Introduction

For decades, the EU and NATO have guaranteed security, stability and prosperity in Europe. In 2016 and 2018, both organizations agreed on two joint declarations in which provisions were spelled out to work closer together. On the basis of these declarations, a more structured relation was established, which paved the way for a new cooperative momentum. These documents, not only signalled the will to strengthen political dialogue but also how to move forward in the strategic and operational domains. This is particularly meaningful at a time when both Europe and the US are challenged by significant geopolitical realities. Both organizations face revisionist foreign policies of authoritarian states, the rise of illiberal democracies, intractable conflicts in the near abroad, strategic competition among international actors, and the effects of emerging and disruptive technologies and disinformation.

The EU-NATO joint declarations set the course are of cooperation rather than competition, and complementarity rather than duplication in the Euro-Atlantic area. They also offered the opportunity for each organization to further develop what each one does best, whether that is crisis management, deterrence, or collective defence. By pooling sovereignty and sharing defence resources, the EU and NATO have much to contribute to international and regional stability. Both organizations also have different means to uphold a rules-based international security order, by making use of their distinct security and defence instruments and resources.

Of the 47 areas of cooperation agreed upon, four are of particular relevance in the current strategic context, to which the Portuguese Presidency of the Council of the European Union has dedicated a special focus. First, the idea that the EU and NATO must improve cooperation over the management of complex emergencies, from public health risks to extreme weather events. Second, in the fight against cyber and hybrid threats, the EU and NATO should look for an appropriate balance between legal measures and procedures on the one hand, and deterrence on the other hand. Third, maritime security cooperation between the EU and NATO off the coast of Somalia and in the Mediterranean, has proven successful on land and at sea, and this experience should continue in those scenarios and beyond, whenever Euro-Atlantic interests are at stake. Fourth, in order to effectively respond

to emerging crises, it is important to rapidly deploy capabilities and forces over larger distances, which underlines the relevance of further developing military mobility and improving regulations and civilian-military infrastructure across Europe.

With the aim of tackling these issues, providing an assessment of ongoing inter-organizational relations and identifying existing opportunities, the National Defence Institute (IDN) organised a high-level conference on 15 February 2021, under the framework of the Portuguese Presidency of the Council of the European Union. The event took place under Chatham House rule and examined the complementarity between the two organizations as well as how the Common Security and Defence Policy (CSDP) and NATO can best strengthen the Euro-Atlantic region. The event gathered 400 registered participants from governments, EU institutions, academia and think tanks. This report outlines the main conclusions of the conference.

EU-NATO Cooperation – Political and Strategic Challenges

Sub-strategic cooperation

The Joint Declarations of 2016 and 2018 provided considerable momentum for the institutionalization and operationalization of the EU-NATO partnership. However, while a lot has already been achieved, EU-NATO cooperation remains, for the most part, ad-hoc and sub-strategic. One of the main problems standing in the way of a strategic level partnership concerns the lack of a clear division of labour between both organizations. A clearer debate and definition over who does what and when, is essential to remedy this situation. To that end, increased compatibility between European defence efforts and NATO needs to be ensured, to enable further burden sharing and make European strategic autonomy compatible with NATO aims. Proposals for a better division of labour range from strengthening the conventional line of defence in Europe against possible external aggressors, establishing a permanent European strategic presence in the Mediterranean, to more explicitly linking the EU's Capability Development Plan (CDP) with the NATO Defence Planning Process (NDPP).

However, the informal nature of EU-NATO cooperation hinders any proposals of the sort given the reduced likelihood of a review of the Berlin Plus Agreement due to difficult relationships between

some member states (e.g. Greece, Cyprus, Turkey). For this reason, the EU and NATO should focus on advancing cooperation on more depoliticized issues such as resilience, capacity building, and training. Yet, it is also important to bear in mind that while these areas are important for channelling additional cooperation, real strategic impact cannot be achieved solely through informal channels. Meaningful political commitment is a prerequisite for further cooperation and the political timing should be seized, particularly in terms of the ongoing review processes concerning the EU's Strategic Compass and NATO's Strategic Concept.

Transatlantic relations

The advantages and disadvantages of informal inter-organizational cooperation are closely related to the complex relations between member states and allies. The two Joint Declarations, released at a time of tension between the US and its European allies, became symbols of important advances, but considerable difficulties in the transatlantic relation remain. Primarily, while it is argued that the US should dialogue with the EU as a whole, EU-NATO cooperation cannot and should not be solely understood as a two-player game. That is best exemplified by the diverging positions within the EU over its own defence developments and compatibility with NATO, as well as by the different priorities of the Member states regarding EU-NATO cooperation, which are partly attributed to not all states being members of both organizations.

