Countering hybrid threats

Steps for improving EU-NATO cooperation

Dick Zandee
Sico van der Meer
Adája Stoetman

Clingendael Report

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Countering hybrid threats

Steps for improving EU-NATO cooperation

Dick Zandee
Sico van der Meer
Adája Stoetman

Clingendael Report
October 2021

Disclaimer: The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

October 2021

About the Clingendael Institute

The Netherlands Institute of International Relations 'Clingendael' is a leading think tank and academy on international affairs. Through our analyses, training and public platform activities we aim to inspire and equip governments, businesses, and civil society to contribute to a secure, sustainable and just world.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

About the authors

Dick Zandee is Head of the Security Unit and Senior Research Fellow at the Clingendael Institute. His research focuses on European security and defence issues, EU-NATO, military forces and capability development, defence industry and other security topics.

Sico van der Meer is a Research Fellow at the Clingendael Institute. His research focuses on non-conventional weapons such as Weapons of Mass Destruction (nuclear, chemical, biological) and cyber weapons from a strategic policy perspective.

Adája Stoetman is Junior Researcher at the Security Unit of the Clingendael Institute. Her research focusses both on security and defence as well as strategic foresight. Her area of expertise is international security, with a specific interest in European defence cooperation.

Contents

1 Introduction

In recent years the word 'hybrid' has dominated the debates on security and defence. Much has been written about hybrid peace, hybrid conflict and hybrid warfare. Cyber-attacks, disinformation and election interference: these are just three often cited examples of hybrid threats. Western countries are struggling with the question of how to respond to these threats, in particular as military responses alone are insufficient and inappropriate to deal with such challenges. A whole-of-government or even a whole-of-society approach is required, as hybrid threats are targeted at wider governmental infrastructure, at privately-owned entities and at citizens at large or at specific organisations.

Countering hybrid threats has also become a priority on the EU and NATO agendas as both organisations and their member states are confronted with 'sub-threshold' or 'grey zone' challenges. In 2016, when both organisations agreed on a list of topics for EU-NATO cooperation, countering hybrid threats was selected as one of the important fields of action. Correspondingly, in 2016 and 2017 the EU and NATO drafted at least 22 concrete proposals for enhancing cooperation in the area of countering hybrid threats. Since then, both organisations have issued six progress reports with an overall positive assessment of their cooperation, but it remains unclear what has actually been achieved. This begs the question which concrete results have the EU and NATO produced? This report will analyse the progress made so far and will provide – based on the analysis – ideas and suggestions for further improving EU-NATO cooperation in the area of countering hybrid threats.

Hybrid is one of the new buzzwords, but the question remains what constitutes 'hybrid threats'. Chapter 2 provides an overview of some of the definitions used. In the subsequent chapter 3 the authors assess the results of EU-NATO cooperation in the field of countering hybrid threats, drawing from that analysis the reasons for 'what works' and 'what does not work' (or 'does not work to the full extent'). Based on the outcome of what has been achieved, the fourth chapter points to the potential for 'what could be further achieved'. Taking into account the (political) limitations of EU-NATO cooperation, this chapter also looks at the potential for alternative cooperation formats. The fifth and final chapter draws conclusions and provides recommendations for action to improve EU-NATO cooperation in countering hybrid threats.

The underlying methodology of this report consists of the combination of analysing the relevant literature and other written, publicly available sources, and conducting interviews with EU and NATO officials. Interviews were conducted in the time period June-August 2021, under the application of the Chatham House Rule.

2 Hybrid threats: searching for a definition

The term 'hybrid' has become a mainstream word in recent years. We drive hybrid cars, golfers hit balls with hybrid clubs and, increasingly, houses are equipped with hybrid heating systems. The term 'hybrid' originates from biology, meaning "a plant or animal that has been produced from two different types of plant or animal especially to get better characteristics". In general terms it is "something that is a mixture of two very different things".[1] When applying this to (security) threats, this would indicate a mixture of military and non-military challenges. As such, this is nothing new: other terms have been used in the past for the same meaning; 'hybrid' is just the new buzzword.[2] However, as yet, no widely accepted definition of 'hybrid' threats or activities exists. Diverging definitions circulate, even within the EU and NATO. A few examples:

The EU's 'Joint Framework on Countering Hybrid Threats' states that[3]:

"While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare".

The EU External Action Service (EEAS) uses the following definition[4]:

"Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive

1 Definitions from the Cambridge Dictionary.

2 Hugo Klijn & Engin Yüksel, Russia's hybrid doctrine: is the west barking up the wrong tree?, (The Hague: The Clingendael Institute, 29 November 2019).

3 European Union, 'Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council, EU Document JOIN(2016) 18 final, 6 April 2016.

4 European External Action Service, A Europe that Protects: Countering Hybrid Threats (Factsheet), 13 June 2018.

and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion to hinder swift and effective decision-making".

NATO uses the following definition[5]:

"Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies".

Last but not least, the European Centre of Excellence for Countering Hybrid Threats[6], also known as the Hybrid Centre of Excellence, or Hybrid CoE – an international, network-based organisation in Helsinki that also serves as a platform between the EU and NATO providing a forum for strategic discussions and joint training and exercises – defines hybrid threats as follows[7]:

"Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means; Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international); Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target".

There are clear similarities between these definitions: for example, they all describe hybrid threats as a combined use of military and non-military means to undermine societies. Yet, discussion is possible on which activities can and cannot be included within the concept of hybrid threats. For example, the EU's 'Joint Framework on Countering Hybrid Threats' includes a very broad area of activities to counter hybrid threats, demonstrating the broadness of the field. The frameworks lists:

- strategic communication to counter the systematic spread of disinformation;
- protecting critical infrastructures (e.g. energy supply chains, transport) from unconventional attacks (which in the description includes very broad policy goals such as further diversifying the EU's energy sources, suppliers and routes, transport

5 NATO, NATO's response to hybrid threats, 2 July 2018.

6 For more information on the Hybrid Centre of Excellence and its tasks, see: Hybrid Centre of Excellence, About us.

7 The European Centre of Excellence for Countering Hybrid Threats, Hybrid threats as a concept.

and supply chain security, but also protecting infrastructure in space from hybrid threats, as well as increasing defence capabilities in general);
- protecting public health and food security (including protection against CBRN threats);
- enhancing cyber security (with a special focus on industry, energy, financial and transport systems);
- targeting hybrid threat financing; and building resilience against radicalisation and violent extremism.[8]

The EEAS also includes cyber threats within the scope of hybrid threats, and adds that "Chemical, Biological, Radiological and Nuclear (CBRN) threats delivered by non-conventional means fall within a category of their own" while still including them within the category of hybrid threats.[9]

Turning to policy documents regarding EU-NATO cooperation in countering hybrid threats, there is no unambiguous perspective either. The 'Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization' of December 2016, followed by an additional set of proposals in 2017, lists four categories of action within the section 'Countering hybrid threats': Situational Awareness, Strategic Communication, Crisis Response, and Bolstering Resilience.[10] 'Cyber security and defence' is a separate category, apart from hybrid threats, and CBRN threats are not mentioned at all.[11]

All in all, it is clear that the term 'hybrid threats' has no unambiguous definition and will be continuously evolving depending on the circumstances and debates.[12] As there is no widespread consensus on the definition, this report will use the 2016 and 2017 sets of proposals for EU-NATO cooperation as a starting point; these sets have not been

8 European Union, 'Joint Framework on countering hybrid threats, a European Union response', Joint Communication to the European Parliament and the Council, EU Document JOIN(2016) 18 final, 6 April 2016.

9 'A Europe That Protects: Countering Hybrid Threats', EEAS Factsheet, June 2018.

10 Council of the European Union, 'Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization', EU Document 15283/16, 6 December 2016.

11 Council of the European Union, Council conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, EU Document 14802/17, 5 December 2017; and information from interviews.

12 For a more detailed discussion of the concept of hybrid threats, see: G. Giannopoulos, H. Smith & M. Theocharidou, The Landscape of Hybrid Threats: A Conceptual Model (Public Version), Joint Research Centre European Commission, 2021.

changed since then. The focus will primarily lie on the sections on 'countering hybrid threats' and 'cyber security and defence'. Even though 'cyber security and defence' is included in the set of proposals as a separate category alongside 'Countering hybrid threats', generally cyber threats are considered to be a main part of hybrid threats. For that reason, they are included in this study. The justification for focusing solely on the 2016 and 2017 sets of proposals derives from the scope of this study: EU-NATO cooperation in the field of countering hybrid threats. Therefore, the analysis of what has been achieved so far in this area of EU-NATO cooperation (chapter 3) is narrowed down to those fields that have officially been included as cooperation areas between both organisations.[13]

13 Although the 2016 and 2017 sets of proposals also include counterterrorism as well as gender issues under the category of 'situational awareness' with regard to hybrid threats, these two topics will not be dealt with in the current report, because they are not mentioned under the actual categories of hybrid threats in the proposals.

3 EU-NATO cooperation: what has been achieved so far?

Acknowledging the need for increased cooperation between the EU and NATO is not something new but has gained momentum in recent years. This is particularly true since the EU and NATO are redefining their roles in light of changing security challenges. The EU's Joint Communication on Countering Hybrid Threats from April 2016 and the EU Global Strategy of June 2016 already emphasised the need for a strengthened partnership with NATO.

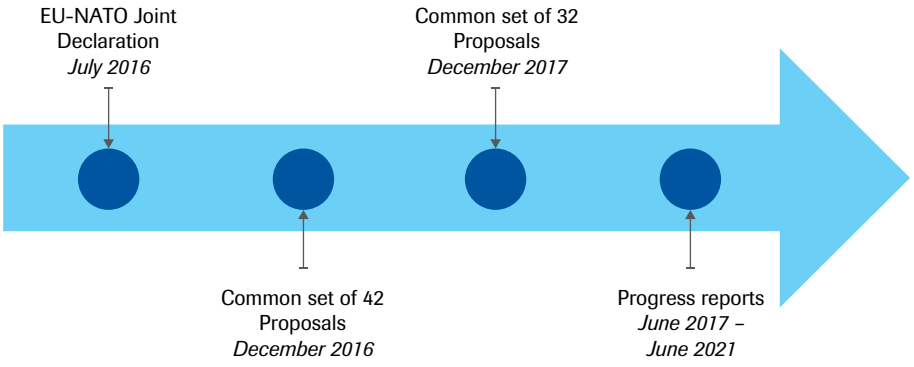
Eventually, this need for further cooperation led to the adoption of the EU-NATO Joint Declaration at the NATO Summit in Warsaw in July 2016. This declaration identified seven areas of cooperation: countering hybrid threats; broadening and adapting operational cooperation; expanding coordination on cyber security and defence; developing coherent, complementary and interoperable defence capabilities; facilitating a stronger defence industry; stepping up coordination on exercises; and building defence and security capacity and fostering the resilience of partners.[14]

Following the adoption of the declaration in 2016, the EU and NATO drafted the 2016 and 2017 common sets of proposals, resulting in a total of 74 concrete actions. These 74 proposals were meant to implement the objectives that were laid down in the 2016 Joint Declaration. In order to evaluate the implementation of these proposals, the EU

14 European Council, European Commission and NATO, Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, (Warsaw: 8 July 2016).

and NATO have published six progress reports since 2016.[15] It should be recognised, however, that the majority of the 74 proposals have a long-term perspective requiring continuous implementation, since they represent recurring processes which produce gradual results, rather than single one-off events.[16] Figure 1 presents a timeline of (recent) EU-NATO cooperation.

