Briefing
March 2017

European Parliament

Countering hybrid threats:
EU-NATO cooperation

SUMMARY

The concept of hybrid threat has gained traction in relation to Russia's actions in Ukraine and the ISIL/Da'esh campaigns going far beyond Syria and Iraq. Faced with this constantly evolving challenge, the European Union and NATO have taken several steps to strengthen their respective capabilities and pursue common objectives through closer cooperation. The EU-NATO joint declaration adopted in July 2016 in the margins of the Warsaw NATO Summit represents a clear step forward in this regard. The document outlines new areas for practical cooperation, in particular with regard to hybrid threats, building resilience in cybersecurity, and strategic communications.

The Council conclusions of 6 December 2016 stressed that the implementation of the joint declaration is a key political priority for the EU. It welcomed the progress achieved in advancing EU-NATO relations, including implementing and operationalising parallel procedures and playbooks for interaction in countering hybrid threats. With a view to ensuring further progress, the Council endorsed a common set of proposals focused on better coordination, situational awareness, strategic communication, crisis response, and bolstering resilience. The North Atlantic Council endorsed the same set of measures. Reports on implementation, including possible suggestions for future cooperation, should be provided on a biannual basis from the end of June 2017.

This is an updated edition of an At a Glance note published in June 2015.

In this briefing:

EPRS | European Parliamentary Research Service
Author: Patryk Pawlak
Members' Research Service
PE 599.315

Hybridity: a new normal?

The concept of hybrid threat has been revived in relation to Russia's actions in Ukraine and the ISIL/Da'esh campaigns going far beyond Syria and Iraq. However, elements of hybridity can be traced in many other dimensions of the current security environment. Various governments in the EU's southern neighbourhood (i.e. the Gaddafi regime in Libya or the current government of Turkey) have used the complexity of migratory movements as a pretext to demand various concessions from the European Union. Simultaneously, ISIL/Da'esh seeks to instil fear in EU citizens and governments, pushing them to take more hostile attitudes towards refugees, ultimately strengthening the image of the EU as an anti-Muslim society, to its discredit.

In addition to intentional actions, there are increasing concerns about the potential consequences of complex crises that result from or combine different elements that require an equally complex response. Abnormal weather conditions and climate-induced resource scarcity, for instance, increasingly influence relations between states, and might provoke confrontation over access to water or crops production. Researchers on the impact of climate change in the Middle East and North Africa have found that, by 2050, summer temperatures across the region will reach around 46 degrees Celsius and that hot days will occur five times more often than was the case at the beginning of the 2000s. Such extreme temperatures, in combination with increasing air pollution by windblown desert dust, will render living conditions in parts of the region intolerable, leading to a 'climate exodus' and social unrest, that might be exploited to destabilise the region by state and non-state actors alike.

As these examples suggest, the term 'hybrid threat' is a metaphor that captures complexities and dilemmas related to a changing global environment. As such, it is a useful concept that embraces the **interconnected nature** of challenges (i.e. ethnic conflict, terrorism, migration, and weak institutions); the **multiplicity of actors** involved (i.e. regular and irregular forces, criminal groups); and the diversity of **conventional and unconventional means** used (i.e. military, diplomatic, technological). Taking into account different levels of intensity of a threat and the intentions of actors involved, it is useful to introduce a conceptual distinction between hybrid threat, hybrid conflict and hybrid war.

- **Hybrid threat** is a phenomenon resulting from the convergence and interconnection of different elements, which together form a more complex and multidimensional threat.
- **Hybrid conflict** is a situation in which parties to the conflict refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.
- **Hybrid war** is a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic).

Most references to hybrid war encompass the notion of an adversary who controls and employs a mix of tools to achieve their objectives. Establishing responsibility and intentionality of actions is necessary to ensure that the policy response is legitimate and proportionate. However, this is not always easy in practice, due to the limitations of international law, technological constraints, or the diffusion of power to non-state actors, which increase the opportunities for deniability. For instance, due to technological limitations and the involvement of non-state actors, it is currently difficult to attribute,

beyond any doubt, a cyber-attack to a specific country. Nonetheless, the US government has in the past indicted Chinese officials suspected of involvement in cyber-attacks against its computer networks, and imposed sanctions on North Korea following the attack on Sony Pictures Entertainment. In January 2017, the USA imposed sanctions on Russian individuals and entities over 'significant malicious cyber-enabled activities' against the Democratic Party. Without prejudice to these two cases, there is a risk that an excessive focus on hybridity may lead to misunderstandings and escalation even though certain events may be beyond the control of any particular actor or an accident.

