetings on Ukraine, and one informal meeting on the eastern and southern neighbourhoods. See Dakic 2015. prevented more ambitious strategic cooperation. Berlin Plus arrangements have been used only for two operations: Operation Concordia in the Former Yugoslav Republic of Macedonia (FYROM), which ended in September 2003, and EUFOR Operation Althea in Bosnia and Herzegovina, an operation deployed since 2004. While formal cooperation was limited, in practice a division of labour in crisis management took shape, roughly along the lines of soft/civilian and hard/military security. Although the CSDP was created to carry out both civilian and military crisis management tasks, the EU did not become the preferred instrument for more ambitious military operations. Member states limited the use of CSDP to softer, non-combat operations, whereas NATO took care of militarily more demanding environments and combat tasks. This division was evident in the two locations where both organisations had an operation running simultaneously: Kosovo and Afghanistan. Staff-level cooperation between the missions on the ground worked reasonably well, thanks to individual efforts to find flexible and creative ways to work around the formal obstacles.23 It was also a setback to the CSDP that EU Battlegroups were never deployed due to the lack of political will to actually use this new tool. One of the hurdles was the reluctance of member states to finance their deployment. As of today, discussions on improved usability and more effective financing of the Battlegroups continue, but the issue has been pushed down the list of priorities by new, more promising areas of defence cooperation, to be described below. Apart from the structural hurdles, the EU side was simply not very interested in close cooperation. The EU nurtured an ambition to be a different kind of international actor, described as a civilian, normative, ethical or soft power.24 This aspiration favoured taking a step back from NATO, characterised by many as a relic of the Cold War that was struggling to find a new purpose.25

#### Bureaucratic procedures, misalignments, and overlap tank coordination.

Soare 21, Simona R. Soare was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest, “Innovation as Adaptation: NATO and Emerging Technologies”, German Marshall Fund, https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies)

The Biden administration also provides a window of opportunity to progress and be ambitious in broadening and regularizing NATO-EU cooperation in the field of innovation and EDTs. While political dialogue among their leadership has been steadily increasing over the past five years, the EU and NATO have consulted on their respective EDTs agendas only twice. Furthermore, bureaucratic procedures and misalignments sometimes frustrate even staff-to-staff cooperation in this area. The EU and increasingly NATO are proliferating agencies that conduct work on innovation in EDTs, including in security and defense. This makes it challenging to achieve internal coherence of activities within one organization, let alone coordinating agendas between the two.

#### It fails – duplicity, internal divisions, and empirics.

ND 22 [New Direction, 05-22-2022, "Why an EU Army is a bad idea – We don’t need a political bloc of the unwilling", https://newdirection.online/the-european-journal/article/why\_an\_eu\_army\_is\_a\_bad\_idea\_we\_dont\_need\_a\_political\_bloc\_of\_the\_unwilling, DOA: 6-23-2022 //ArchanSen]

You might argue that it can only be a good thing if the Europeans step up their defence arrangements. But this has little to do with increasing military muscle. It is not the answer to the plea by successive US presidents for the Europeans to do more on defence. NATO is well established, well proven and credible. 27 of its 30 member countries are European, including 21 that also happen to be EU countries. So why create another structure? Any EU force would have to draw on the same limited military resources and would be a duplicative, divisive distraction. EU ambitions already intrude into NATO where coordination structures between the two organisations have now been set up, in spite of the fact that their membership is largely the same. The EU wants to become the European leg of NATO – so where would that leave key non-EU European members of NATO such as the UK, Norway and Turkey? In any case, the EU countries can’t even agree among themselves. Many pay lip service to the idea of CSDP while refusing to participate in any meaningful way. Even the arch-federalist European Parliament, in its most recent report on EU defence, noted that “in over 15 years of existence EU battlegroups have never been used, in particular due to the lack of political consensus among Member States and the complexity of implementation and funding…” At NATO HQ in the early ‘90s, the French were already pushing for European military capabilities separate from NATO. When the Bosnian crisis began they demanded that the matter should be discussed not at NATO but ‘in another place’ – by which they meant the Western European Union (WEU), a purely European group whose headquarters was just down the road in central Brussels. As a consequence, nonsensically, two allied navies operated in the Adriatic and Mediterranean, one under NATO command and the other under WEU, with more or less the same ships rotating between the two. Once the Bosnian military operations got more serious, even France gave up on this farce and backed the NATO option.