Figure 1 Timeline of (recent) EU-NATO cooperation



Countering hybrid threats is one of the main areas of cooperation between the EU and NATO: at least 20 out of the 74 proposals are related to countering hybrid threats. Taking into account cyber security and defence as a domain that is also of relevance for countering hybrid threats as well, this leads to a total of 22 out of the 74 proposals. Below, a reflection on these existing cooperation proposals and the progress that has been made is provided. As explained in chapter 2, the focus will be on the proposals that are highlighted under the topics 'countering hybrid threats' and 'cyber security

15 EU & NATO, Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016, 14 June 2017; EU & NATO, Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016, 29 November 2017; EU & NATO, Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 8 June 2017; EU & NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 17 June 2019; EU & NATO, Fifth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 16 June 2020; EU & NATO, Sixth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 3 June 2021.

16 3rd Progress report, p. 1.

and defence'. Hence, the analysis will focus on the following sub-themes: situational awareness, strategic communication, crisis response, bolstering resilience, and cyber security and defence.

Situational awareness

Situational awareness refers to being aware of relevant developments, events and threats that occur in a certain environment, including the geographical environment and cyberspace, that might affect a state's or an organisation's security.[17] It is well represented in the common set of proposals for EU-NATO cooperation. Out of the 74 proposals, three proposals (and two sub-proposals) concern situational awareness (see Table 1).

Table 1 Overview of concrete proposals on situational awareness

Proposals	Year
Concrete measures will be put in place by May 2017 to enhance staff-to-staff sharing of time critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart including by exchanging the analysis of potential hybrid threats. This will include the establishment of technical means to allow systematic exchange of information relating to hybrid threats.	**2016**
Intensify relations among actors at staff level engaged in countering hybrid threats and strengthen cooperation, including: • In developing their approaches to operate in the domain of Publicly Available Information including processes and tools of collecting, analysing, and disseminating as well as exchanging of unclassified products. • In developing collaboration with the European Centre of Excellence for Countering Hybrid Threats including in support of situational awareness.	**2017**
Strengthen cooperation at staff level on threat assessments, including terrorism, emanating from the South and the East; Consider contributions by the NATO Hub for the South, as appropriate.	**2017**

As for the first proposal on establishing concrete measures to enhance staff-to-staff sharing of information between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch, this was adequately followed up when both organisations drafted the 2017 proposals. In the 2017 proposals, more detailed measures for enhancing staff-to-staff sharing of information were incorporated. Therefore, it can be said that both organisations quickly complied with this 2016 proposal.

17 Definition by the authors. There is no internationally agreed definition.

Mixed results have been achieved regarding the second proposal, the intensification of relations between those actors at staff level that are engaged in countering hybrid threats. A positive result is that staff-to-staff discussions have been established along geographical and thematic clusters of the EU's Single Intelligence Analysis Capacity and NATO's Joint Intelligence and Security Division. This has contributed to the creation of a shared situational picture.[18] With reference to the first bullet of this proposal, the development of approaches to operate in the domain of publicly available information, some progress has been achieved: the EU Hybrid Fusion Cell and the NATO Hybrid Analytical Branch are exploring how best to make use of the Hybrid CoE for the exchange of publicly available information[19]; and the EU Hybrid Fusion Cell, the NATO Hybrid Analytical Branch and the Hybrid CoE are reflecting on the establishment of trilateral cooperation through open-source material.[20] It is however unclear whether and to what extent these two aspects have been materialised. In addition, during the conduct phase of a parallel and coordinated exercise, NATO liaison officers were hosted in EU premises and an EU liaison officer was deployed in NATO.[21] Moreover, video teleconferences between EU and NATO staff were organised to exchange information to enhance situational awareness. Progress has been made with reference to intensified cooperation in this domain, but these steps are so far relatively small and the most recent progress reports, the fifth and sixth, do not refer to any further progress with regard to the development of approaches for the exchange of publicly available information or the establishment of a trilateral cooperation forum.

Nevertheless, important steps have been taken to intensify relations between EU and NATO staff that are involved in countering hybrid threats. In essence, this comes down to the second element of this proposal, collaboration with the Hybrid CoE. The progress reports highlight that increased interaction can be witnessed between the staff of the EU Hybrid Fusion Cell, the NATO Hybrid Analysis Branch, and the Hybrid CoE. Concrete output in this regard are the high-level retreats, hosted by the Hybrid CoE, in which EU and NATO staff participated. In these retreats, which took place in 2018 and 2019, possible concrete actions and recommendations for further cooperation were formulated, including in the area of situational awareness.[22] This highlights that this format yields benefits, as it provides staff members of both EU and NATO with a forum in which they can update each other on their work, reflect on the progress made, and explore options for further cooperation. The literature supports this by stating that 'cross-fertilisation' in EU-NATO cooperation is occurring within the framework

18 3rd Progress report.
19 2nd Progress report.
20 3rd Progress report.
21 4th Progress report.
22 3rd and 4th Progress reports.

of the Hybrid CoE[23], the establishment of which is marked as a milestone in EU-NATO cooperation.[24]

Thirdly, and closely related to information sharing, is the proposal to strengthen cooperation on threat assessments. Threat assessments are important for creating situational awareness, as they provide a more detailed insight into existing threats, including into the actors involved. As reported, the general understanding on the nature of threats has increased over time and the views of the EU and NATO have converged.[25] Nevertheless, at present, there is no joint EU-NATO threat assessment. Both organisations have their own threat assessments, which to a certain extent align but also differ, building upon the different nature and operating regions of the organisations. Moreover, the age-old obstacle of sharing (classified) information and intelligence seriously hinders the creation of a joint EU-NATO threat assessment.[26] As information on hybrid threats is at least partly classified, such a joint assessment seems almost impossible. Logically, the progress reports do not substantiate any advancements that have been made in this area. Furthermore, the literature highlights the lack of information and intelligence sharing, emphasising that sharing information on situational awareness and open-source intelligence is required "to promote a shared view on our common security environment and events unfolding in it."[27] The lack thereof indicates that increased cooperation on threat assessments has not progressed much in recent years, leaving room for improvement.

Strategic communication[28]

An important hybrid threat is disinformation creating distrust and disorder in societies. Both the EU and NATO are active in strategic communication to counter the threat of societal problems related to the spread of incorrect information. The NATO Strategic Communications Centre of Excellence (StratCom CoE) describes the concept of strategic communications as follows: "A holistic approach to communication, based on values and interests, that encompasses everything an actor does to achieve objectives,

23 Hanna Smith, 'Countering hybrid threats', in: Gustav Lindstrom & Thierry Tardy (Eds.), The EU and NATO. The essential partners, p. 17.

24 Nicole Koenig, 'The EU and NATO: A Partnership with a Glass Ceiling', Istituto Affari Internazionali, 2018, p. 3.

25 Hanna Smith, 'Countering hybrid threats', p. 17.

26 Information from interviews.

27 Aapo Cederberg, Pasi Eronen & Juha Mustonen, Hybrid CoE Working Paper 1, Regional Cooperation to Support National Hybrid Defence Efforts, p. 9.

28 This encompasses both the overall strategic communication as well as countering misinformation. In the list of 74 proposals both topics are listed in the same category, although they could be treated separately.

in a contested environment. It means that strategic communication is understood more as a holistic mind-set in projecting one's policies. We cannot focus on short-term, single-dimension, local issues. We have to think long-term, complex solutions, and effective ways of influencing big, important discourses in a very competitive environment. That is a permanent state of agility, whilst remaining true to own values."[29]

In 2016 and 2017 the EU and NATO articulated various proposals for increased cooperation on the topic of strategic communication (see Table 2). Based on the various progress reports that have been published, below the progress is reported for all four proposals on strategic communication.

Table 2 Overview of concrete proposals on strategic communication

Proposals	Year
Intensify cooperation and undertake shared trend analysis of misinformation, including through social media targeting the EU and NATO; produce, by the end of 2016, an analysis on the above; cooperate to improve quality and outreach of positive narrative.	**2016**
Enhance mutually reinforcing efforts regarding support for stratcom capabilities of partner countries including through coordinated or joint trainings and sharing of platforms.	**2016**
Encourage cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS Stratcom division (specifically task forces East and South) including further joint trainings/seminars.	**2016**
Coordinate strategic communications messaging on security threats where appropriate, including terrorism related issues.	**2017**

First of all, progress is reported on the proposal to intensify EU and NATO cooperation and to undertake joint trend analysis of misinformation. The various progress reports list improvements in information exchange regarding strategic communication and the threat of misinformation. The increased exchange of information particularly takes place through formal and informal consultations and contacts between EU and NATO staff. Especially the establishment of the EU Hybrid Fusion Cell (created within the EU Intelligence and Situation Centre) in 2016 and its interaction with the NATO Hybrid Analysis Cell enabled a shared situational picture to be drawn up. This focused cooperation resulted in 'Joint Intelligence Assessments' as well as 'Parallel and Coordinated Analyses' in which disinformation threats were included. Furthermore, the EEAS, the European Parliament and the European Commission were regularly briefed by NATO officials, while EEAS officials were invited on different occasions to brief NATO staff on the strategic communication taskforces of the EEAS and on disinformation in particular.

29 NATO StratCom COE, 'About Strategic Communications'.

A clear example of increased cooperation is offered by the Covid-19 pandemic during which disinformation surrounding the health crisis extensively increased: "EU and NATO staffs shared with each other dedicated Information Environment Assessments and held weekly calls with international partners such as the G7 Rapid Response Mechanism. NATO staff has shared with EU staff the NATO Covid-19 Strategic Communications Framework, the Covid-19 Integrated Communications Plan and a weekly selection of proactive communications products."[30] This is also acknowledged in an article written by NATO Deputy Secretary General Mircea Geoana: "On Covid-19, there is regular top-level contact, briefing and information sharing. High Representative Josep Borrell recently attended the NATO Defence Ministers meeting and the Secretary General and I regularly attend EU meetings. Our strategic communications teams work together to combat disinformation and propaganda, and the NATO and EU disaster response coordination centres are in regular contact as they respond to requests for help."[31]

Concerning the second aim, enhancing mutually reinforcing efforts regarding support for strategic communication capabilities of partner countries, including through coordinated or joint training and the sharing of platforms, the progress reports mainly mention consultations and calls to share information and ideas between EU and NATO staff. General capacity-building efforts in partner countries outside the EU and NATO, such as in Bosnia-Herzegovina, Moldova and Tunisia, often include elements of strategic communication. How to measure the level of success is difficult; according to some interviewees more improvement in this area could certainly be accomplished, although the 'which and how' remained unclear.