Adjusting to hybrid challenges

Even though no international legal framework specifically regulates hybrid conflict or hybrid warfare, any use of force in international relations is regulated by the United Nations Charter, which states clearly that, in the absence of an armed attack against a country or its allies, a member state can use force legally only if authorised by a United Nations Security Council resolution. Rules and principles regarding armed conflict are laid down in international humanitarian law and human rights law. With regard to hybrid conflict and threats, a patchwork of legal instruments covers specific policy areas, including the seas, counter-terrorism, money laundering and terrorist financing, and human rights. At the same time, as the application of existing international law and the functioning of global governance institutions becomes increasingly complicated, the meaning of concepts such as sovereignty, legitimacy and legality is constantly challenged, and in some cases redefined. The continued military, economic and political action against the ISIL/Da'esh forces, the debate on the application of existing international law in cyberspace, and maritime disputes in the South China Sea, are all good examples of the challenges stemming from this complexity. Consequently, it is important to understand that any adjustments made to the existing legal and institutional framework will have a long-term impact on the stability of the international order and may eventually result in global power shifts. In that respect, several trends stand out:

- **Conceptual trends**: Government-led comprehensive approaches are increasingly complemented by whole-of-society strategies aimed at managing risks and building resilient societies. The focus on resilience helps to mitigate risks that might lead to hybrid conflicts in the future (i.e. over energy or access to water), and improves associated resource management practices.
- **Material trends**: Resources to counter hybrid threats reside with many different stakeholders, including governments, civil society, the private sector, and individual citizens. This joint ownership is reflected in public-private cooperation on security and development. At the same time, many governments have recently taken concrete steps to increase and modernise their civilian and military capabilities.
- **Legal trends**: Some of the present legal concepts and frameworks are anachronistic and do not always address hybrid threats adequately. This leads increasingly to incoherent application of the existing rules, whereby states use treaties and conventions selectively in order to justify their positions. The choice between status quo and new instruments might increase the need for alternative approaches (i.e. confidence building measures, law enforcement cooperation, etc.).
- **Institutional trends**: Many countries have adjusted to hybrid threats by expanding the missions of existing institutions (i.e. new powers for intelligence agencies, bolstering EU strategic communication) or creating new organisations (i.e. the Ministry of Truth in Ukraine).

Another challenge lies in the fact that current policy responses are based on a rather static picture of the security environment (i.e. something is, or is not, a hybrid threat) while not giving due recognition to the dynamic nature of hybridity (i.e. processes through which certain situations evolve to become hybrid threat or result in a hybrid conflict and motivations or reasons behind these processes).

NATO approach: the curse of hard power

Concerns about hybrid threats were first reflected in NATO's 2010 strategic concept and incorporated in NATO's capstone concept, which defined hybrid threats as 'those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'. Due to their complex nature and because their inherent operations in the grey area between what is legal and illegal under international law, hybrid threats challenge the need for a maximum certainty, a basic assumption underpinning the collective self-defence principle, expressed in Article 5 of the North Atlantic Treaty. The lack of operational certainty about the intensity of the conflict also pushed NATO members towards more frequent consultation of the North Atlantic Council under Article 4 of the Washington Treaty, including with regard to the conflict in Eastern Ukraine (invoked by Poland on 3 March 2014), terrorist attacks in Suruç (invoked by Turkey on 26 July 2015), and conflict in Syria (invoked by Turkey on 22 June and 3 October 2012).