### EU Weak

#### EU initiatives fail and they’re too weak – this is the 1nc author!

De Maio ’21 (Giovanna was a nonresident fellow in the Center on the United States and Europe at Brookings. She is currently a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. She holds a doctorate in international studies from the University of Naples, “OPPORTUNITIES TO DEEPEN NATO-EU COOPERATION”, December 2021, Brookings Institute, <https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf>)

Yet NATO-EU cooperation remains somewhat limited because of political tensions between member states (which hinders intelligence sharing) as well as weak European military capabilities and inadequate defense spending. Over the past few years the EU has made important progress in this domain through the establishment of the European Defense Fund and several defense projects under the Permanent Structure Cooperation (PESCO) mechanism. Yet, according to several studies in the field, the state of European defense appears insufficient to tackle more serious military threats or to enable the EU to take initiatives in its neighborhood independently from the United States. In its “Strategic Compass” to be published in March 2022, the EU is supposed to adopt a bolder approach to its defense capabilities. In parallel, in a new strategic concept to be released in June 2022, NATO is supposed to tackle security throughout a widened angle, looking at domains that are not strictly defense-related.

#### EU doesn’t have the expertise

Lawrence and Cordy 20, \*Christie Lawrence is a Director for Research and Analysis working on international AI cooperation and intellectual property. Prior, she worked at Harvard Belfer Center’s Cyber Project, the State Department, and as a management consultant. She holds a B.A. in Public Policy from Duke University and is a concurrent MPP/JD candidate at Harvard Kennedy School and Stanford Law School. \*\* Researcher, Center for Security Studies, ETH Zurich. Koichiro Komiyama – Director, Global Coordination Division, JPCERT/CC, (Christie and Sean, “The Case for Increased Transatlantic Cooperation on Artificial Intelligence”, Belfer Center, https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence)

The European Union’s Juncker 26 Commission (2014-2019) actively avoided regulating AI, causing the European Parliament to increase their efforts as a proactive voice in favor of stronger AI regulation. However, since the beginning of Ursula von der Leyen’s tenure, the Commission has initiated efforts to adopt stronger regulation for AI applications (i.e., differentiating regulation of AI based on defined “high-risk” and “low-risk” sectors”) and associated data spaces.27,28 These legislative proposals and their associated discussions are planned to be completed by the end of 2020. During the strategic planning and budgeting process of its R&D programs, the EU committed to providing at least EUR10.7 billion29 for AI-related research conducted between 2021 and 2027.30 Despite these financial and political efforts, the EU still remains technologically dependent on the US and China and suffers from a lack of capital and private funding, decentralized and uncoordinated AI expertise, severe brain drain (including to the US), and slow adoption of AI programming in its education and public sectors.

#### Only the US can do security cooperation with NATO on AI---EU is far behind on funding, adoption, and private investment.

Christie 22, Senior Research Fellow for the Finnish Institute of International Affairs, Research in the areas of International Affairs and International Security, with a particular focus on: Geoeconomics, Economic Statecraft, Defence Economics, Defence Innovation, Artificial Intelligence, NATO, Great Power Competition., (Edward Hunter, “Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe” in *European View*, Volume 21(1), Wilfried Martens Centre for European Studies, https://journals.sagepub.com/doi/pdf/10.1177/17816858221089372) //CHC-DS 🐱‍👤

Before proceeding, it is worth spelling out the extent to which European security is dependent on NATO and in particular on the US. Of the EU’s 27 member states, 21 are members of NATO. These countries account for about 93% of the population1 of the EU. Within NATO, those Allies that are also EU members only account for about 20% of total defence expenditure across the Alliance, while the US alone accounts for about 70% of the same total.2 Beyond these aggregate indicators, it is furthermore the case that the US is considerably ahead of the EU in terms of practical adoption of AI. For illustration, in 2020 US private-sector investment in AI was around $23.6 billion, but was only $2 billion in the EU, implying a ratio of 12 to 1 in favour of the US (Zhang et al. 2021, 96). Scientific output indicators offer a more nuanced picture. In 2019, the EU accounted for 16.4% of the world’s peer-reviewed AI publications, ahead of the US with 14.6%, while China occupied the top spot with 22.4% (Zhang et al. 2021, 20). On the other hand, if one measures research output in terms of publications on the Arxiv database, the US is ahead of the EU (Zhang et al. 2021, 33) by a ratio of almost two to one, which is nonetheless much less than the large gap in private investment mentioned above. That the EU performs similarly to the US in terms of scientific research, but far less well in terms of investment and commercialisation of new digital technologies, is an old problem which has proven very difficult to address, whether at national or EU level (Baroudy et al. 2020).