The Hybrid CoE in Helsinki has played an important role in encouraging cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS StratCom division. The main duties of the Centre are sharing best practices, testing new ideas and approaches, and providing training courses and exercises, including on strategic communication. The progress reports also mention continuous information exchanges between the EEAS StratCom division and the NATO StratCom Centre of Excellence in Riga, for instance on training materials, developing joint simulations and awareness-raising activities. An example is a jointly developed training course simulating disinformation attacks and responses delivered to EU staff. Although cooperation could be further deepened, the aim of encouraging cooperation was accomplished.

The fourth aim, concerning the coordination of strategic communications messaging on security threats, was accomplished but only to some extent; on this topic the progress

30 5th Progress report, p. 3.

31 Mircea Geoana, 'Stronger Together', *European Defence Matters*, No. 19, June 2020, p.42.

reports particularly mention exchanges at the technical level of NATO and EU staff without going into much detail.

In general, the cooperation between the EU and NATO in the field of strategic communication seems to have increased in recent years, not least because of the Covid-19 crisis during which the spread of disinformation reached new levels. In the interviews this relatively positive image was confirmed, especially with regard to increased staff-to-staff contacts to exchange information. Yet, apart from mere information exchange, more practical cooperation in identifying and countering disinformation campaigns in a quick and effective manner is considered as a necessary next step for the coming years, also in more general terms that reach beyond the Covid-19 pandemic. A few publications touching upon the issue provide a similar perspective. Eitvydas Bajarūnas, Ambassador-at-Large at the Ministry of Foreign Affairs of the Republic of Lithuania, praises the progress that both the EU and NATO have made in recent years in raising awareness for the relatively new phenomenon of large-scale disinformation, but also reiterates that much more efforts are required.[32] Hanna Smith, the Director of Strategic Planning and Responses at the Hybrid CoE, concluded in 2019 that: "In the area of strategic communication, people-to-people contacts have become frequent and common approaches have been explored, for example in relation to the Western Balkans and Europe's eastern and southern flanks".[33]

Crisis response

Out of the 74 concrete proposals for EU-NATO cooperation that have been created in 2016 and 2017, only two proposals are explicitly related to crisis response (see Table 3). However, proposals in other categories (for example in the cyber area), especially in relation to 'exercises', are relevant here as well, as these proposals have the objective of enhancing the crisis response activities of both organisations. Below, the progress that has been made with reference to EU-NATO cooperation in the field of crisis response will be outlined.

32 Eitvydas Bajarūnas, 'Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond', *European View* 2020, Vol. 19, No. 1, pp. 62-70.

33 Hanna Smith, 'Countering hybrid threats', in: Gustav Lindstrom & Thierry Tardy (eds.), The EU and NATO: The essential partners, European Union Institute for Security Studies, 2019, pp. 13-23, see p. 18.

Table 3 Overview of concrete proposals on crisis response

Proposals	Year
Enhance preparedness, inter alia, by holding regular meetings at staff-to-staff level.	**2016**
Bearing in mind the EU's crisis response procedures, including the Integrated Political Crisis Response arrangements (IPCR) and NATO's Crisis Response System, seek to synchronize the two organisations' parallel crisis response activities with the goal of providing coherent support in response to hybrid threats.	**2016**

With respect to the first proposal, enhancing preparedness through regular meetings at staff-to-staff level, the EU and NATO have made important steps. Both NATO staff and EU staff actively participated in high-level retreats that were hosted by the Hybrid Centre of Excellence, where further actions for enhanced EU-NATO cooperation, including in the domain of crisis response, were specified.[34] Furthermore, various workshops and briefings in which both organisations participated were hosted to enhance staff-to-staff dialogue. Examples include: cross-briefings on EU crisis response mechanisms, NATO Counter Hybrid Support Teams, the European Medical Corps and capability development under the Civil Protection Mechanism; a workshop on EU-NATO cooperation in civil protection in February 2019; an intensified dialogue on CBRN issues; EU staff participating in the NATO Energy Security Roundtable in December 2017; and EU staff providing a briefing on energy security issues to the NATO Industrial Resources and Communications Services Group in March 2018.[35]

In addition, the EU and NATO have dedicated significant efforts over the past five years to improve the synchronisation of the EU's and NATO's crisis response activities. For example, NATO shared its guidance on Improving Resilience of National and Cross-Border Energy Networks and its guidance for Incidents Involving Mass Casualties with EU staff, thereby making better synchronisation between the EU and NATO possible.[36] The most remarkable effort in enhancing synchronisation, however, was the various EU-NATO exercises that took place. During the EU PACE17/CMX17 exercise in 2017, NATO staff were present at a Presidency-chaired Integrated Political Crisis Response arrangement (IPCR) roundtable, while EU-staff participated in the discussions of NATO's Civil Emergency Planning Committee.[37] In November 2018, the EU Hybrid Exercise Multi-Layer 18 took place. This EU-led exercise was the largest crisis management exercise ever conducted with the aim of improving and enhancing the ability to respond to a complex crisis of a hybrid nature with an internal and an external dimension, as well as to improve cooperation with NATO. The exercise included a hybrid scenario

34 3rd Progress report.
35 3rd and 4th Progress reports.
36 3rd Progress report.
37 2nd Progress report.

designed to create meaningful interactions with NATO staff in the area of cyber security, disinformation and civil protection. Furthermore, EU staff participated in the May 2019 crisis management exercise of NATO, in which an EU Crisis Response Cell contributed to complement the crisis scenario with generic crisis responses from the EU institutions and the deployment of six EU staff members at NATO headquarters.[38]

The most recent example of an improved synchronisation of the crisis response activities of EU and NATO is the close coordination between both organisations during the Covid-19 pandemic. Various elements of the common set of proposals proved to be relevant in the context of the pandemic: countering disinformation, logistical support, responding to cyber threats and exploring the effects of the pandemic on operational engagements in theatres.[39] Moreover, NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and the EU's Emergency Response Coordination Centre (ERCC) further intensified their cooperation and coordination during this period. In this regard they were able to build upon earlier practices in which the ERCC engaged in field exercises with the EADRCC.[40] Regular consultations and the continuous exchange of information on the organisations' responses to the pandemic contributed to the creation of mutual situational awareness and helped to avoid unnecessary duplication. One very concrete output is the pandemic wargame 'Resilient Response 20', hosted by the Hybrid CoE in cooperation with the Multinational Medical Coordination Centre/European Medical Command and the German Federal Office of Civil Protection and Disaster Assistance. Both EU and NATO staff actively participated in this wargame[41], but it is still unclear what lessons have been learned and what it could entail for future cooperation in this area.

Bolstering resilience

As for hybrid threats, no single definition of resilience exists. It essentially comes down to states that possess the capacity and ability to minimise the potential disruptive impact that external shocks and events may have. The fluidity and broadness of the concept derives from the fact that 'resilience' needs constant adaptation following a continuously evolving international security environment.[42] The EU and NATO both have essential roles to play in enhancing resilience, abroad and at home. For the EU,

38 2nd and 4th Progress reports.

39 5th and 6th Progress reports.

40 Tania Latici, Understanding EU-NATO cooperation. Theory and practice, European Parliament Briefing, (European Parliamentary Research Service, October 2020), p. 7.

41 5th and 6th Progress reports.

42 Dick Zandee, Adája Stoetman & Bob Deen, The EU's strategic compass for security and defence. Squaring ambition with reality, (The Hague: The Clingendael Institute, May 2021), p. 19.

the focus has primarily been on enhancing resilience abroad to safeguard security interests at home, incorporating it as a central element of the EU's external policy framework. NATO regards Article 3 of its Treaty – namely that Allies should "maintain and develop their individual and collective capacity to resist an armed attack"[43] – as the reference for strengthening resilience.[44] Although the article was originally drafted to underline the importance of collective defence against the Soviet threat, today NATO has recognised that the changing security environment requires a broader perspective of an 'armed attack'. Two clear expressions of this new interpretation can be derived from the Summit declarations of 2014 and 2021. The NATO Wales Summit of 2014 underlined that a cyberattack could also lead to the invocation of Article 5 of the NATO Treaty.[45] The NATO Brussels Summit of 2021 highlighted that Article 5 could also be called upon by a NATO ally in response to hybrid warfare.[46] However, non-traditional security threats require more than military responses. In contrast, these threats require broader societal resilience, something for which NATO is not necessarily well equipped – although Article 3 may suggest the opposite. In that sense, broader societal resilience is a relatively new domain for NATO, given that the organisation can primarily deploy military forces.

Both organisations therefore have a clear role to play when it comes to resilience. Logically, this has therefore been one of the focus areas where practical cooperation has increased in recent years. The concrete proposals for EU-NATO cooperation substantiate this, as no fewer than eight proposals are related to bolstering resilience (see Table 4).[47] Below, the progress that has been made with reference to EU-NATO cooperation in the field of bolstering resilience will be outlined.

43 The North Atlantic Treaty, Washington D.C., 4 April 1949.

44 NATO, Resilience and Article 3, Last updated: 11 June 2021.

45 Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, paragraph 72, 5 September 2014.