Several elements of NATO's response to hybrid threats emerge from the comprehensive approach to crises and were gradually strengthened, starting with the adoption of the comprehensive approach action plan in the 2008 Bucharest Summit Declaration and the 2010 Lisbon Summit Declaration. A comprehensive approach to crisis management provides a framework for combining political, civilian and military crisis management instruments and requires multiple actors – including from the private sector and NGOs – to contribute to a concerted effort, taking their respective strengths, mandates and roles into account. At the Wales Summit, NATO members agreed the readiness action plan (RAP) to ensure the Alliance is ready to respond swiftly and firmly to new security challenges, including through additional assurance measures (e.g. air-policing patrols over the Baltic States, AWACS surveillance flights, maritime patrol of the Baltic Sea and the Eastern Mediterranean), and adaptation measures (e.g. the NATO Response Force, the Very High Readiness Joint Task Force – also known as 'spearhead force', NATO Force Integration Units across Europe, and high readiness multinational headquarters). NATO's decision to extend the application of Article 5 to cyberattacks represents a significant step, even though no threshold for triggering a collective-defence mechanism was established. In December 2015, the NATO Foreign Affairs ministers adopted a strategy on hybrid warfare, supplemented by the NATO hybrid warfare playbook, laying out who does what in dealing with complex security threat scenarios that combine militias, cyber-attacks, targeting of critical infrastructure, as well as types of assistance the alliance would provide should a member state come under outside pressure. The task of articulating, elaborating, and developing strategies to meet hybrid threats has been assigned to NATO Allied Command Transformation (ACT). At the 2016 NATO Summit in Warsaw, the Allies adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. While acknowledging the readiness to counter hybrid warfare as part of collective defence and the willingness to assist an ally at any stage of a hybrid campaign, NATO clearly assigns the primary responsibility to respond to the targeted nation.

European Union response: soft power in action

At an informal meeting in Riga, in February 2015, EU Defence Ministers called for greater unity and concrete action at EU level. In May 2015, the European External Action Service circulated a food-for-thought paper on 'countering hybrid threats', which reaffirms that the EU needs to be able to recognise the overall effect of hybrid threats, and counter them by building more resilience. The Foreign Affairs Council of 18 May 2015 invited the High Representative to present a joint framework with actionable proposals to help address hybrid threats and foster the resilience of the EU, its Member States and partners. In June 2015, the European Council re-stated the need to mobilise EU instruments to help counter hybrid threats in a comprehensive way, making better use of all instruments at the EU's disposal (diplomatic, military, economic, technological). This led to the joint framework on a European Union response to countering hybrid threats, presented in April 2016, and welcomed in the Foreign Affairs Council conclusions of 19 April 2016. While the framework reaffirms states' primary responsibility for countering hybrid threats related to national security and defence and the maintenance of law and order, it also states that threats with a cross-border dimension (i.e. to communication networks, infrastructure, etc.) can be more effectively addressed through cooperation at EU level, making the full use of EU instruments and the potential of the Lisbon Treaty. The communication particularly focuses on:

- **Improving situational awareness** by monitoring and assessing EU vulnerabilities, including through developing security risk assessment methodologies and promoting risk-based policy formulation. That includes, among other things, establishing a European Centre of Excellence for designing strategies to counter hybrid threats, creating an EU hybrid fusion cell, raising public awareness about hybrid threats through strategic communication, and closer dialogue and cooperation with other stakeholders such as NATO, regional organisations and the private sector.
- **Building resilience** (i.e. the capacity to withstand stress and recover from shocks or crisis) into critical infrastructure networks (e.g. energy, transportation, space), protecting public health and food security, enhancing cybersecurity, tackling radicalisation and violent extremism, strengthening strategic communication, developing relevant defence capabilities, and improving relations with third countries.
- **Strengthening the ability of Member States and the Union to prevent and respond to crisis, and for coordinated recovery**. The EU will make full use of existing mechanisms such as the European Emergency Response Coordination Centre or EU Integrated Political Crisis Response (IPCR), and Treaty-based instruments like the Solidarity Clause or Mutual Assistance Clause. Common Security and Defence Policy is an important element of the EU approach, in particular with regard to civilian and military training, advisory missions to strengthen the capacities of states under threat, strengthening early warning capabilities and contingency planning, support for border control management, and specialised assistance in areas such as chemical, biological, radiological or nuclear (CBRN) risk mitigation or non-combatant evacuation.
- **Cooperation with NATO** to ensure complementarity of measures undertaken, including on situational awareness, strategic communication, and cybersecurity.

The global strategy for EU foreign and security policy of June 2016 stressed the importance of a joined up response through building tighter institutional links between internal and external action, creating synergies between defence policy and policies covering the internal market, industry, law enforcement, judicial and intelligence services. The implementation plan on security and defence – one of the elements of the

defence package that resulted from the debate about the implementation of the EU global strategy – stressed the possible use of Common Security and Defence Policy (CSDP) missions and operations to provide expertise and assistance to strengthen partners' resilience and counter hybrid threats. Possible areas of engagement include strategic communication, cybersecurity and border security. The European defence action plan presented by the Commission in November 2016 and endorsed by the European Council in December the same year, puts forward several concrete initiatives that contribute to strengthening EU capacity to respond to hybrid threats, such as launching a European Defence Fund, fostering investment in the defence supply chain, and reinforcing the single market for defence. In July 2016, the European Commission and EEAS presented the EU operational protocol for countering hybrid threats – the so-called 'EU Playbook' – which outlines the modalities for coordination, intelligence fusion and analysis, informing policy-making processes, exercises and training, and cooperation with partner organisations, notably NATO. The first report from the Commission and the High Representative is expected by July 2017.