In this context, the work carried out under the framework of the Strategic Compass may function as an enabler for further inter-organizational cooperation, as it creates a common European position that could be used to expand the debate on the upcoming revision of NATO's Strategic Concept. Hence, not only should the EU and the US forge a deeper common understanding of the current world order and how to best manoeuvre in it, but the EU should also work towards building more productive relations with third countries that are NATO members (e.g. Turkey) in order to avoid lingering tensions reflected on the EU-NATO partnership as a whole.

Countering Disinformation and Hostile Propaganda

Complex cross-domain threats

Disinformation and hostile propaganda need to be understood and analysed in the wider context of multilayered hybrid threats that occur in different political, social, and economic situations. In order to fully grasp and assess the goals of hybrid actors and the threat they represent it is necessary to adopt a more holistic approach, which considers the geopolitical, historical, and cultural contexts, and simultaneously monitors developments in a wide range of domains. Hybrid threats are not a new phenomenon, but they resort to new and more effective means associated with the development and use of new technologies, such as social media and artificial intelligence, which entails reaching broader audiences with lesser costs and lower risks of retribution after each attack. It is expected that highly effective disinformation generated by artificial intelligence, designed to target individuals based on their profiles, may become dominant in the future, posing even greater risks and challenging even more the resilience of democratic societies.

In order to deter this kind of hybrid threats, there is a need for more effective countermeasures that strengthen the resilience of states and societies. However, for these to work, they have to be comprehensive, engaging society as a whole by raising awareness and fostering education. Possible measures to fight disinformation may include working directly with social media platforms, both in regulatory and non-regulatory terms, by providing terms of service, duty of care and legally defining what type of content should be removed, instead of letting the platforms define it on their own terms. There is also a need for increased proactivity against these threats, which requires considerable political will. Accordingly, recent guidelines such as the European Democracies Action Plan, and more specifically the Digital Services Act, comprise important steps in the right direction.

Common understandings

Since the 2016 Joint Declaration, EU-NATO cooperation on hybrid threats has progressed significantly, as evidenced by the ensuing activities of the EU INTCEN's Hybrid Fusion Cell and NATO's Hybrid Analysis Branch, through regular staff-to-staff exchanges, joint hybrid exercises, or the collaboration promoted by the European Centre of Excellence for Countering Hybrid Threats

(Hybrid CoE). Understanding that hybrid activities present a common threat to all Member states and allies, together with the additional dangers of disinformation that the COVID-19 pandemic has exposed, further reinforces the case for the development of more substantial cooperation programs in this domain.

However, it is necessary to overcome crucial obstacles such as the impossibility to share classified information between both organizations, as well as diverging understandings on key concepts and existing approaches to hybrid threats. In order to devise more effective countermeasures, the EU and NATO must share and generate a more common knowledge over the impact of these threats. Together with formal cooperation mechanisms, which largely depend on political will, less formal initiatives could potentially facilitate the creation of new common routines and processes that enhance mutual response capabilities.

Cooperation in Cyber Space

Global transitions

The transition from a US-led liberal order to a post-liberal word is being driven by contestation of power relations, values and institutions. Cyber space is at the centre stage of this contestation, given how it has been dominated by Western norms, values and institutions since its very inception. Hence, there is a growing push for a balancing act, in which major players use cyber capabilities to advance their interests, but in which smaller powers also use cyber tools to try and punch above their weight. The growing influence of non-state actors (e.g. proxy hackers and international companies) needs to be considered as well. Disagreement is also visible between countries that defend an open and free internet, and those that defend cyber sovereignty. Countries like China contest pre-existing governance models, because they do not give enough power to governments, preferring instead a more state-based regulatory system.

In this global context, it is possible to identify five issues standing in the way of further EU-NATO cooperation vis-a-vis the ongoing global power shift. The first deals with how to best promote relevant intelligence sharing between the two organizations. The second concerns the need to avoid duplication of resources or functional overlapping. The third has to do with the potential lack of

institutional flexibility to handle a fast-pacing international context. The fourth concerns potential factual irrelevance of new initiatives, given how decisions are made or events are taking place outside the framework of each organization. Finally, the possibility that both organizations misunderstand their role in a post-liberal world, in which cyber grey zones will lead to more difficult operational responses over how to respond to a potential attack can also further constrain EU-NATO cooperation. Overall, the bulk of cyber activities are taking place below the military threshold, for which NATO is not equipped for, but also beyond a level that the EU is not yet ready to address.