46 Brussels Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, paragraph 31, 14 June 2021.

47 Concrete proposals 2016 & 2017.

Table 4 Overview of concrete proposals on bolstering resilience

Proposals	Year
Staff contacts will be intensified, including cross-briefings to respective bodies on resilience requirements.	**2016**
Assess requirements, establish criteria and develop guidelines in the context of greater coherence between the EU Capability Development Plan (CDP) and the NATO Defence Planning Process (NDPP).	**2016**
Work to be ready to deploy, by mid-2017 in a parallel and coordinated manner, experts to support EU Member States/Allies, upon request, in enhancing their resilience, either in the pre-crisis phase, or in response to a crisis.	**2016**
Strengthen staff-to-staff cooperation on civil preparedness, including risk assessments, medical evacuation (MEDEVAC), mass casualty incidents, and population movement.	**2017**
Develop a programme of staff-to-staff scenario-based discussions and workshops designed to promote mutual understanding of hybrid crisis management, in line with the respective playbook/operational protocol, as well as the implications on capability development upon the findings of the relevant Hybrid Threats Table Top exercises conducted in 2016.	**2017**
The European Centre of Excellence for Countering Hybrid Threats could facilitate scenario-based discussions, workshops and exercises.	**2017**
NATO and the EU staffs to map their civil preparedness efforts between NATO's Resilience Baselines and the EU's Prevention and Preparedness work-streams and set out proposals on where further co-operation may add value in the course of 2018.	**2017**
Building on established practice and applied procedures, explore the inclusion, where appropriate, of EU staff in the NATO Resilience Advisory Support Teams and other assistance teams and NATO staff in relevant EU advisory prevention and preparedness missions conducted under the Union Civil Protection Mechanism (UCPM) subject to consent by the receiving State.	**2017**

As for the first proposal, staff-to-staff contact between EU and NATO staff members has clearly intensified in the past five years. With the exception of the first progress report, all reports mention that staff-to-staff contacts regarding resilience have continued over time. In addition, the reports mention that EU and NATO staff have participated in various cross-briefings and workshops, such as an EU-NATO Resilience Workshop and a NATO-hosted workshop on 5G networks and foreign direct investment.[48] The participation of EU and NATO staff in these workshops and scenario-based discussions also contributed to the fulfilment of the fifth proposal, to develop a programme of staff-to-staff scenario-based discussions and workshops to promote the mutual understanding of hybrid crisis management. In this respect, there is also room for improvement, which mainly comes down to embedding these workshops and scenario discussions more explicitly in EU-NATO cooperation, so that these become more

48 Progress reports 2, 3, 4, 5 & 6.

regular exercises, instead of their currently more ad hoc nature.[49] Closely related is the facilitation role performed by the Hybrid CoE, thereby fulfilling the sixth proposal. The Hybrid CoE clearly fulfilled a hub function between EU and NATO staff by organising various scenario-based discussions, workshops and exercises.

Furthermore, in relation to the first proposal an important milestone was reached in 2020 when NATO international staff were included in the International Cooperation Space on the EU's Rapid Alert System. The inclusion of NATO international staff in this forum allows for direct exchanges with EU member states and relevant EU institutions.[50] These developments have contributed to the improvement of staff-to-staff interaction, the exchange of information, increasing transparency and raising mutual awareness. Moreover, the Covid-19 pandemic provided a window of opportunity for both organisations to enhance staff-to-staff contacts on resilience and civil preparedness. EU and NATO staff continued to engage on these themes, including through the exchange of information on the organisations' respective activities in response to the pandemic. In addition, the EU's Emergency Response Coordination Centre (ERCC) and NATO's counterpart, the EuroAtlantic Disaster Response Coordination Centre (EADRCC), closely cooperated throughout the pandemic, highlighting the benefit of previous joint field exercises.[51]

With reference to the second proposal, which dictates the establishment of greater coherence between the EU's CDP and NATO's NDPP, various efforts have been undertaken. For example, a staff-to-staff meeting was organised in May 2018, discussing and raising awareness of the status of the EU's CDP and NATO's NDPP and how resilience and hybrid threats were addressed in these two processes.[52] In addition, staff from both organisations participated in relevant events, including the NATO Defence Policy and Planning Symposium, contributing to further increasing transparency and raising awareness on the role of resilience in the two processes.[53] Moreover, regular contact between EU and NATO staff ensures the exchange of information on NATO's baseline requirements for national resilience. Although these requirements have been shared with the EU, this does not yet guarantee that the EU automatically copy pastes all the requirements that are laid down. This has partly to do with the different nature of the organisations and the different instruments they have at their disposal to enhance resilience. Therefore, this can be a focus area to streamline EU-NATO cooperation

49 Information from interviews.

50 6th Progress report.

51 Tania Latici, Understanding EU-NATO cooperation. Theory and practice, European Parliament Briefing, (European Parliamentary Research Service, October 2020), p. 7.

52 3rd Progress report.

53 4th Progress report.

further.[54] Moreover, a unique opportunity arises here, as the EU is in a position to create a legal framework for these standards with which EU member states have to abide.[55] This will eventually also benefit NATO. On a more general level, individual NATO Allies continued to invite EU staff for bilateral and multilateral consultations within the framework of the NDPP process, while EU member states that are also a member or partner of NATO invited NATO allies to attend (bilateral) meetings of the Coordinated Annual Review on Defence process.

As for the third proposal, establishing readiness to deploy experts to support EU member states and Allies in enhancing resilience, no concrete progress is mentioned in the evaluation reports. Nevertheless, NATO's response to hybrid threats document, dating from 2018, states that NATO is ready to assist an ally at any stage of a hybrid campaign. The only prerequisite would be a North Atlantic Council (NAC) decision that allows NATO to do so. Moreover, the NAC could also decide to invoke Article 5 of the North Atlantic Treaty in cases of hybrid warfare.[56] This implies that NATO has taken the necessary measures to deploy experts at the request of member states. Two concrete examples where this has been put into practice are Montenegro (2019) and Lithuania (2021), where NATO supported both nations, at their request, in countering hybrid threats.[57] In the case of Lithuania, being an Ally and also an EU member state, it received NATO assistance. However, the fact remains that the progress reports do not mention that any progress has been made on EU-NATO cooperation in this area.

Progress has been made, though, with reference to the fourth proposal, strengthening staff-to-staff cooperation on civil preparedness. Staff from both organisations took part in various workshops, cross-briefings and table-top exercises, in which information was exchanged and guidelines, requirements and methods were shared.[58] Central themes were civil protection, critical infrastructure protection and foreign direct investment. An example includes NATO sharing its guidance for Incidents Involving Mass Casualties with EU staff.[59] More concretely, the EU's and NATO's medical communities enhanced their cooperation by cross-linking civilian and military expertise in medical-related

54 Information from interviews.

55 Information from interviews.

56 Brussels Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, paragraph 31, 14 June 2021; and Laris Gaiser, 'NATO-EU Collaboration on Hybrid Threats: Cooperation out of necessity with potential consequences on international legal framework', in: *National Security and the Future,* 1-2(20), 2019, p. 19.

57 Ministry of National Defence of the Republic of Lithuania, 'The decision has been made: NATO Counter Hybrid Support Team will arrive to Lithuania', 25 August 2021; and The Baltic Times staff, 'NATO to send Counter Hybrid Support Team to Lithuania', *The Baltic Times,* 25 August 2021.

58 Confirmed by interviews.

59 3rd Progress report.

topics, including a cross-briefing to evaluate potential synergies with reference to medical evacuation.[60] Next to the exchange of information on the organisations' activities in response to the pandemic, the Commission, in September 2020, updated NATO's Civil Emergency Planning Committee on the EU's response to Covid-19, while NATO, in November 2020, shared with the EEAS and the Commission its updated Baseline Requirements for Resilience.[61]

The fact that NATO shared its Baseline Requirements for Resilience with the EEAS and the Commission is also in line with the seventh proposal, which prescribes that NATO and EU staff should map their civil preparedness efforts between NATO's Resilience Baselines and the EU's Prevention and Preparedness work-streams and outline additional proposals for increased cooperation. In addition, the staff of both organisations are sharing information regarding civil preparedness efforts between NATO's Resilience Baselines and the EU's Prevention and Preparedness work-streams. However, besides these two aspects the progress reports do not mention any further cooperation. Moreover, they also do not incorporate proposals where further cooperation may be of added value. Therefore, this proposal has only been partially fulfilled. This is confirmed by the interviews, in which it was highlighted that the only substantial accomplishment that has so far been achieved is the sharing of the Baseline Requirements. Although the sharing of the Baseline Requirements should be regarded as an important milestone, it is only a first step. It is up to the EU what the subsequent action will be and to what extent the organisation will make use of the existing NATO requirement. Moreover, besides the sharing of these requirements, further steps regarding enhanced cooperation have not been made and no concrete accomplishments have been achieved in this respect.[62]

With reference to the eighth and final proposal, it can be concluded that progress has been achieved. The proposal prescribes that, when appropriate, both organisations should explore the possibility to include EU staff in the NATO Resilience Advisory Support Teams and NATO staff in relevant EU advisory prevention and preparedness missions. Already in 2017, the EU participated as an observer in NATO's advisory mission to Romania.[63] More structural cooperation was established in Ukraine, however, where experts from the EU's Advisory Mission were part of the NATO-led team for Building Integrity Peer Review process for Ukraine. EU and NATO staff also coordinated their advisory support to Ukraine's security and defence sector, with a specific focus on the reform of the security and intelligence services.[64] Another example is the cooperation

60 4th progress report.

61 5th and 6th progress reports.

62 Information from interviews.

63 2nd Progress report.

64 3rd, 4th, 5th and 6th Progress reports.

between the EU Advisory Mission in Iraq and the NATO Mission Iraq. In this case, regular coordination took place in order to avoid duplication and to establish greater synergies. Both NATO and the EU have, in close cooperation with international partners, "developed a robust coordination and cooperation framework for the Security Sector Reform effort delineating roles and responsibilities"[65]. Other examples where EU and NATO staff closely coordinate in partner countries are Bosnia and Herzegovina, the Republic of Moldova and Georgia (on strategic communication and resilience).[66]

Cyber security and defence

Cyber security and defence is one of the main pillars of EU-NATO cooperation. In the sets of proposals of 2016 and 2017, five proposals are directly related to the area of cyber security and defence (see Table 5).

Table 5 Overview of concrete proposals on cyber security and defence

Proposals	Year
With immediate effect, EU and NATO will exchange concepts on the integration of cyber defence aspects into planning and conduct of respective missions and operations to foster interoperability in cyber defence requirements and standards.	**2016**
In order to strengthen cooperation on training, as of 2017, EU and NATO will harmonize training requirements, where applicable, and open respective training courses for mutual staff participation.	**2016**
Foster Cyber Defence Research and Technology Innovation cooperation by further developing the linkages between EU, NATO and the NATO Cooperative Cyber Defence Centre of Excellence to explore innovation in the area of cyber defence: considering the dual use nature of cyber domain, EU and NATO will enhance interoperability in cyber defence standards by involving industry where relevant.	**2016**
Strengthen cooperation in cyber exercises through reciprocal staff participation in respective exercises, including in particular Cyber Coalition and Cyber Europe.	**2016**
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, such as analysis of threats and malware information, with a view to improving the understanding of and identifying potential synergies between the two organisations' approaches, including existing cyber security incident response teams.	**2017**

Regarding the first proposal on exchanging concepts and fostering interoperability, the progress reports list several exchange activities between the EU and NATO, such as meetings, joint workshops and other ways of information sharing. These activities

65 6th Progress report.