EU-NATO cooperation on hybrid threats

The analysis of complex challenges facing the EU and NATO led both organisations to develop a comprehensive approach that blends all relevant actors and available instruments: military forces, diplomacy, humanitarian aid, political processes, economic development, and technology. Countering hybrid threats is about gaining new understanding of such threats and the innovative use of existing capabilities, many of which – like economic development, the fight against corruption or eliminating poverty – reside in non-military governmental and intergovernmental agencies, private sector and international non-governmental organisations. Acknowledging the need for dialogue and coordination with like-minded partners in countering hybrid threats, the EU's joint communication and EU playbook identified a number of areas for closer EU-NATO cooperation, including situational awareness, strategic communications, cybersecurity, and crisis prevention and response. The commitment to a deeper partnership with NATO in countering hybrid and cyber threats was also expressed in the European Union global strategy of June 2016. EU-NATO cooperation was discussed at the European Council on 28 June 2016, and contributed to the adoption of the EU-NATO joint declaration at the NATO Summit in Warsaw (8-9 July 2016). The EU-NATO declaration outlines the new areas for practical cooperation to strengthen capacity to deal with hybrid threats, in particular through building resilience, situational awareness, and strategic communications.

Hybrid threat cooperation priorities in the EU-NATO joint declaration

- Ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, early detention, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response. The development of coordinated procedures through respective playbooks will contribute to implementing these efforts;
- Coordination on cyber security and defence, including in the context of their missions and operations, exercises and on education and training;
- Coordination on exercises, including on hybrid threats, by developing parallel and coordinated exercises;
- Defence and security capacity building and fostering resilience of partners in the east and south.

A number of concrete proposals were circulated in advance of the NATO summit in Warsaw, but have not been formally adopted. In April 2016, a group of 10 NATO member states (Croatia, Denmark, Germany, Latvia, Lithuania, Norway, Poland, Romania, the United Kingdom and the USA) presented a 'food for thought' (FFT) paper on **NATO-EU**

counter hybrid teams (CHTs). The paper proposes CHTs, including a Brussels-based 'hub' (modelled on the NATO-EU joint analysis platform proposed in the German FFT paper in October 2015) and CHT 'spokes', established at the request of individual countries. According to the proposal, counter hybrid teams – in complement to the ongoing process of strengthening deterrence and defence – would be relatively small, and include officials from NATO, EU Member States and EU institutions with expertise in emergency response, counter-terrorism, border management, intelligence analysis, energy security or strategic communications. Their main functions would be information fusion and analysis to enhance situational awareness in support of the decision-making process, preparation for, and resilience against hybrid threats, and response to hybrid threats.

Table 1 – Implementation of the EU-NATO declaration: common set of proposals

Policy area	Actionable points for 2016-2017
Coordination	• Encourage participation by EU and NATO as well as EU Member States and NATO Allies in the work of the European Centre for Countering Hybrid Threats
Situational awareness	• Propose concrete measures to enhance staff-to-staff sharing of time-critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart, including by exchanging analysis of potential hybrid threats and establishing the technical means that facilitate such systematic exchange of information
Strategic communication	• Intensify cooperation and undertake shared trend analysis of misinformation, including through social media targeting the EU and NATO; • Cooperate to improve quality and outreach of positive narrative; • Enhance mutually reinforcing efforts regarding support for partner countries' 'stratcom' capabilities, including through coordinated or joint training and sharing of platforms. • Encourage cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS Stratcom Division (specifically Task Forces East and South) including further joint training/seminars.
Crisis response	• Enhance preparedness, inter alia, by holding regular meetings at staff-to-staff level. • Seek to synchronise the two organisations' parallel crisis response activities with the goal of providing coherent support in response to hybrid threats (i.e. the integrated political crisis response arrangements and NATO's crisis response system).
Bolstering resilience	• Intensify staff contacts, 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 capability development plan and the NATO defence planning process • Work to be ready to deploy, 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.

