OSW **Commentary**

CENTRE FOR EASTERN STUDIES **NUMBER 328** 24.04.2020 **www.osw.waw.pl**

Towards greater resilience: NATO and the EU on hybrid threats

Piotr Szymański

In recent years, NATO and the EU have taken greater responsibility for countering hybrid threats. This group of threats covers a wide range of hostile methods used by states and non-state actors. It includes both military and non-military activities, for instance special forces operations and irregular warfare, and also disinformation and cyberattacks. NATO and the EU are involved in facilitating international cooperation on countering hybrid threats and protecting their own structures and institutions against them. In this way, both organisations reinforce the efforts at the national level, since fighting hybrid threats is primarily a task of the member states. Nevertheless, NATO's and the EU's actions in this respect are constrained by insufficient financing, and by the member states' unwillingness to enhance the sharing of intelligence and sensitive information related to, for example, critical infrastructure protection or cybersecurity. The recent spike in anti-Western COVID-19 disinformation campaigns clearly shows that both NATO and the EU could do more to counter hybrid threats.

The role of NATO and the EU in tackling hybrid threats

NATO and the EU perceive hybrid threats in a similar way. According to NATO "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". They are aimed at "blurring the lines between war and peace, and sowing doubt in the minds of target populations".[1] The EU's definition seems to be more complex. From its perspective "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". The EU places emphasis on the multidimensional character of hybrid threats, which "range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions". They are targeted against "critical vulnerabilities" and exploit "coercive and subversive measures", being "difficult to detect or attribute" and designed "to create confusion to hinder swift and effective decision-making".[2]

[1] 'NATO's response to hybrid threats', NATO, 8 August 2019, www.nato.int.

[2] 'A Europe that Protects: Countering Hybrid Threats', EEAS, 13 June 2018, www.eeas.europa.eu.

OSW

Centre for Eastern Studies
ul. Koszykowa 6a, 00-564 Warsaw, Poland
tel.: (+48) 22 525 80 00, info@osw.waw.pl
www.osw.waw.pl

EDITORS: Mateusz Gniazdowski, Justyna Gotkowska
Tomasz Strzelczyk, Szymon Sztyk
TRANSLATION: Piotr Szymański
CO-OPERATION: Nicholas Furnival
DTP: Urszula Gumińska-Kurek

Therefore, hybrid threats should be considered an umbrella term, encompassing various destabilising actions. On the one hand, this blurry definition may water dawn the security debate. On the other, it may foster discussions as individual states are able bring their own priorities to the security agenda. Addressing hybrid threats takes into account not only kinetic operations, such as the use of troops without insignia, actions against critical infrastructure, orchestrating coups d'état or assassinations commissioned by foreign intelligence agencies, but also non-kinetic means – for instance a wide range of disinformation and propaganda measures, sponsoring radical political movements, exerting economic pressure, or covert actions aimed at destabilising other countries (including corrupting politicians).

" In countering hybrid threats, both organisations are focused on the protection of their own structures, decision-making processes and infrastructure.

The main responsibility for countering hybrid threats lies with NATO's and the EU's member states. Only governments have adequate resources for this, in the form of intelligence and counterintelligence agencies (both civilian and military), uniformed services (ensuring public order and safety), means of communication with citizens and cyber incident response capabilities. Moreover, the national authorities are closer to potential threats than international organisations. This, combined with a shorter decision-making process, makes them more capable of dealing with hostile hybrid operations. Safeguarding internal security belongs to each state's vital interests; individual governments thus pay more attention to enhancing resilience against hybrid threats than international organisations.

NATO and the EU have stepped into the fight against hybrid threats mainly in response to the elevated risk of terrorist attacks, related to the emergence of Islamic State, the rise of information warfare, increasingly common foreign interference in elections (primarily from Russia) and ever more harmful cyberattacks. In countering hybrid threats, both organisations are focused on the protection of their own structures, decision-making processes and infrastructure. With regard to the member states, NATO and the EU perform subsidiary and coordinating roles (for example in ensuring shared situational awareness), which means involvement in areas where action at the national level proved to be ineffective or insufficient. NATO and the EU aim for the development of international cooperation in countering hybrid threats (including NATO-EU cooperation), which has been hindered by the divergent threat perceptions of the member states. It translates into their engagement in facilitating the exchange of lessons learned and improving knowledge on hybrid threats, as well as in conducting international exercises which involve hybrid scenarios. In addition, both organisations set common standards and minimum requirements for their member states regarding resilience to hybrid threats (in order to eliminate national vulnerabilities affecting European and transatlantic security). It relates to, for instance: cybersecurity, preventing money laundering, and the protection of critical energy infrastructure.