66 6th Progress report.

took place at various staff levels, varying from, for example, high-level EU-NATO staff talks to cross-briefings by EU and NATO staff members in relevant Committees and/or Working Groups. According to the progress reports, these varying exchanges provided "a platform to establish a comprehensive overview of all mutually beneficial NATO and EU conceptual ideas and documents in the cyber domain and to explore their individual releasability as well as their potential for coordinated development."[67] Whether the exchanges of information actually contributed to the increased integration of cyber defence aspects into planning or to more interoperability in cyber defence requirements and standards cannot be read from the progress reports. Interviewees acknowledged that exchanges between the EU and NATO have increased in recent years, and that this contributed to better interoperability, but it is hard to quantify the level of improvement that has been accomplished. More improvements in this field were considered to be possible and desirable.[68]

The second proposal, concerning harmonising training requirements and opening respective training courses for mutual EU-NATO staff participation, has been met to some extent: almost all progress reports include examples of EU and NATO staff participating in exercises organised by each other's organisation, as well as joint workshops on education and training issues. While the opening of several training exercises for mutual participation is mentioned as a success, it is not clear whether, or to what extent, training requirements have been harmonised.[69]

The third proposal focussed on cooperation in Cyber Defence Research and Technology Innovation by further developing the linkages between the EU, NATO and the NATO Cooperative Cyber Defence Centre of Excellence, and enhancing interoperability in cyber defence standards. Some progress reports mention that NATO staff were involved in EU staff efforts to develop generic standard operating procedures for cyber defence at headquarters level[70], and that 'cyber' was also the topic of an EU-NATO staff-to-staff dialogue on industrial aspects.[71] Yet, how far linkages and interoperability have actually improved is unclear.

The fourth proposal, on strengthening cooperation in cyber exercises through reciprocal staff participation in respective exercises, including in particular Cyber Coalition and Cyber Europe, partly overlaps with the second proposal on opening respective training courses for mutual EU-NATO staff participation. Several progress reports mention reciprocal EU-NATO staff participation in respective cyber defence exercises, so this aim seems to have been adequately accomplished.

67 5th Progress report, p. 6.

68 Information from interviews.

69 Confirmed by the interviews.

70 4th Progress report, p. 5.

71 3rd Progress report, p. 5.

The fifth proposal was on the exchange of good practices concerning cyber aspects and the implications of crisis management and response, as well as operational aspects of cyber defence, to enhance understanding and identifying potential synergies between EU and NATO approaches, including existing cyber security incident response teams. The progress reports describe many coordination meetings between EU and NATO staff, which are held at various levels on a regular basis, where exchanges on good practices have taken place. Moreover, the Technical Arrangement on Cyber Defence between the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU) continued to be implemented in line with existing provisions, to which end the Malware Information Sharing Platform (MISP) was being leveraged.[72] Information exchange between CERT-EU and the NCIRC is listed as an accomplishment as well, including the organisation of a joint workshop on good practices. In the interviews conducted for this research, the progress regarding the exchange of information, including on good practices, was confirmed; the increased staff-to-staff level of communications might even be regarded as the most important progress regarding cyber security and defence. However, as will be discussed below, more efforts to improve effective information exchange are needed.

Although the progress reports sketch a positive image of increased EU-NATO cooperation in the field of cyber security and defence, in the (scarce) literature on the topic some more critical perspectives are offered. For example, in 2019 Piret Pernik of the Estonian Academy of Security Sciences stated that EU-NATO cooperation on cyber security and defence had made important strides, but that it proved difficult to engage the capitals "as top-level tangible activities are still needed to improve the common understanding of threats and the interoperability of national capabilities."[73] Even though information exchanges and the sharing of threat assessments and resilience measures have improved, Pernik signals that "Brussels officials complain that these exchanges are bureaucratic, overly generic and lacking in substance." An important problem in the cooperation, he suggests, is the limitation on sharing classified information, while such information is necessary to attribute cyberattacks with a sufficiently high level of confidence and to develop mutual trust. Next to the lack of sharing classified information, cooperation is hindered by different prioritisation. According to Pernik, NATO prioritises military doctrinal development and mission assurance, as well as integrating sovereign cyber effects to support NATO missions and operations. The EU, however, focuses on developing its cyber diplomacy tools, setting up a framework for the certification of ICT services and products, as well as creating stronger research and competence capabilities. Pernik further states: "Differences in state interests and in organisational memberships complicate taking meaningful common action. Countries

72 4th Progress report, p. 6.

73 Piret Pernik, 'EU-NATO Cooperation in Cyber Security and Defence', in: EU-NATO Cooperation: A Secure Vision For Europe, Discussion Paper, Friends of Europe, June 2019, p. 8-11.

differ in operational capabilities, the maturity of their national civilian and military cyber capabilities and their bilateral strategic partnerships with major cyber powers. Moreover, they have a variety of priorities and interests when it comes to protecting critical infrastructure and securing military assets."

Bruno Lété, of the German Marshall Fund of the United States, also observes improved cooperation between EU and NATO in the field of cyber security. He states that "Since neither organisation possesses the full range of capabilities to tackle contemporary 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."[74] Concerning the successes of increased cooperation, Lété mentions exchanges between staff on concepts and doctrines, information on training and education courses, ad-hoc exchanges on threat assessments, cross-briefings, including on the cyber aspects of crisis management, and an annual high-level EU-NATO staff-to-staff dialogue. He also highlights 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 the mutual participation of EU and NATO staff.

In general, one may conclude that EU-NATO cooperation in the field of cyber security and defence has increased in recent years, but that external observers still see various obstacles to effective cooperation. Even if one should consider the cooperation proposals of 2016-2017 as modest first steps, much more bold steps will be needed to attain actual close cooperation, and an important question in this regard is whether the member states of both organisations actually desire such close cooperation. At this moment in time, there may be too little support in the various capitals.

Summary of the progress

Table 6 provides a summary of the assessment of existing EU-NATO cooperation with reference to countering hybrid threats. The assessment is based on a combination of the content of the Progress Reports, the literature and interviews with EU and NATO officials.

74 Bruno Lété, 'Cooperation in cyberspace', in: Gustav Lindstrom & Thierry Tardy (eds.), *The EU and NATO: The essential partners*, European Union Institute for Security Studies, 2019, pp. 28-36, see pp. 29-30.

Table 6 Assessment of existing proposals regarding EU-NATO cooperation on countering hybrid threats

Theme	Assessment
Situational awareness	
Concrete measures will be put in place by May 2017 to enhance staff-to-staff sharing of time critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart	
Intensify relations among actors at staff level engaged in countering hybrid threats and strengthen cooperation, including: • In developing their approaches to operate in the domain of Publicly Available Information. • In developing collaboration with the Hybrid CoE in support of situational awareness.	
Strengthen cooperation at staff level on threat assessments.	
Strategic communication	
Intensify cooperation and undertake shared trend analysis of misinformation; produce, by the end of 2016, an analysis on the above; cooperate to improve quality and outreach of positive narrative.	
Enhance mutually reinforcing efforts regarding support for StratCom capabilities of partner countries including through coordinated or joint trainings and sharing of platforms.	
Encourage cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS StratCom division.	
Coordinate strategic communications messaging on security threats where appropriate, including terrorism related issues.	
Crisis response	
Enhance preparedness, inter alia, by holding regular meetings at staff-to-staff level.	
Seek to synchronize the two organisations' parallel crisis response activities with the goal of providing coherent support in response to hybrid threats.	

Theme	Assessment
Bolstering resilience	
Staff contacts will be intensified, including cross-briefings to respective bodies on resilience requirements.	
Assess requirements, establish criteria and develop guidelines in the context of greater coherence between the EU CDP and the NDPP.	
Work to be ready to deploy, by mid-2017 in a parallel and coordinated manner, experts to support EU Member States/Allies, upon request, in enhancing their resilience.	
Strengthen staff-to-staff cooperation on civil preparedness, including risk assessments, medical evacuation (MEDEVAC), mass casualty incidents, and population movement.	
Develop a programme of staff-to-staff scenario-based discussions and workshops designed to promote mutual understanding of hybrid crisis management, in line with the respective playbook/ operational protocol.	
The European Centre of Excellence for Countering Hybrid Threats could facilitate scenario-based discussions, workshops and exercises.	
NATO and the EU staffs to map their civil preparedness efforts between NATO's Resilience Baselines and the EU's Prevention and Preparedness work-streams and set out proposals on where further co-operation may add value in the course of 2018.	
Explore the inclusion of EU staff in the NATO Resilience Advisory Support Teams and other assistance teams and NATO staff in relevant EU advisory prevention and preparedness missions conducted under the Union Civil Protection Mechanism (UCPM) subject to consent by the receiving State.	

Cyber security and defence	
EU and NATO will exchange concepts on the integration of cyber defence aspects into planning and conduct of respective missions and operations to foster interoperability in cyber defence requirements and standards.	
To strengthen cooperation on training, as of 2017, EU and NATO harmonize training requirements, where applicable, and open respective training courses for mutual staff participation.	
Foster Cyber Defence Research and Technology Innovation cooperation by further developing the linkages between EU, NATO and the NATO Cooperative Cyber Defence Centre of Excellence to explore innovation in the area of cyber defence: considering the dual use nature of cyber domain, EU and NATO will enhance interoperability in cyber defence standards by involving industry where relevant.	
Strengthen cooperation in cyber exercises through reciprocal staff participation in respective exercises, including in particular Cyber Coalition and Cyber Europe.	
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 the understanding of and identifying potential synergies between the two organisations' approaches.	

Legenda

Red	**Does not work**
Orange	**Works partly, improvement possible**
Green	**Works and can be continued**

Obstacles to cooperation on hybrid threats

Since the beginning of EU-NATO cooperation, there have been obstacles that have hindered the optimalisation of cooperation, leading to sub-optimal outcomes. Some obstacles are age-old, others have emerged over time as a result of the changing security environment.

The first and most important obstacle to further cooperation is the organisations' difference in member states. Although there is quite some overlap – 21 states are both a member of the EU and NATO – there are also EU countries that are not a NATO member and vice versa. The differences in membership are especially an obstacle when it comes to sharing more sensitive security-related information. It is common that some states only want to share information with either the EU or NATO, but not with both. Bruno Lété of the German Marshall Fund of the United States describes this as follows: "(…) the EU and NATO nevertheless remain two separate bodies, and each uphold restrictive information-sharing procedures that prevent the emergence of a culture of shared situational awareness or cyber threat assessment."[75]

In practice, this problem is sometimes solved through sharing information only between EU and NATO staff, explicitly mentioning that information cannot be shared with representatives from member states. In such situations, NATO and EU staff are able to cooperate on the basis of this information, while at the same time individual member states do not receive the classified information. This way of information sharing has enabled the EU and NATO to circumvent certain (political) obstacles.[76] So far, this construction has worked for EU and NATO staff, but if joint EU-NATO follow-up action would be required, the involvement of member states cannot be avoided and political obstacles would then still prevail. Moreover, the absence of a secure communication system sometimes also makes this very difficult. Even if there is a willingness among EU and NATO staff to share sensitive or classified information, there is no quick and easy communication system to share this information. Moreover, the EU's and NATO's standards and practices in securing information also diverge[77], which further complicate matters. Therefore, this possibility of circumventing the (political) obstacles is no sustainable solution for the long term.