Policymakers in the EU and NATO have been also involved in preparing a **EU-NATO hybrid playbook** that would establish interfaces for effective interaction between EU and NATO in responding to instances of a recognised hybrid attack, including establishing contacts between crisis management structures and points of contact in the functional areas

mentioned above, political coordination between the Political and Security Committee (PSC) of the EU and the North Atlantic Council (NAC), sharing relevant information, and coordination of strategic communication messaging and on crisis management coordination structures. However, the plan has not materialised, primarily due to arguments that the EU's response to hybrid threats goes far beyond purely military means and as such should not be linked exclusively to cooperation with NATO. Consequently, each side has developed its own approach, albeit in close cooperation. The 'EU playbook', for instance, envisages operationalisation of EU-NATO cooperation in four areas 'based on the principle of inclusiveness, while respecting each organisation's decision-making autonomy'. These are: situational awareness, strategic communication, cybersecurity, and crisis prevention and response.

From declaration to implementation

The Council conclusions of 6 December 2016 stressed that the implementation of the joint declaration is a key political priority for the EU. It welcomed the progress achieved in advancing EU-NATO relations, including in implementing and operationalising parallel procedures and playbooks for interaction in countering hybrid threats. With a view to ensuring further progress, the Council endorsed the common set of proposals focused on better coordination, situational awareness, strategic communication, crisis response, and bolstering resilience. The North Atlantic Council endorsed the same set of measures. Reports on implementation, including possible suggestions for future cooperation should be provided on a biannual basis starting by the end of June 2017. Coordination between the two organisations continues in the framework of an informal EU-NATO staff-to-staff dialogue on hybrid threats.

The case of EU-NATO cyber defence cooperation

As the case of the US Presidential elections has demonstrated, cyberspace presents policymakers with a set of challenges of a political and technological nature. As such, it also provides a space for misunderstandings and conflict escalations and deserves a more detailed discussion. As digital networks now constitute the backbone of our societies' functions (i.e. financial systems, energy infrastructure, political systems, and communication tools), there is a risk that organised criminal groups or foreign governments will exploit their vulnerabilities. Many countries have included the protection of critical information infrastructure in their national security strategies. Due to the fact that criminal networks often operate in several jurisdictions, or receive support from third country governments, and that some cyber-attacks might pose a serious threat to a state's security – potentially resulting in a military conflict – the EU-NATO discussion about secure and safe cyberspace necessarily involves both diplomats and military staff. The need to think in broad national security terms (something which law enforcement and critical infrastructure operators are not always used to doing), and a possible response going beyond law enforcement, technical measures or national borders (which other actors are not empowered to do), brings diplomats and 'cyber soldiers' into the picture.

According to United States intelligence, a limited number of countries (including China, Russia, and Iran) have the capacity to disable the computer systems of power utilities, financial institutions or aviation networks. However, establishing in practice whether a cyberattack constitutes an armed attack, whether it constitutes a legitimate use of force (*jus ad bellum*), and how force may be employed (*jus in bello*), remains contentious among international legal scholars. The basic conceptual framework for EU-NATO

cooperation in this respect is provided in the report of the United Nations Governmental Group of Experts (UN GGE), published in June 2015. The report sets out the norms regulating state behaviour. These forbid states to knowingly allow their territory to be used for cyber-attacks; to conduct or knowingly support attacks that damage critical infrastructure; to conduct or knowingly support activity intended to harm the information systems of another state's emergency response teams (CERT/CSIRTS), and to use their own teams for malicious international activity. However, their voluntary nature means that further diplomatic efforts are likely to be needed to find a consensus with countries like China and Russia on the practical steps towards their implementation.