Since Russia's military aggression against Ukraine in 2014, NATO has been more focused on strengthening collective defence and the capabilities essential for Article 5 operations. This adaptation of NATO's military posture has been complemented by calls for greater investment in beefing up allied resilience to hybrid threats. It was mainly due to hostile non-military actions by Russia, including: interference in the 2016 United States elections, the Salisbury nerve agent attack, and attempts to prevent Montenegro joining NATO. An important strategic message was delivered in the 2016 Warsaw Summit Communiqué, stating that "NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty".[3] In order to counter the military aspects of hybrid threats (such as

[3] Warsaw Summit Communiqué, NATO, 9 July 2016, www.nato.int.

irregular warfare), NATO has strengthened its intelligence capabilities and increased the readiness of the enhanced NATO Response Force (NRF), by establishing the Very High Readiness Joint Task Force (VJTF). In the non-military dimension, NATO gives priority to cybersecurity.

The EU has been increasingly concerned with hybrid threats. Since 2014, it has adopted more than 20 different documents in this field (on countering weapons of mass destruction, ensuring the security of energy supplies, screening foreign direct investments, maritime security, data protection, border protection, the security of space domain, and others).[4] In addition, the EU has been developing its Programme of Critical Infrastructure Protection embedded in the 2008 Directive on European Critical Infrastructures. However, in recent years, the EU has decided to put situational awareness, cybersecurity and disinformation at the heart of its efforts to counter hybrid threats. In 2019, the Council of the EU acknowledged "the possibility for the Member States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity".[5]

NATO's priorities: situational awareness, cyber defence, exercises

(1) NATO assistance for its member states in responding to hybrid activities encompasses monitoring and analysing, the exchange of intelligence and experiences, and ensuring shared situational awareness. Establishing a new branch for the analysis of hybrid threats (including cyber threats) within the structure of the Joint Intelligence and Security Division in the NATO Headquarters, along with enhancing cooperation between civilian and military intelligence, have been significant developments in this field. It was part of a broader reform of NATO's intelligence conducted in 2017. The hybrid branch was tasked with the comprehensive analysis of the challenges to transatlantic security, involving various military and non-military aspects of hybrid threats. It has, however, been only a first step towards enhancing shared situational awareness with regard to hybrid threats. NATO does not have its own intelligence service and thus relies on intelligence provided by the national agencies. Furthermore, the member states remain reluctant to share intelligence within NATO. This results from the deficits in mutual trust between them and concerns about the safety of classified data and information.[6] In practice, more advanced intelligence cooperation has been taking place on a bilateral basis or within smaller groups of the member states.

> **" NATO assistance for its member states in responding to hybrid activities encompasses the exchange of intelligence and experiences, and ensuring shared situational awareness.**

(2) In 2018, NATO set up counter-hybrid support teams, which consist of experts specialised in providing assistance to members struggling with hostile hybrid activity. This mechanism was activated for the first time in 2019 by Montenegro. It wants to take advantage of NATO's expertise in responding to Russia's hybrid threats in order to protect the 2020 parliamentary elections. These extraordinary measures were motivated by Russia's efforts to destabilise Montenegro, including the attempted coup d'état in 2016. The team's mission was focused on the necessary changes in legislation and cybersecurity. In this case, NATO's experts worked together with the US ones.[7] There is no open source information on the further deployments of counter-hybrid support teams. Perhaps other member states have not experienced large-scale hybrid activities, which would have required assistance from NATO experts. However, the unwillingness to reveal the vulnerabilities

[4] D. Fiott, R. Parkes, *Protecting Europe: the EU's response to hybrid threats*, European Union Institute for Security Studies, 2019.

[5] 'Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions', The Council of the European Union, 10 December 2019, data.consilium.europa.eu.