In addition to the difference in membership, the EU and NATO are also, by their very nature, different organisations. Whereas NATO is a political-military organisation, the EU deals with a much broader variety of policy areas and is a law-making organisation. Consequently, the EU and NATO have different toolboxes at their disposal that can be

75 Lété, 'Cooperation in cyberspace', p. 30.

76 Information from interviews.

77 Lété, 'Cooperation in cyberspace', p. 30.

deployed in response to security threats. NATO possesses mainly military tools, while the EU can deploy civilian tools and military forces but the latter with serious limitations. This will not change fundamentally and practice shows that sometimes it takes a great deal of time to understand each other as definitions, context and responsibilities diverge. On the other hand, the different mandates and constitutions of the EU and NATO are the basis for complementarity and mutual reinforcement. This applies also to countering hybrid threats.

Another factor that hinders intensified cooperation is the changing security environment, which is increasingly characterised by hybrid threats. These threats cannot solely be addressed by military or civilian tools. In contrast, they require a whole-of-society approach, in which government and private actors must work together and where military and civilian tools need to be combined.[78] This is exactly why the EU and NATO, given their diverging toolboxes, could very well complement each other. In that context, the EU could primarily exhaust its civilian toolbox and to a lesser extent its military resources, while NATO can mainly provide resources from its military toolbox. Nevertheless, more is necessary in order to be able to counter hybrid threats effectively. The involvement of non-state actors, like private companies, is a field where both the EU and NATO as well as national governments often lack experience. Yet, the EU and NATO can prove to be a valuable part of the 'whole-of-society' chain when they create a joint platform where their respective member states can share information on hybrid threats. This will facilitate smoother cooperation between member states on countering hybrid threats, a necessity as no member state or organisation can address these threats by itself. In addition to functioning as a platform for their member states, the organisations can also enhance existing coordination between them to ensure smoother collaboration. It should, however, be prevented that cooperation will be experienced as forced, which runs the danger of reinforcing existing (political) obstacles.

Last but not least, there are obstacles on the member state level concerning non-traditional threats. Especially when it comes to hybrid cyber threats, various member states of the EU and NATO still consider cyberspace as a critical domain of national interest, and they are not always convinced that the EU or NATO should play a role here. Understandably, member states are reluctant to share all their threat intelligence or (technical) information on cyber incidents, information about their national cyber vulnerabilities and offensive or defensive cyber capabilities, or to put at common disposal their technical and intelligence capabilities to attribute cyber incidents. In addition, the cyber capabilities of the various member states are often not interoperable nor complementary, which implies that there is a growing gap across member states in terms of both civilian and military cyber capabilities.[79]

78 Hanna Smith, 'Countering hybrid threats', in: Gustav Lindstrom & Thierry Tardy (eds.), The EU and NATO: The essential partners, European Union Institute for Security Studies, 2019, p. 15.

79 Information from interviews; and Lété, 'Cooperation in cyberspace', p. 31.

Assessment

In general terms, EU-NATO cooperation in countering hybrid threats has improved in recent years. In particular, improved staff-to-staff contacts, the structured (political) dialogue and joint exercises can be highlighted as important results. In addition, both organisations have worked hard towards creating shared situational awareness, in particular through making use of the Hybrid CoE. However, obstacles to enhanced EU-NATO cooperation still exist. Some of these obstacles might be overcome in due course – such as recognising the different nature of both organisations – but others are likely to remain, at least for the foreseeable future. The political blockade caused by the Turkey-Cyprus issue is the key factor that hinders a better use of the formal cooperation channels and continues to block the exchange of classified information.

Despite these obstacles there is still room for a further improvement of EU-NATO cooperation in countering hybrid threats. Various of the common proposals dating from 2016-2017 have not yet been (fully) implemented, leaving sufficient opportunities for further cooperation between both organisations. Experts emphasise, however, that advanced EU-NATO cooperation on hybrid threats is a long-term process that takes time and should be met with patience. They underscore the importance of the cooperation efforts within the EU-NATO framework and warn against alternative cooperation formats. Moreover, it was highlighted that, often, strategic vision behind counter-hybrid efforts is lacking. The focus tends to lie on finding appropriate responses to the deployment of hybrid tools, while less attention is paid to the actors' objectives and intentions behind the use of these hybrid tools.[80] Adopting a more strategic approach, in which more focus would be directed towards the objectives and intentions of (potential) adversaries, could benefit both organisations in the long run. Nevertheless, one should not cling too much to the EU-NATO framework, without considering alternative formats of international cooperation on countering hybrid threats, which are included in the next chapter.

80 Information from interviews.

4 Potential for future EU-NATO cooperation and beyond

The 2016-2017 common set of proposals has played a vital role in improving EU-NATO coordination and cooperation in the field of countering hybrid threats. However, multiple obstacles remain in place and there is still room for increased cooperation, both with regard to the existing set of cooperation topics as well as in exploring new potential. Furthermore, the structural limitations of EU-NATO cooperation also raise the question of whether other formats should be explored to strengthen international counter-hybrid cooperation.

Potential for further EU-NATO cooperation

Before exploring additional areas of EU-NATO cooperation in countering hybrid threats, it is important to acknowledge the following. First, this EU-NATO cooperation is a necessity as such. The EU and NATO need each other, as neither of them can address hybrid threats by itself. This is especially true in light of the complex nature of hybrid threats. Hence, the analysis of hybrid threats needs to be multidisciplinary, and in addition a comprehensive approach is necessary when developing counter-mechanisms and building resilience.[81] Considering their different toolboxes, the EU and NATO can or rather must complement each other. Furthermore, it should be reminded that creating resilience is, by nature, a state matter, rather than an EU or NATO issue. However, no one state or organisation can address hybrid threats by itself. Consequently, the EU and NATO have a vital role to play in reinforcing the resilience of their respective member states.[82] Finally, the obstacles to closer formal cooperation between the EU and NATO will continue to exist for the foreseeable future, as explained in the previous chapter. Therefore, it is unlikely that maximum cooperation between both organisations will be established[83], and this should also not be expected. Nevertheless, there are still plenty of opportunities to optimise the cooperation between both organisations. These will be outlined below.

81 Hanna Smith, 'Countering hybrid threats', in: Gustav Lindstrom & Thierry Tardy (eds.), The EU and NATO: The essential partners, European Union Institute for Security Studies, 2019, p. 15.

82 Kristi Raik & Pauli Järvenpää, A new Era of EU-NATO Cooperation. How to Make the Best of a Marriage of Necessity, (Tallinn, Estonia: International Centre for Defence and Security, May 2017), p. 11-13.

83 Information from interviews.

Expectation management

First of all, room for improvement can be found on the conceptual level. From the literature and interviews the perception arises that it is not always completely obvious what exactly can be expected from the EU and NATO. Where do the responsibilities (and possibilities) of the EU and NATO begin, and where do they end? Of course, there is a wide understanding of the general differences between the two organisations: the EU is a much broader focussed organisation with a mainly civilian and legal outlook, while NATO is a more narrowly focussed political-military organisation as has been stated in chapter 3. It is also obvious that there is a certain overlap between the organisations' capabilities and responsibilities, and more importantly, even a certain complementarity when it comes to countering hybrid threats. The cooperation between the two organisations has successfully intensified in the past few years. Yet, expectations as to the respective roles of the EU and NATO with regard to countering hybrid threats could be better managed. Do the EU, NATO and their member states fully realise where the responsibilities of both organisations begin and end? What are the possibilities and limits of both organisations?

Based on various interviews that were conducted for this report, the image arises that there is a grey zone in the expectations from different sides. An example is the delineation of responsibility and military tasks with regard to cyber threats. A related perception arising from interviews is that for the EU, NATO is only one of many partners in countering hybrid threats, while for NATO the EU is at least one of the main, if not the main partner organisation in this field. The different levels of expectations may sometimes lead to disappointments at staff levels or in member states. More clearly and publicly identifying the capabilities and limits of both organisations when it comes to joint activities to counter hybrid threats could be helpful in managing expectations. This could help in updating the list of common proposals in the counter-hybrid area. Retreats, organised by the Hybrid CoE, could again be used to explore any necessary updates to the list and to explore the potential for additional categories.

Information sharing

With respect to the obstacles to information sharing, the analysis presented here has demonstrated that open-source information sharing between EU and NATO staff members has improved over the past few years, but additional steps for full implementation still have to be taken. This lies primarily in embedding regular exchanges of information between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch. Examples may include the exchange of analyses of potential hybrid threats and recommendations on how to address them.[84] In this regard, one could think of

84 Elena Denise Petrescu, Hybrid Threats: An avenue for a more solid NATO-EU cooperation, (Atlantic Forum, September 2020).

creating a (digital) information-sharing platform, within the Hybrid CoE, in which relevant stakeholders, both civilian and military, could share information and research results on hybrid activities.[85] Naturally, the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch should be included in such a platform. In addition, in order to achieve a comprehensive approach, one could also think of involving relevant private actors, such as companies that specialise in cyber security. Such a platform would greatly benefit open-source information sharing in general and would enhance situational awareness on hybrid threats more specifically.[86]

More problematic, however, is the sharing of classified information. The most pressing issue in this regard is the need for an appropriate and secure communication system through which EU and NATO staff are able to exchange classified information. At present, such a system is not available, and EU and NATO staff members sometimes have no other option than to meet in person in order to share more sensitive information with their counterparts.[87] Although no easy solution is available, exploring options for a shared communication platform is advisable. Perhaps specific priority categories of exchanging classified information between the two organisations could be chosen and agreed upon by both organisations as a starting point.

Crisis response

With reference to the area of crisis response, the EU and NATO have undertaken valuable efforts in the past six years. Nevertheless, more cooperation and coordination are needed to enhance the proposal for a further synchronisation of the crisis response activities of both organisations. The various exercises that have taken place and the interaction between EU and NATO staff during those exercises have proven to be very valuable. From this perspective, such exercises could be organised more often. The exercises help to deepen cooperation between the two organisations and their member states, but also reveal where improvement is still needed and possible. This includes, for example, the exchange of (classified) information and more effective secure communications[88]as already mentioned. In an attempt to improve cooperation in these two areas, it would be advisable that NATO and EU staff structurally embed the regular exchange of information and scenarios in their coordination and cooperation processes, so that this becomes common practice for both organisations. Furthermore, in the long term, when the EU and NATO have optimised their cooperation efforts, they

85 Aapo Cederberg, Pasi Eronen & Juha Mustonen, Regional Cooperation to Support National Hybrid Defence Efforts, Hybrid CoE Working Paper 1, (Helsinki, Finland: Hybrid Centre of Excellence, October 2017).