Cyber defence in the EU

EU-NATO cyber defence cooperation builds on the respective developments on each side. In the EU, the EU cyber security strategy adopted in 2013 lists developing cyber defence policy and capabilities related to the framework of the CSDP as one of its main objectives. The June 2013 Council conclusions on the cybersecurity strategy of the EU further stressed the need to strengthen EU-NATO cooperation on cyber defence and identifying priorities for continued cyber defence cooperation within the existing framework. The EU cyber defence policy framework adopted by the Council in November 2014 further strengthened the EU's thinking about cyber defence, including with regards to supporting the development of Member States' cyber defence capabilities related to CSDP and enhancing cooperation with relevant international partners, most notably NATO. In policy terms, the Horizontal Working Party on Cyber Issues provides an overall coordination function where various proposals are discussed, such as on developing a joint EU diplomatic response against coercive cyber operations. In 2016, Member States also approved the EU concept on cyber defence for EU-led military operations and missions drafted under the auspices of the European Union Military Staff. The European Defence Agency (EDA), on the other hand, plays a particularly relevant role in ensuring operational synergies between the EU and NATO. Cyber defence has been added to the collaboration database (CoDaBa) and is fully integrated in the new capability development plan (CDP) tool by the EDA. Several projects are also implemented under the pooling and sharing umbrella, including cyber ranges, deployable cyber situation awareness packages for headquarters (CySAP), a multi-agent system for advanced persistent threat detection (MASFAD), and pooling of EU member states' demand for private sector training.

Cyber defence in NATO

At the 2014 NATO Summit in Wales, members adopted the NATO enhanced policy and action plan on cyber defence. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, however, it has not established any clear procedures or thresholds for the use of Article 5 for cyber defence, insisting that this will be a political decision taken on a case-by-case basis. Such an approach is in line with arguments presented by legal scholars, who argue that damage or destruction of data does not necessarily generate consequences that would qualify them as an armed attack. An automatic acceptance that a cyber-attack constitutes armed conflict would otherwise substantially lower the threshold at which states have a right to use force in their response to actions directed at them. The decisions taken at the Wales summit have resulted in several concrete initiatives that contributed to streamlining cyber defence governance, procedures for assistance to allied countries, and integration of cyber defence into operational planning. NATO's approach to cyber defence policy was further advanced at the Warsaw Summit in July 2016. The Warsaw Summit communiqué reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of

operations in which NATO must defend itself. Through the cyber defence pledge, NATO members have committed to enhance the cyber defences of their national networks and infrastructures, as a matter of priority. While emphasising NWTO's role in facilitating cooperation on cyber defence, including through multinational projects, education, training, and exercises and information exchange, the pledge reaffirms the responsibility of each member state to enhance the cyber defences of national infrastructures and networks. In line with Article 3 of the Washington Treaty, the pledge ensures that the Alliance is 'cyber aware, cyber trained, cyber secure and cyber enabled'. While advancing its cyber defence capabilities and doctrine, NATO has acknowledged its commitment to international law, including the UN Charter, international humanitarian law, and human rights law, as applicable. A regular annual assessment based on agreed metrics will help to monitor and review progress in the implementation of the pledge.

EU-NATO cooperation

EU-NATO cooperation on cyber defence has picked up speed with the high level staff-to-staff consultations held in January 2015. Regular cooperation has also taken place at the working level between the European Union Military Staff (EUMS), EDA and NATO C3 staff. Regular cross-briefings on cyber defence issues have also taken place in the Political-Military Group and relevant NATO committees. Regarding the development of capabilities, NATO (Allied Command Transformation, NATO Communications and Information Agency) has been accepted as an observer to the cyber ranges project and EDA has been invited as an observer for the NATO cyber education, training and exercises NATO smart defence project led by Portugal. An important milestone in the implementation of the EU cyber defence policy framework was reached with the signing of the European Union and NATO technical arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU) on 10 February 2016. The agreement aims to improve cyber incident prevention, detection and response in both organisations, by facilitating technical information sharing between NCIRC and CERT-EU. This will be achieved, for instance, through sharing of routine information exchange products (e.g. non-public indicators of compromise, situational awareness, reports), sharing of event or incident related information, as well as visits to facilities and laboratories.

Elements of NATO's cyber defence pledge

I. Develop the fullest range of capabilities to defend national infrastructures and networks;
II. Allocate adequate resources nationally to strengthen cyber defence capabilities;
III. Reinforce the interaction amongst respective national cyber defence stakeholders to deepen cooperation and the exchange of best practices;
IV. Improve understanding of cyber threats, including the sharing of information and assessments
V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.