### No Cyber Solvency

#### The EU will seek commercial advantages on AI which undermines broader cooperation.

Franke 21, Dr. Ulrike Franke is a senior policy fellow at the European Council on Foreign Relations (ECFR), “Artificial divide: How Europe and America could clash over AI”, European Council on Foreign Relations, <https://ecfr.eu/publication/artificial-divide-how-europe-and-america-could-clash-over-ai/#why-work-together-disagreements-and-shared-goals>)

The EU’s effort to strengthen ethical AI, and to make ‘trustworthy AI’ a unique selling point for Europe, might also end up creating problems for transatlantic cooperation. Many EU policymakers believe that the EU’s insistence on ethical AI will eventually become a location advantage for Europe (much like data privacy): as more people become concerned about unethical AI and data security, they will prefer to use or buy AI ‘made in Europe’ rather than elsewhere. In this respect, two European aims are at odds with each other: on the one hand, Europeans want to ensure that AI is developed and used in an ethical way. Partnering with a powerful player such as the US on this matter should be an obvious way to help them achieve this goal. However, if the EU considers ethical AI not just a goal for humanity but a development that may also create commercial advantages for Europe, then transatlantic cooperation on this issue is counterproductive, as it would undermine Europe’s uniqueness.

### No NB

#### NB is non-unique – Squo solves EU autonomy---E12 and NORDEFCO.

Retter et al 21, 1) Lucia Retter is a research leader at RAND Europe and co-directs RAND Europe's Centre for Defence Economics and Acquisition, M.A. in international relations and international economics, The Johns Hopkins University School of Advanced International Studies (SAIS); B.A. in modern and medieval languages, University of Cambridge, 2) Stephanie Pezard is a senior political scientist at the RAND Corporation, Ph.D. in political science, Graduate Institute of International and Development Studies, Geneva; M.A. in history, French Institute of Political Science, Paris (Sciences Po); M.A. in political science, Graduate Institute of International and Development Studies, Geneva; B.A. in history, French Institute of Political Science, Paris (Sciences Po) 3) Stephen J. Flanagan is an adjunct senior fellow at the RAND Corporation. Ph.D. in international relations, Fletcher School, Tufts University; A.B. in political science, Columbia University 4) Gene Germanovich is an international defense researcher and currently serves as the acting international portfolio lead for the RAND National Security Research Division. B.S. in international affairs, Georgia Tech; M.A. in security studies, Georgetown University 5) Sarah Grand-Clement; publisher, 6) Pauline Paillé is an analyst at RAND Europe working in the area of defence and security. M.A. in international relations, Sciences Po Bordeaux (“European Strategic Autonomy in Defence: Transatlantic visions and implications for NATO, US and EU relations”, RAND Europe, https://www.rand.org/pubs/research\_reports/RRA1319-1.html) //CHC-DS 🐱‍👤

In addition to these overarching EU initiatives, a number of separate bi- and multi-lateral groupings and frameworks have also emerged in the last 10 to 15 years, aiming to unite like-minded nations in pursuit of greater defence integration. This trend further confirms that EU member states and partners recognise that, individually, their defence capabilities are insufficient to independently deliver most, if not all, defence missions and that collaboration and harmonisation are necessary. Under the leadership of French President Macron, for example, the European Intervention Initiative (EI2) was launched in 2018 to be an agile, nonbinding, voluntary forum, among the most capable European governments willing to employ their military forces, complementary both to the EU (including PESCO) and NATO.88 The EI2 seeks to deepen cooperation in four areas: intelligence sharing and strategic foresight, planning and scenario development, support to operations and lessons learned.89 In practice, the initiative consists of meetings between the militaries of participating member states and periodically at the ministerial level.90 In Northern Europe, for example, Denmark, Finland, Iceland, Norway and Sweden take part in the Nordic Defence Cooperation (NORDEFCO), a political and military framework that establishes cooperation in five areas: capabilities, armament, human resources and education, training and exercises as well as operations. The aim of NORDEFCO is to increase interoperability between those five members, develop a common understanding in these areas and optimise the use of their resources based on their common strategic culture.91 In addition, members of the Northern Group, including 12 countries bordering on the Baltic or North Sea, have been working to deepen regional defence and security cooperation including on information sharing, exercises and military mobility.92

C

### Agent CPs Bad

#### Agent CPs are a Voting Issue –

a) Topic education – agency debates are not grounded in the resolution – kills debate about military presence.

b) Aff ground – moots the 1AC and makes it impossible to garner offense – they open the floodgates for an infinite number of unpredictable counterplans

c) Read the CP as a DA – solves their offense

### International Fiat Bad

#### International Fiat is a voting issue –

--Not an opportunity cost – the judge is the US – logical decision making is the portable impact of debate

--CP justifies infinite intrinsicness because it expands the ambit of the judge – means we get to permute their DAs

--Fairness – impossible to research every possible actor – kills clash. And pressure CPs and international DAs solve their offense