86 Ibid.

87 Information from interviews.

88 Tania Latici, Understanding EU-NATO cooperation. Theory and practice, European Parliament Briefing, (European Parliamentary Research Service, October 2020), p. 7.

could consider expanding these exercises by also including the participation of private actors, which have become increasingly important when it comes to addressing modern security threats and could therefore prove to be a valuable addition to these exercises – perhaps not as direct participants but by inviting representatives of companies to response cells.

In addition, with reference to the proposal to enhance the synchronisation of the EU's and NATO's crisis response mechanisms more efficiently, additional capacity should be created. At present, the increased interaction between EU and NATO staff members does not provide a solid basis for guaranteeing an effective collective response in case a real crisis emerges. In that respect, it would be helpful if a roadmap or playbook for a collective response to a (hybrid) crisis is created.[89] This roadmap could address different scenarios in which a collective response by the EU and NATO would be required and could define the respective roles of each of the organisations in those scenarios. Such a roadmap or playbook could also elaborate how and when member states are allowed to chip in or stay out regarding certain counter-hybrid activities, according to their national interests or concerns, without slowing down the rest.

Cyber domain

With regard to the hybrid threats in the cyber domain, EU-NATO cooperation is effectively intensifying, although this is slow. Opportunities for further cooperation remain. First of all, information exchange, including a common understanding of cyber threats and possible countermeasures, offers room for improvement. Yet, some of the obstacles to improved information exchange will not be easy to overcome (see chapter 3).

However, an additional way to improve information exchange may be the following. In July 2021, the European Parliament (EP) proposed the creation of a common EU-NATO cyber threat information hub, as well as a joint EU-NATO Task Force for cybersecurity, in order to define and agree on collective responses to cyber threats. The EP also called for stronger coordination between the EU Agency for Cybersecurity (ENISA) and the NATO Cooperative Cyber Defence Centre of Excellence and for increased EU-NATO coordination as regards establishing collective attribution for malicious cyber incidents.[90] A recent Clingendael report also advocates transforming the existing NATO Cyber Centre of Excellence in Tallinn into a joint NATO-EU Cyber Centre of Excellence that

89 Bruno Lété, 'Cooperation in cyberspace', in: Gustav Lindstrom & Thierry Tardy (eds.), The EU and NATO: The essential partners, European Union Institute for Security Studies, 2019, p. 32 & Information from interviews.

90 European Parliament, EU-NATO Cooperation in the context of transatlantic relations, EP Resolution, P9 TA(2021)0346, 7 July 2021, p. 15.

could provide the main forum for strategic discussions, joint training and exercises.[91] Establishing a completely new institution to further improve EU-NATO cooperation regarding cyber threats does not seem very beneficial[92], yet exploring whether to make existing organisations more 'joint' might be worthwhile to further improve information sharing, staff-to-staff contacts, joint workshops and exercises.

Additionally, synchronisation between the EU and NATO response activities to cyber threats deserves more attention. The EU and NATO could discuss more concretely the delineation of responsibilities and especially of military tasks with regard to cyber threats: when and how should the EU and/or NATO respond to actual cyber threats? For example, a logical division of labour could be an EU focus on enhancing coordination and cooperation among its member states regarding the protection of critical civilian digital infrastructure, while NATO concentrates on enhancing coordination and cooperation among its member states concerning the protection of military digital infrastructure. The focus for both organisations in this regard should be both preventive (sharing threat analysis and protection advice) as well as responsive (in case of actual cyberattacks). The development of a set of EU-NATO basic principles or (non-binding) guidelines on what would trigger a joint response would be a useful step as well. The Tallinn Manual published by the NATO Cyber CoE could offer assistance on how to define these principles while respecting the application of international law.[93] Some experts advocate a common EU-NATO cyber strategy to better align EU-NATO efforts in tackling cyber threats, but currently there seems to be little support for this idea among the member states.[94]

Resilience

Finally, for EU-NATO cooperation in the field of bolstering resilience more steps are needed, despite the progress that has been achieved since 2016. This is underlined by a recent EP resolution on EU-NATO cooperation, which highlights that, for example, "efforts to create more synergies between civilian and military components, to advance common resilience and hence avert future hybrid threats"[95] are necessary. Some even argue that, at present, the resilience strategies of NATO and the EU are not sufficient

91 Dick Zandee, Adája Stoetman & Bob Deen, The EU's Strategic Compass for Security and Defence. Squaring ambition with reality, (The Hague: The Clingendael Institute, May 2021).

92 Supported by the interviews.

93 The NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual *on the International Law Applicable to Cyber Operations,* Cambridge University Press, February 2017.

94 Peter Poptchev, 'NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages', *Information & Security*, vol. 45, 2020, pp. 35-55, especially p. 38; and information from interviews.

95 European Parliament, EU-NATO Cooperation in the context of transatlantic relations, EP Resolution, P9_TA(2021)0346, 7 July 2021, p. 15.

in countering hybrid threats.[96] Fortunately, resilience is an area that has a great deal of potential for further cooperation between the EU and NATO, mainly because this area is not yet very politicised.[97]

In general, more effective counter-hybrid efforts would require tailor-made responses, an increased number of (joint) scenario-building exercises and a change of mindset from a reactive to a proactive approach.[98] In addition, suggestions that have been outlined above to enhance cooperation in the areas of crisis response and cyber security and defence will also contribute to enhancing cooperation in the field of bolstering resilience. In particular, this refers to the following suggestions: more regular organisation of joint counter-hybrid exercises (with a specific focus on resilience); a joint EU-NATO taskforce for resilience building; and clarifying the delineation of responsibilities between the EU and NATO.

Another opportunity to enhance cooperation for the benefit of bolstering resilience lies in disaster relief. During the corona pandemic, the ERCC and the EADRCC have demonstrated that advanced cooperation is indeed possible. The EU and NATO should build upon this experience. This should start with exchanging best practices and lessons learned. This could then be a solid foundation for and ease future cooperation. In addition, the number of (joint) crisis management exercises could be expanded. Such exercises should include those scenarios that test the resilience of member states, including hybrid threats, cyberattacks and pandemics. In case a real crisis would occur, the EU and NATO would already have an idea of what is expected and which actions will be required.

In addition, bolstering resilience at the benefit of countering hybrid threats entails more than merely responding to immediate and sudden calamities and crises. One should also take into consideration, amongst other things, general societal resilience, the resilience of critical infrastructure, protecting the stability of democratic systems, and financial and economic resilience. To assess the potential role of the EU and NATO in these domains, their respective toolboxes should be analysed. In this regard, it makes sense that NATO will be responsible for enhancing the resilience of the critical (military) infrastructure of its member states. In contrast, the EU might be better equipped to promote resilience in the societal, financial-economic and political domain. Both organisations should discuss the delineation of responsibilities in the area of resilience.

96 Friends of Europe, EU-NATO Cooperation. A Secure Vision for Europe, Discussion paper, 3 June 2019, p. 13.

97 See for example Dick Zandee, Adája Stoetman & Bob Deen, The EU's Strategic Compass for security and defence. Squaring ambition with reality, (The Hague: The Clingendael Institute, May 2021), p. 49-50.

98 Friends of Europe, EU-NATO Cooperation. A Secure Vision for Europe, Discussion paper, 3 June 2019, p. 13.

In December 2021, a new Joint EU-NATO Declaration is planned to be released.[99] This occasion should be used to boost cooperation between the two organisations, in particular in view of addressing the changing security challenges of the coming decades. Countering hybrid threats has to be an important part of the new Declaration, not only to fully implement the agreed list of topics but also to explore the potential for additional areas and subjects to increase EU-NATO cooperation.

International cooperation outside the EU-NATO framework

Even though experts have emphasised that, preferably, cooperation on countering hybrid threats occurs within the EU-NATO framework, there is a risk that this is not always possible. The remaining political obstacles to the enhanced use of the EU-NATO format should not restrict the potential for increasing international cooperation on countering hybrid threats. If the 'royal road' is blocked, alternative avenues should be explored. Below, three alternatives for cooperation are outlined: cooperation in European formats; increased EU-US cooperation; and using EU and NATO partnerships.

European formats

European countries cooperate in various constitutions on security and defence matters: bilateral, subregional or other ad hoc formats. An important initiative in this regard is the Permanent Structured Cooperation (PESCO). It is a framework and process to deepen defence cooperation between those EU member states which are capable and willing to do so. Twenty-five EU Member States participate in PESCO and have subscribed to binding commitments to invest, plan, develop and operate defence capabilities together, within the Union framework. The objective is to jointly arrive at a coherent full spectrum of defence capabilities available to the member states for national and multinational missions and operations, not only in the EU context but also for operations in, for example, the NATO or UN context. If the political obstacles to a further improvement of EU-NATO cooperation on countering hybrid threats may be regarded as too difficult to overcome, at least on certain aspects, PESCO may offer an opportunity to invest more in joint counter-hybrid capabilities in the EU context. For example, there are at present already eight PESCO projects in the cyber domain[100], which could contribute to enhancing countering hybrid threat efforts. The third-party rules allow for non-EU states to join PESCO projects. This option is already used by NATO members Canada, Norway and the United States by joining the military mobility PESCO project.

99 See: 2021 State of the Union Address by President von der Leyen, European Commission, 15 September 2021.

100 Information derived from the official PESCO website.

In addition to the options that can be resorted to within the EU framework, there are also many security and defence cooperation formats that exist outside the EU and NATO frameworks. For example, bilateral or subregional arrangements exist between France and the UK, France and Germany, the Benelux countries, the Visegrád-4 and the Nordic countries. All these formats can be used to discuss and streamline national assessments of hybrid threats and to discuss potential responses. Practical results could be introduced by respective member states in the EU and NATO context in order to look for opportunities to widen cooperation potential to other countries, and perhaps to propose new cooperation issues for the EU-NATO list.

EU-US

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

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

101 Harry I. Hannah, 'How the US and EU can counter digital threats together', *The Atlantic Council,* 3 May 2021.

102 Sebastian Sprenger, 'US-European momentum on military mobility still stuck in bureaucracy', *Defense News*, 25 August 2021.

EU and NATO Partnerships

Both organisations have an extensive network of partners across the globe, which should be used for exploring the scope of cooperation in countering hybrid threats. In particular, countries in the Indo-Pacific area are challenged by hybrid threats from China, e.g. Chinese fishing vessels sailing into their waters. Therefore, these countries seem to have a particular interest in teaming up with the EU and/or NATO. The recently released EU strategy for cooperation in the Indo-Pacific refers to the increase in hybrid threats, and announces that cybersecurity cooperation in particular will be strengthened.[103]

Scope for the Netherlands

What could individual member states of the EU and NATO, such as the Netherlands, do to enhance international cooperation in counter-hybrid activities? First and foremost, The Hague should continue to promote increased EU-NATO cooperation. In May 2021, Germany and the Netherlands tabled a food-for-thought paper on enhancing EU-NATO cooperation, including on hybrid threats and cyber resilience.[104] The proposals in this food-for-thought paper should definitely be further discussed in both organisations in order to explore the potential for further action, in particular with regard to situational awareness and resilience. The motto is leading by example, which in this case means: being open to and actively encouraging counter-hybrid cooperation between EU and NATO as much as possible, which may be an effective way to show more hesitating states that this is the most effective way to go.