[6] J. Ballast, 'Trust (in) NATO – The future of intelligence sharing within the Alliance', NATO Defense College, Research Paper, No. 140, September 2017, www.ndc.nato.int.

[7] S. Lekic, 'First NATO counter-hybrid warfare team to deploy to Montenegro', Stars and Stripes, 8 November 2019, www.stripes.com.

of their defence systems or doubts about the prospects of receiving timely and well-tailored assistance may serve as an alternative explanation.

(3) Cybersecurity has never been more essential for NATO. This was proved by cyberspace being recognised as a domain of operations (equal to the air, land and sea military domains) at the 2016 Warsaw Summit as well as by affirming that a cyberattack could trigger Article 5 at the 2014 Newport Summit.[8] NATO plays a triple role in cyberspace. It motivates the allies to invest more in cybersecurity, serves as a platform for information sharing and training, and protects its own networks and supports the security of its member states' networks.

In 2016, NATO adopted the Cyber Defence Pledge aimed at strengthening capabilities vital for the cyber defences of national infrastructures and networks. It also mentioned the need of allocating adequate resources for cyber defence, however, without setting a NATO target level for cyber spending as a share of defence budget.[9]

In recent years, among the European NATO members, the largest investments in cyber defence were declared by the United Kingdom and France (1.9 billion pounds in 2016-2021 and 1.6 billion euros in 2019-2025 respectively). Some of the member states have also developed offensive cyber capabilities. Already nine of them made these capabilities available for NATO operations.[10] In terms of cyber exercises and expertise, NATO relies on the Tallinn-based Cooperative Cyber Defence Centre of Excellence (established in 2008). It organises the biggest allied cyber defence Locked Shields exercises, held on an annual basis. NATO's networks are, in turn, protected by the Computer Incident Response Capability (NCIRC), which has 200 personnel. The NCIRC is ready to reinforce the member states' networks by dispatching the NATO Cyber Rapid Reaction teams as well. These standby teams are intended to provide short-notice assistance to allies facing cyberattack.

> **NATO plays a triple role in cyberspace. It motivates the allies to invest more in cybersecurity, serves as a platform for information sharing and training, and protects its own networks.**

In 2018, NATO established the Cyberspace Operations Centre. Its core tasks include: ensuring a shared situational awareness on cyber threats, coordinating member states' activities in cyberspace, as well as protecting NATO's operations and mission. However, it is expected to reach full operational capability only in 2023. This lengthy process may result from the difficulties in hiring experts due to competition with the private sector. The cooperation in cyber defence is also hindered by the member states' attitude. Governments, which invested a lot in cybersecurity, are not eager to share technologies with countries which neglected this area.[11] In addition, cybersecurity experts point to the lack of NATO plans to develop joint offensive capabilities in cyberspace. These are provided by individual allies, which follow different strategies. The absence of a proper cyber command in NATO is considered to be another shortcoming. Such a command would enable NATO to develop a single doctrine, and to integrate and plan capabilities.[12] Finally, there is concern that NATO will inevitably lag behind the cyber aggressors due to the growing scale of hostile activities in cyberspace. Therefore, the cooperation with business has become increas-

[8] Warsaw Summit Communiqué, *op. cit.* "Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis". Wales Summit Declaration, NATO, 5 September 2014, www.nato.int.

[9] Cyber Defence Pledge, NATO, 8 July 2016, www.nato.int.

[10] Namely: the US, the UK, the Netherlands, Estonia, Norway, Germany, France, Denmark and Lithuania. S. Vavra, 'NATO cyber-operations center will be leaning on its members for offensive hacks', Cyberscoop, 30 September 2019, www.cyberscoop.com.

[11] M. Veenendaal, K. Kaska, P. Brangetto, 'Is NATO Ready to Cross the Rubicon on Cyber Defence?', CCDCOE, Tallinn 2016, ccdcoe.org.

[12] S. Arts, 'Offense as the New Defense: New Life for NATO's Cyber Policy', GMF, 13 December 2018, www.gmfus.org.

ingly important. NATO works with the private sector through its Malware Information Sharing Platform (sharing information on malware and their indicators with trusted partners) and through the Industry Cyber Partnership (led by the NATO Communications and Information Agency).

(4) NATO exercises are of key importance for enhancing allied resilience against hybrid threats. NATO has employed here a two-track approach. On the one hand, since 2016, NATO has incorporated hybrid scenarios into its annual Crisis Management Exercise (CMX), which rehearses internal political and military decision-making mechanisms. On the other, it has tested allied military capabilities and readiness to respond to hybrid activities in various live exercises (NRF and VJTF exercises like Trident Juncture or Brilliant/Noble Jump). During these exercises, NATO forces have been mastering, for instance, critical infrastructure protection and combating irregular troops (including urban warfare).

The EU's priorities: situational awareness, cybersecurity and disinformation

(1) The EU strives for an improvement of European capabilities to analyse and share information on hybrid threats for the needs of its institutional framework and the member states. In 2016, it established a Hybrid Fusion Cell as part of the EU Intelligence and Situation Centre. The cell deals with threat analyses and collecting data on hybrid activities on the EU's territory and in its neighbourhood. In the following year, in 2017, the EU's anti-hybrid toolbox was expanded to include the Helsinki-based European Centre of Excellence for Countering Hybrid Threats, which is open to both EU and NATO members. The goal of this international research and training platform is to develop a better understanding of hybrid threats and the best practices in fighting them. It is legitimate to assume that intelligence sharing within the EU faces similar limitations as in NATO.

(2) The commitment to secure cyberspace plays a central role in the EU's approach towards hybrid threats. Both protecting critical infrastructure and the functioning of the single market are increasingly dependent on the resilience of national networks. Existing vulnerabilities were revealed by two large-scale cyberattacks in 2017: WannaCry and NotPetya.[13] The first one disrupted activities of the UK's National Health Service, Germany's Deutsche Bahn, France's Renault and Spain's Telefónica, among others. The latter targeted mainly Ukraine, however Denmark's A.P. Møller-Mærsk also suffered significant financial losses (estimated at the level of US$ 300 million).

" The commitment to secure cyberspace plays a central role in the EU's approach towards hybrid threats. Existing vulnerabilities were revealed by two large-scale cyberattacks in 2017.

The adoption of the first EU-wide legislation on cybersecurity, the 2016 Directive on Security of Network and Information Systems (NIS Directive), was a major breakthrough in enhancing resilience against hybrid threats. Consequently, Brussels started to develop the horizontal regulatory framework for cybersecurity and obliged the member states to ensure a common minimum level of the security of national networks. On the basis of the NIS Directive, countries were required to adopt their own cybersecurity strategies, establish Computer Security Incident Response Teams (CSIRT) and a European CSIRT Network (in order to strengthen information sharing and a coordinated response to cyber threats). Moreover, operators of essential services (energy, transport, water, banking, financial market and digital infrastructures, healthcare) as well as providers of key digital services (search engines, cloud computing and online marketplaces) were required to notify serious incidents to the relevant national authority.[14]

[13] D. Fiott, R. Parkes, *op. cit.*

[14] M. Grzybowski, '9 faktów o Dyrektywie NIS, które powinieneś znać', Fundacja Bezpieczna Cyberprzestrzeń, 15 November 2016, www.cybsecurity.org. NIS Directive was supplemented by the 2019 EU Cybersecurity Act, which introduced an EU-wide cybersecurity certification framework for digital products, services and processes.

These legislative actions have been bolstered through complementary measures aimed at strengthening "deterrence" in cyberspace and cyber defence capabilities. In 2019, the Council of the European Union allowed sanctions on non-EU actors (persons or entities) to be imposed where they are responsible for cyberattacks (carried out from outside the EU). A new sanctions regime includes a travel ban to the EU and an asset freeze.[15] In the future, it could become an important tool for the EU in its fight against malicious behaviour in cyberspace, especially against state-sponsored hacking groups. Besides, since 2017, thanks to Permanent Structured Cooperation (PESCO) on security and defence (part of the EU's Common Security and Defence Policy), several European military cooperation projects on cyber defence have been launched. They are directed at streamlining information sharing and coordination, developing rapid response capabilities in cyberspace, and enhancing cyber education and innovations.

> **In combating disinformation, the EU focuses on monitoring and revealing hostile campaigns, as well as on cooperation with online platforms.**

In the field of cybersecurity, aside from protecting its own networks, the EU provides support for the development of research programmes and of public-private partnership. The EU Agency for Cybersecurity (ENISA) and the European Cyber Security Organisation (established in 2016) are particularly active here. The first one is tasked with drawing recommendations and delivering expertise on cybersecurity issues, while the latter focuses on deepening trilateral cooperation between businesses, the European Commission and the member states.

Despite these efforts, the EU's cooperation on cybersecurity has so far been developed below the level of the European Commission's ambitions. This is because the member states consider data on cyberattacks as sensitive information. In addition, compared to investments at the national level, the EU's engagement in cyberspace lacks proper funding. ENISA's endless struggle for extra financing and personnel may serve as an example here. The cooperation has also been inhibited by different goals pursued by individual countries with respect to cybersecurity. It is visible, for instance, in the incoherent approaches to use of Chinese technologies in developing 5G.

(3) The EU defines disinformation as "verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public".[16] For the European intuitions, the issue of disinformation has been in the spotlight due to the urgent need to protect democratic elections from external meddling and manipulations. The spread of terrorist propaganda has been another important factor. In combating disinformation, the EU focuses on monitoring and revealing hostile campaigns, as well as on cooperation with online platforms.[17]

In recent years, the EU has created a toolbox for tracking and detecting disinformation. It started in 2015 with the establishment of the European External Action Service's East StratCom Task Force, responsible for analysing disinformation trends and exposing disinformation narratives originating from Russia. There are two other StratComs: profiled on the Southern Neighbourhood and the Western Balkans. In connection with the 2019 European Parliament election, the European network of fact-checkers and the Rapid Alert System against online disinformation have also been created. The latter is a secure network for sharing information about disinformation, designed for the EU institutions and the member states. It was supposed to facilitate the coordination of responses to disinformation campaigns, but it has never been activated.[18] Despite being one

[15] 'Cyber-attacks: Council is now able to impose sanctions', The Council of the European Union, 17 May 2019, www.consilium.europa.eu.

[16] 'Tackling online disinformation', European Commission, www.ec.europa.eu.

[17] The EU has adopted a whole raft of "soft laws" concerning the fight against disinformation.

[18] S. Stolton, 'EU mulls disinformation regulation but admits alert system has 'never been triggered'', Euractiv, 29 October 2019, www.euractiv.com.

of the main planks of EU's fight against hybrid threats, the European anti-disinformation system has faced several problems. Firstly, it does not cover the dissemination of disinformation by EU-based actors, which significantly limits the effectiveness of the anti-disinformation measures. Secondly, newly-established institutions struggle with underfunding and personnel deficits. This is well illustrated by repeated calls for strengthening the East StratCom, staffed with sixteen full-time specialists, made by experts and members of the European Parliament. The most recent ones were related to disinformation campaigns around the COVID-19 pandemic.[19]

The EU's defensive and reactive approach to disinformation, based on monitoring and exposing, presents another challenge. This strategy lacks efforts to create a European narrative which would undermine the credibility of actors spreading disinformation. It could include, for instance, coordinated public statements by members of the European Parliament or regular media campaigns with a broad outreach.

However, the future ups and downs in countering disinformation will be determined mainly by the development of public-private partnership, especially by cooperation with the biggest online platforms – the signatories of the Code of Practice against disinformation (2019). These are: Google, Facebook, Twitter and Mozilla, which agreed to self-regulatory standards in this area (on a voluntary basis). Being concerned with the rise of online disinformation, the EU strives for transparency in political advertising, advertising policy and algorithms, and for effective solutions in detecting and marking bots, and in closing fake accounts. Previous experiences show that the online platforms have not fully complied with the Code of Practice. In future this may lead to the introduction of regulatory measures by the European Commission.

[19] G. Gotev, 'Experts lament underfunding of EU task force countering Russian disinformation', Euractiv, 23 November 2018, www.euractiv.com; parliamentary question by Anna Fotyga on strengthening the East Stratcom Task Force, extending its work and turning it into a fully-fledged permanent structure within the EEAS, European Parliament, 6 April 2020, www.europarl.europa.eu.