The political mandate for enhanced EU-NATO cyber defence cooperation was provided at the NATO Summit in Warsaw in July 2016. The EU-NATO joint declaration of 8 July 2016 highlighted the need to expand coordination on cybersecurity and defence. A set of concrete proposals for the implementation of the declaration was adopted by the Council

of the EU and the NATO Ministers of Foreign Affairs on 6 December 2016. The list includes measures aimed at enhancing cooperation on cybersecurity and defence, such as:

- Exchange of 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.
- Strengthening cooperation on training through harmonisation of training requirements, where applicable, and open training courses for mutual staff participation.
- Fostering cyber defence research and technology innovation cooperation by further developing the links between EU, NATO and the NATO Cooperative Cyber Defence Centre of Excellence to explore innovation in the area of cyber defence.
- Strengthening cooperation in cyber exercises through reciprocal participation in respective exercises, including 'cyber coalition' and 'cyber Europe' in particular.

Stakeholders' views

A need for closer EU-NATO cooperation, including on countering hybrid threats, has been stressed by many observers. In a 2015 report, researchers from the Clingendael Institute pointed to the paradox that, while NATO is 'ill-suited' and struggling to respond to hybrid threats, the EU relies exclusively on non-military instruments such as diplomatic-political measures; economic, trade and energy policies; and, financial and economic sanctions. The authors make several observations regarding EU-NATO cooperation in countering hybrid threats, such as: the need to make maximum use of the informal formats of meetings involving representatives of all member states of both organisations; fully align their responses to the hybrid threats from the east and the south; transmitting the same strategic message to their challengers; underlining the principles and norms that both organisations stand for; and agreeing on a set of common criteria for escalatory and de-escalatory steps. In a more recent study on 'Forward resilience' by the Center for Transatlantic Relations, a group of scholars has focused primarily on responding to hybrid threats through making resilience-building an important element on the EU-NATO agenda. A set of concrete recommendations proposed in the report includes: developing mechanisms for institutional cooperation, including a NATO-EU Resilience Coordinating Council; pooling EU and NATO resources for the Forward Resilience Advisory Support Teams; establishing a comprehensive system of national resilience indicators; holding joint crisis management exercises with a focus on forward resilience; and supporting the Center of Excellence for Countering Hybrid Threats, based in Helsinki.

What role for the European Parliament?

The basic premise for closer EU-NATO cooperation in countering hybrid threats is that effective response and resilience against a wide range of threats require a mix of military and non-military capabilities. Given that hybridity assumes operations under the threshold of an armed conflict, the EU's soft power is particularly valuable. Following the changes introduced in the Lisbon Treaty, the European Parliament has substantial power to influence EU policy in areas such as emergency response, counter-terrorism, border management, law enforcement, energy security or cybersecurity. At the same time, the Parliament contributes to shaping policies in areas under Member State competence, including intelligence cooperation and defence. Consequently, the main challenge remains maintaining a balance between military and non-military capabilities and instruments, including how to shape relations between civilian and military aspects of security and defence, in particular how to ensure that military high readiness is matched

by the exercise of political agility in response to hybrid threats. The Parliament welcomed the joint framework on countering hybrid threats in its resolution of 23 November 2016 on EU strategic communication to counteract anti-EU propaganda by third parties. Regarding cyber defence, in its November 2016 resolution on the implementation of the Common Security and Defence Policy, Parliament underlined the need 'to further deepen cyber defence cooperation and to ensure full cyber-resilience of CSDP missions'. The resolution also calls on the Member States 'to take full use of cyber capacity-building measures under the responsibility of the European Defence Agency (EDA) and to make use of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)'.

While countering hybrid threats requires a mix of soft and hard security measures aimed at building resilience, there is also a risk that too close alignment of the EU response to hybrid threats with NATO's approach – which is primarily a military alliance – risks shifting the optics towards a military prism. Consequently, one of the key tasks is identifying roles and the comparative advantages of partnerships with other regional organisations, including the World Bank, the African Union, as well as NATO's Mediterranean dialogue, the Istanbul cooperation initiative and the Partnership for Peace. In addition, the European Parliament plays an important role in ensuring that limited resources are used in the most efficient way and avoiding overlap between the institutional mandates and activities.

Main references

Drent, M., Hendriks, R., Zandee, D., New threats, new EU and NATO responses, Netherlands Institute of International Relations Clingendael, 2015.

Lasconjarias, G., Larsen, J.A. (eds.), NATO's response to hybrid threats, NATO Defence College, 2015.

Schmitt, M. N. (ed.), Tallinn Manual on the International Law applicable to cyber warfare, Cambridge University Press, 2013.

Schmitt, M. N. (ed.), Tallinn Manual 2.0 on the International Law applicable to cyber operations, Cambridge University Press, 2017.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)