Secondly, the Netherlands could introduce proposals in other formats, such as the Benelux, bilateral cooperation with larger European countries (France, Germany, the United Kingdom) and in multinational formats such as the Nordic Group. Ideas and proposals could be discussed in these bilateral and multinational formats as a first step. Experience gained in counter-hybrid cooperation in smaller international formats could be used to argue for the application of counter-hybrid cooperation in the EU-NATO context.

103 European Commission, Joint Communication to the European Parliament and the Council – The EU Strategy for cooperation in the Indo-Pacific, JOIN (2021) 24 final, Brussels 16.9.2021.

104 As reported to the Dutch Parliament in a letter containing the report on the NATO Summit of 14 June. The food-for-thought paper itself has not been made public. See: Brief van de minister van Buitenlandse Zaken Sigrid A.M. Kaag en de minister van Defensie Ank Th. B. Bijleveld-Schouten aan de Voorzitter van de Tweede Kamer der Staten-Generaal, Betreft Verslag van de NAVO Top van 14 juni 2021, 25 juni 2021.

Thirdly, The Hague has to be more consistent in making human resources available to the EU and NATO. Due to the job rotation system for Dutch public servants, Dutch policy officers at the EU and NATO often leave their position relatively soon. Generally, it takes some time to gain knowledge of the organisations' cultures and working methods before one can have an effective influence. This is particularly true for staff seconded to departments that deal with very complex matters such as hybrid threats. Some interviewees praised the quality of Dutch personnel among EU and NATO staff, but regretted that they leave too soon and do not return for a second or third posting during their career. The Dutch influence could increase if public servants could stay longer in a position or could return more often to positions in the EU or NATO. More coordinated efforts to promote Dutch candidates to key staff positions could also be considered, and strategic secondments might be an option as well in order to gain more influence in practical staff-to-staff cooperation.

5 Conclusions and recommendations

Cooperation between the EU and NATO in countering hybrid threats is not only desirable, but even necessary. Considering the broad and dynamic area of threats, both organisations cannot deal with them alone and their toolboxes are complementary. This is also realised within both organisations and their member states, as can be seen in the intensified cooperation of the past few years.

There is no internationally agreed definition of hybrid threats. However, the common ground between all available definitions is that hybrid threats consist of a combined use of military and non-military means to undermine societies. Less clear is which activities should be included in the toolbox for countering hybrid threats, although undoubtedly they have to consist of a mix of military and non-military measures. The absence of an agreed definition – also in the EU-NATO context – leaves room for flexibility in expanding cooperation between the two organisations in countering hybrid threats.

What has been achieved so far?

Countering hybrid threats makes up for approximately one third of the total of 74 projects on the EU-NATO list, thereby underlining the importance of the topic as an area of cooperation between the two organisations. These 22 cooperation areas are distributed over five categories: situational awareness, strategic communications, crisis response, bolstering resilience, and cyber security and defence (the last area listed in a separate section of the list, but generally considered as 'hybrid'). Generally, EU-NATO cooperation in those five areas has improved in recent years. As the assessment table at the end of chapter 2 shows, staff-to-staff contacts have expanded in all categories. Furthermore, the structured (political) dialogue and joint exercises are important highlights for underscoring the positive judgment. The Helsinki-based European Centre for Countering Hybrid Threats – being neither an EU nor a NATO institution but open to all member states of both organisations – plays a key role as the hub for sharing information and offers the dating venue of national and international experts.

However, the record is more mixed when cooperation starts to involve the formal exchange of information, developing common approaches, combining analyses and initiating activities involving both the EU and NATO. There is still a considerable gap between the political rhetoric of 'EU-NATO cooperation is going well' and the reality of real and concrete 'working together'. One example is that the agreed list

of EU-NATO cooperation areas is not fully used. For example, cooperation in the area of situational awareness has not progressed in the sense that both sides have a shared threat assessment. The same applies to the cyber security and defence area, in which the identification of potential synergies in responding to cyber threats has not been operationalised. Another example is that the list has remained unchanged since 2017, while new hybrid threats have emerged such as the use of migrants as a weapon by Belarus.

Important obstacles to enhanced EU-NATO cooperation continue to exist, despite the well-functioning high-level political contacts between the two organisations. Some of these obstacles might be overcome in due course – such as recognising the different character and nature of the EU institutions and the NATO organisation – but others are likely to remain, at least for the foreseeable future. The political blockade caused by the Turkey-Cyprus issue remains the key factor that hinders a better use of the formal cooperation channels and continues to block the exchange of classified information. Staff are able to circumvent the sharing of (classified) documents, but a full exchange of information among all member states of both organisations is a hurdle that cannot be cleared. Thus, caution is needed to consider a widening of staff-to-staff contacts as the panacea to improve EU-NATO cooperation. The staff contacts can certainly be used to deepen the cooperation at that level, but they cannot replace the required political willingness of all EU member states and NATO Allies to agree to the exchange of all required information. Related to the information exchange blockade is the lack of a secure communications system between the two organisations – a primary requisite if this issue is to be addressed and resolved in the future. Finally, member states themselves can be reluctant in sharing information related to hybrid threats and responses as they regard this to be a domain within predominantly national responsibility.

Potential for future cooperation

The EU and NATO, based on the 2016-2017 list of common proposals, have focused the cooperation efforts since then on concrete matters. However, the orientation on items such as situational awareness, crisis response and the other headings of the list ignores the need for a strategic vision. The focus tends to lie on finding appropriate responses to the deployment of hybrid tools, while less attention is paid to the actors' objectives and intentions behind the use of these hybrid tools.[105] Adopting a more strategic approach, in which more focus would be directed towards the objectives and intentions of (potential) adversaries, could benefit both organisations in the long run. A strategic dialogue between the EU and NATO at the level of high-level officials and in ministerial

105 Information from interviews.

meetings could be a way to overcome this shortfall. Naturally, China and Russia would be high on the agenda for the EU and NATO in determining the strategic level objectives and intentions of these major powers.

The past record of EU-NATO cooperation shows that progress can be made, but step-by-step and at a relatively slow pace. As the overall conditions for speeding up the cooperation between the two organisations remain unchanged due to the political blockades of the Turkey-Cyprus problem, it is unlikely that big steps can be taken. At the same time, the EU and NATO could take two other steps. Firstly, there is still scope for fully implementing the existing 22 proposals dating back to 2016-2017. This applies in particular to training and exercises as well as to further exploiting the use of the Hybrid CoE in Helsinki as the information-exchange hub and dating venue for experts. Secondly, future cooperation could be expanded as stated below, including the use of other formats which could offer more potential for deepening cooperation, also in countering hybrid threats.

Recommendations

Expectation management

- Adopting a more strategic approach towards countering hybrid threats, whereby the emphasis should lie on the strategic objectives and intentions of (potential) adversaries.
- Clearer and publicly identifying the capabilities and comparative advantages of both organisations when it comes to (jointly) countering hybrid threats.
- High-level retreats, organised by the Helsinki-based Hybrid Centre of Excellence, should be restarted to explore these issues with EU and NATO staff members together.

Information sharing

- Intensifying the exchange of open-source information, for example by creating a digital information-sharing platform in which relevant stakeholders, both civilian and military, could share information and research on hybrid activities. Potentially, certain external stakeholders could be included to some extent as well so as to enhance the 'whole-of-society' approach.
- Exploring options for a shared communication platform for the exchange of certain classified information, perhaps based on a number of priority categories.

Crisis response

- NATO and EU staff should structurally embed the regular exchange of information and scenarios in their coordination and cooperation processes, so that this becomes common practice for both organisations. More efficient synchronisation of the EU's and NATO's crisis response mechanisms including creating additional capacity.
- Creating a joint roadmap or playbook for a collective response to (hybrid) crises, addressing different scenarios in which a collective response by the EU and NATO would be required and define the respective roles in those scenarios.
- In this context, exercises should be organised more often, helping to deepen cooperation between the two organisations and their member states.

Cyber threats

- Exploring the potential of making existing organisations, in particular the NATO Cyber CoE, more 'joint' to further improve information sharing, staff-to-staff contacts, joint workshops and exercises.
- Delineation of responsibility and especially of military tasks with regard to cyber threats: when and how should the EU and/or NATO respond to actual cyber threats?
- Development of a set of EU-NATO basic principles or (non-binding) guidelines on what would trigger a joint response would be a useful first step.

Resilience

- Increasing the number of joint scenario exercises, including a change of mindset from a reactive to a proactive approach: more regular organisation of joint counter-hybrid exercises (with a specific focus on resilience); a joint EU-NATO taskforce for resilience building; and clarifying the delineation of responsibilities between the EU and NATO.
- Bolstering resilience in the area of disaster relief by expanding the cooperation between NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and the EU Emergency Response Coordination Centre (ERCC), starting with exchanging best practices and lessons learned. Include pandemics in (joint) exercises.
- Assess the potential roles of the EU and NATO in areas such as general societal resilience, the resilience of critical infrastructure, protecting the stability of democratic systems, and financial and economic resilience.

New EU-NATO Joint Declaration

- Insert in this Declaration, to be released in December 2021, a more strategic approach by the two organisations in countering hybrid threats, such as a delineation of responsibilities and listing additional areas of counter-hybrid cooperation.

Other formats

- Noting that the existing limitations in EU-NATO cooperation will continue, explore the use of other formats, such as: third countries' participation in Permanent Structured Cooperation projects; using other European security and defence cooperation models; and explore the cooperation potential in the EU-US dialogue context.
- Discuss options for cooperation with partners, in particular with countries challenged by hybrid threats from China, as called for in the EU Strategy for cooperation in the Indo-Pacific.

Actions to be undertaken by the Netherlands

- Inject constructive ideas into debates within both organisations, bridging various perspectives and sensitivities, while realising that patience is required to allow other member states to overcome sensitivities or not to chip in because of other priorities or a lack of specific resources.
- Introduce and generate discussion on ideas and suggestions for EU-NATO cooperation in bilateral and subregional formats (such as the Benelux and the Nordic Group) and with larger European countries (France, Germany, the UK).
- Ensuring high-quality staff in key positions by allowing national public servants to stay longer in a position or to return more often to positions in EU or NATO. Coordinated efforts to promote able candidates to key staff positions and strategic secondments to gain more influence in practical staff-to-staff cooperation are an option as well.