Opportunities for institutional cooperation

The EU's Cybersecurity Strategy for the Digital Decade calls for a multi-stakeholder approach that builds upon multilateral processes. This comes as a recognition of the need for a strategic framework for conflict prevention and cooperation, that allows for both the applicability of international law and the adoption of norms of state behaviour and confidence-building measures. However, even though international law on cyber space is supported by the EU, not all NATO members share a common understanding of what constitutes, for instance a violation of sovereignty following a cyberattack. The norms on responsible state behaviour, endorsed by the UN General Assembly in 2015, can therefore provide an important starting point, given how any work needed for new international regulations may have difficulty in striving in the current geopolitical environment.

More inter-organizational dialogue and exchanges between the EU and NATO could also pave the way to avoid duplication of efforts and to better cover the whole spectrum of issues, including leadership in digital transformation, or protection of individual rights and online freedoms. Further cooperation is also possible in terms of dealing with the entanglements of cyber, hybrid and information influence operations. On the one hand, these three areas question the institutional setting and division of labour in both organizations, as well as existing official structures of Member States. On the other hand, any joint approach requires rigorous delineation on how to address these challenges, the means that should be used in the respective responses, and whether or not they should fall under a civilian or military oversight.

Main takeaways

- The lack of a clear division of labour has deprived the EU-NATO relation of meaningful strategic direction. Taken together, the Strategic Compass and the revision of NATO's Strategic Concept provide an opportunity to revisit and eventually review responsibilities, focusing on the comparative advantages of both in each particular domain.
- Excessive informality in cooperation comprises an obstacle to improved formalization of the partnership. Inversely, any revision of existing legal arrangements beyond the Berlin Plus Agreement is unlikely due to lingering disputes between Greece, Turkey and Cyprus.
- Further cooperation should be encouraged in areas such as resilience, capacity building and training.
- EU member states could align their positions following the adoption of the Strategic Compass in order to project a common position during the upcoming revision of NATO's Strategic Concept.
- Hybrid threats need to be understood beyond disinformation alone and be analysed in a holistic format.
- In order to fight disinformation through resilience, societies have to be engaged as a whole by means of comprehensive strategies. Ideally, this should bring together civilian and military elements, media literacy education and regulation, but also intelligence analysis.
- Existing limitations on information sharing hinder more cooperation between the EU and NATO. Informal venues are valuable only if they facilitate common routines and processes, and encourage a common understanding of the threats and their corresponding approaches.
- Proactivity is key as the adversary is constantly looking to exploit existing weaknesses, while regulation and deterrence are crucial for prevention.
- Ongoing international shifts are grounded by overall contestation over power relations, values, and institutions, with a direct reflection on developments in cyber space.

- The bulk of cyber malicious activities take place below the military threshold, for which NATO is not equipped, but also beyond a level in which the EU is not yet fully ready to commit.
- Existing international law provisions on cyber space, including norms on responsible state behaviour, should be further supported, as the work required for new overall regulations would not be compatible with the current geopolitical environment.
- Understanding cyber, hybrid and information influence operations requires questioning the institutional setting and division of labour in both organizations, but also calls for careful delineation on how to address these challenges, the means used in the respective responses, and whether or not they should primarily fall under civilian or military oversight.

Recommended readings

On EU-NATO cooperation

Biscop, S., 2020. The Future of the Transatlantic Alliance: Not Without the European Union. *Strategic Studies Quarterly*, pp. 81-94. Available at: https://www.egmontinstitute.be/content/uploads/2020/09/Biscop-nato-alliance.pdf?type=pdf.

Drent, M., Kruijver, K., and Zandee, D., 2019. *Military Mobility and the EU-NATO Conundrum*. The Hague: Clingendael. Available at: https://www.clingendael.org/sites/default/files/2019-07/Military_Mobility_and_the_EU_NATO_Conundrum.pdf

Latici, T., 2020. *Understanding EU-NATO cooperation: Theory and practice*. Brussels: European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659269/EPRS_BRI(2020)659269_EN.pdf

NATO Council, EU Council. 2020. *Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. Available at: https://www.consilium.europa.eu/media/44445/200616-progress-report-nr5-eu-nato-eng.pdf

On hybrid threats

European Commission, 2020. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan (COM/2020/790 final).* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423

Keršanskas, V., 2021. *Deterrence: Proposing a more strategic approach to countering hybrid threats*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

Pamment, J., 2020. *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. Future Threats, Future Solutions #1. Brussels: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf

Pamment, J., 2020. *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework*. Future Threats, Future Solutions #2. Brussel: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

On cyber space

Barrinha, A., and Renard, T., 2017. Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4-5), pp. 353-364. Available at: https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924.

European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 2020. *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade (JOIN/2020/18 final*). Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

Latici, T., 2020. *Understanding the EU's approach to cyber diplomacy and cyber defence*. Brussels: European Parliamentary Research Service Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651937.

Lété, B., and Pernik, P., 2017. *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. German Marshall Fund of the US, Policy Brief n. 38. Available at: https://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions.