PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

STRATEGIC FILE

NO. 9 (117), AUGUST 2022 © PISM

Editors: Sławomir Dębski, Patrycja Sasnal, Wojciech Lorenz

Tracing the Development of EU Capabilities to Counter Hybrid Threats

Filip Bryjka

Countering hybrid threats is one of the main dimensions of the EU Strategic Compass, guiding the development of the Union's capabilities in the field of international security. The document calls for combining the tools developed since 2016 to combat hybrid methods into an "EU Hybrid Toolbox", which will also include new instruments and modes of action. While the primary responsibility for countering hostile hybrid activity will continue to lie with the Member States, the EU will have greater capacity to support and coordinate prevention and response. The EU approach focuses on non-military aspects and developing military capabilities to respond to hybrid crises, which increases the importance of cooperation with NATO in this area.

Since 2016, the EU has been mobilising its resources and creating new instruments to combat hybrid threats. These actions are primarily the Union's response to the destabilising activities of Russia and China, as well as those of smaller states such as Belarus, Iran, or North Korea. The EU also includes the activities of terrorist organisations and extremist groups in the catalogue of such threats. The Union's efforts to date have focused on combating disinformation and propaganda and on strengthening the protection of critical infrastructure against cyberattacks. In the Strategic Compass, which was adopted by the EU Council on 21 March this year, less than a month after the Russian invasion of Ukraine, the focus is on increasing the resilience of states and societies to foreign information manipulation and interference in political processes, as well as broadening the EU's ability to support the Member States in responding to crises caused by hybrid methods. This is precisely the purpose of the EU Hybrid Toolbox, the exact shape of which will be worked out by the EU in the coming months.

Since 2016, the EU has been mobilising its resources and creating new instruments to combat hybrid threats.

An EU Approach to Combating Hybrid Threats

In 2016, the EU, in the document "Joint Framework on countering hybrid threats", defined the threats as a "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".[1] They can be used to pursue a variety of strategic, operational, and tactical objectives with the common denominator of destabilising states and interfering in their political, social, and economic processes, both Member States as well as the Community as a whole. The Union's broad approach to this issue stems from the specificity of the phenomenon itself, particularly hybrid actions' complexity, multifaceted nature, and ambiguity. The response also reflects the different security perspectives and foreign policy priorities of individual Member States. This flexible approach makes it possible to take into account both threats from the east (Russia, Belarus), the south (Iran, terrorist organisations, irregular mass migration), and those with a global reach (China).

Hybrid threats are defined by EU as a "mixture of coercive and subversive activity, conventional and unconventional methods […]".

Since 2015, the EU has experienced hostile hybrid activity primarily from Russia.

The catalogue of hybrid methods and tactics includes disinformation and propaganda activities, cyberattacks, interference in political processes (e.g., elections and referendums), economic pressure, instrumentalisation of irregular migration, state support of armed groups and employment of mercenaries, intelligence operations of a subversive and sabotage nature, terrorist activities, or the use of chemical, biological, radiological, and nuclear (CBRN) agents. Since 2015, the EU has experienced hostile hybrid activity primarily from Russia. To a lesser extent—but with a clear upward trend—such methods are also used by China, Belarus, Iran, and North Korea, as well as by terrorist organisations and radical groups.

Hybrid methods can be used to varying extents and varying intensities and can be freely combined by state or non-state aggressors whose *modus operandi* is not the same. Moreover, the catalogue of hybrid warfare tools is "open" in nature. In the view of the EU institutions, the increasing political rivalries with Russia (especially after the invasion of

The catalogue of hybrid warfare tools is "open" in nature.

[1] "Joint Framework on countering hybrid threats a European Union response," European Commission, 6 April 2016, https://eur-lex.europa.eu.

Ukraine) and China, the unstable situation in the EU's neighbourhood, and the weaponisation (militarisation) of further sectors (e.g., security issues related to health and the environment). This is exemplified by the Russian and Chinese disinformation campaigns on vaccination during the COVID-19 pandemic. Similarly, issues such as those related to environmental protection can be used to create social polarisation and divisions within the EU. Climate change, in turn, can contribute to the destabilisation of the Union's southern neighbourhood, migration crises, and the rise of terrorist organisations. The instrumentalisation of these phenomena by external actors (e.g., creating routes for the smuggling of irregular migrants or inspiring radicals to carry out terrorist attacks) poses a direct threat to EU states. The catalogue of hybrid threats is also broadened by emerging and disruptive technologies (EDTs), including the development of artificial intelligence, providing advanced technical capabilities for disinformation and propaganda campaigns, as well as intelligence and subversion activities. These considerations make it much more difficult to develop procedures for responding to various hybrid attack scenarios, which, due to the cross-border and networked nature of hybrid threats, require a comprehensive and multidimensional approach to their early detection, counteraction, and emergency response.

Since 2016, the EU is developing the capacity to counter hybrid threats in four areas: (1) situational awareness; (2) building resilience; (3) countering and responding to crises (including overcoming their effects); and, (4) cooperation and coordination with partners and international organisations (mainly NATO). The Compass calls for strengthening these areas by creating new mechanisms and improving their use as part of the Union's coordinated response to hybrid crises. Indeed, the burden of responsibility for countering hybrid threats lies with national security institutions (i.e., intelligence, security services, police, and military), which have the legal authority and executive powers to do so (as per Article 4(2) TEU). The Strategic Compass makes no changes in this area. Instead, the instruments being developed under the EU Hybrid Toolbox are intended to provide greater support to national efforts to combat hybrid threats and to coordinate joint action by Member States to achieve synergies and a more effective response.

The burden of responsibility for countering hybrid threats lies with national security institutions.

Situational Awareness

The Strategic Compass highlights the importance of further strengthening EU intelligence capacity to provide situational awareness and threat forecasting capabilities. Creating information-sharing mechanisms on hybrid threats is of particular importance here, not least because the use of such tactics is primarily the *modus operandi* of foreign intelligence services. Improving the awareness of EU institutions and Member States in this area will enhance the EU's ability to rapidly detect and respond to crises caused by hybrid methods. It will also improve the coordination of actions taken by individual states. Activities in this area were initiated in 2016 with the creation of the Hybrid Fusion Cell at the EU Intelligence and Situation Centre (EU INTCENT).[2] It is staffed by civilian and military analysts (from the Intelligence Directorate at the EU Military Staff, EUMS) responsible for producing reports, briefings, and analysis under the Single Intelligence Analysis Capacity (SIAC) on hybrid threats occurring in EU countries and its neighbourhood. Access to the material is available to EU institutions—the European Council, the European Commission (EC), the European External Action Service (EEAS), the Horizontal Working Group on Strengthening Resilience and Countering Hybrid Threats (ERCHT)—and individual Member States (through contact points; in the case of Poland, it is the liaison officer of the Internal

Improving the awareness of EU institutions and Member States will enhance the EU's ability to rapidly detect and respond to crises caused by hybrid methods.

[2] The Cell reached full operational capacity in mid-2017.

Security Agency, or ABW, at the Permanent Representation of the Republic of Poland to the EU). The studies are produced on the basis of information from both open and classified sources provided by the intelligence and security services of the Member States, EU agencies (e.g., the European Cybercrime Centre, the European Counter Terrorism Centre, or Frontex), and partner countries (e.g.,the U.S., Canada, Norway). In terms of cyberthreat intelligence, the work of the Hybrid Fusion Cell is supported by representatives of the Computer Emergency Response Team for the EU Institutions (CERT-EU). The exchange of sensitive information concerning, for example, the technical details of accounts, administrators, software, or infrastructure used to carry out a disinformation operation, is crucial to being able to attribute responsibility for these actions to a specific entity and to impose sanctions on it.[3]

The Hybrid Fusion Cell is the lead institution responsible for providing situational awareness to EU institutions and Member States.

The Hybrid Fusion Cell is the lead institution responsible for providing situational awareness to EU institutions and Member States. Its creation has contributed to enhancing the EU's ability to detect hybrid-induced crises at an early stage, as well as to accelerate and coordinate the joint response of Member States. An example of this is the EU's response (including in the form of effective strategic communication) to the Belarus state-sponsored migration crisis triggered in mid-2021 (with the assistance of Russia), which lasting several months on the borders with Poland, Lithuania, and Latvia.[4] Despite Belarusian-Russian disinformation activities aimed at creating divisions over the interpretation of the situation on the border,[5] the Union remained consistent and considered it a hybrid attack.[6]

To increase the situational awareness of hostile information manipulation, in March 2019 the Union established the Rapid Alert System on Disinformation.

To increase the situational awareness of hostile information manipulation, in March 2019 the Union established the Rapid Alert System on Disinformation. The exchange of information under this system takes place through contact points established in individual Union countries. In Poland, it is a special desk for strategic communication at the Ministry of Foreign Affairs, which deals primarily with disinformation in relation to Poland's foreign policy priorities. The system was used in 2020 during the COVID-19 pandemic when the information space was flooded by a wave of Russian and Chinese disinformation undermining confidence in Western vaccines (mainly mRNA-type), EU institutions, and vaccination strategies, and fuelling anti-vaccination movements.[7] Targets of the attacks at the time included the European Medicines Agency. The system was used to exchange information between EU institutions and the Member States, private sector representatives, and G7 and NATO members. However, these actions did not stop the wave of conspiracy theories spread by, among others, anti-vaccine circles or pro-Russia and pro-China news channels (including "troll factories").

Building Resilience

Building resilience of EU states and their societies is aimed at reducing their vulnerability to hostile disinformation and propaganda and to strengthening the protection of critical infrastructure against

[3] E. Kaca, "EU Sanctions for Disinformation Campaigns: Prospects and Limits," *PISM Bulletin,* No. 104, 26 May 2021, www.pism.pl.

[4] A.M. Dyner, "The Border Crisis as an Example of Hybrid Warfare," *PISM Strategic File*, No. 2, February 2022, www.pism.pl.

[5] F. Bryjka, A. Legucka, "Russian and Belarusian Disinformation and Propaganda in the Context of the Polish-Belarusian Border Crisis," *PISM Bulletin*, No. 212, 09 December 2021, www.pism.pl.

[6] "European Council conclusions of 21 and 22 October 2021," European Council, https://www.consilium.europa.eu/media/52622/20211022-euco-conclusions-en.pdf.

[7] A. Legucka, M. Przychodniak, "Disinformation from China and Russia during the COVID-19 Pandemic," *PISM Bulletin*, No, 86, 21 April 2020, www.pism.pl.

cyberattacks, terrorism, subversion, and sabotage. The Strategic Compass devotes particular attention to strengthening the EU's resilience against foreign information manipulation and interference in political processes.

The Strategic Compass devotes particular attention to strengthening the EU's resilience against foreign information manipulation and interference in political processes.

The EU approach to combating information manipulation consists of four elements adopted by the EC in December 2018 in "The Action Plan against Disinformation": (1) enhancing the capacity of EU institutions to detect, analyse, and expose disinformation; (2) strengthening coordinated and collective responses to disinformation; (3) mobilising the private sector to combat disinformation; and, (4) raising awareness and improving public resilience by supporting independent journalism, fact-checking initiatives, and promoting media education.

In 2015, in response to Russian information and psychological operations, the East StratCom task force was established within the EEAS to monitor, analyse, and respond to Russian propaganda and disinformation campaigns. Initially comprising just three people, the team now has 16 full-time staff. East StratCom monitors information messages published in more than 20 languages. By mid-May this year, the team had identified nearly 14,000 cases of Russian disinformation and catalogued them in the EUvsDisinfo database. In addition, the team conducts training for partner country staff, undertakes activities to strengthen independent journalism, and promotes awareness of the EU and its policies in the Eastern Partnership countries. Similar tasks are carried out by analogous teams (with six full-time staff members each) established in 2017, responsible for the Western Balkans region (Western Balkans Task Force), and the Middle East and North Africa region (South Stratcom Task Force), focusing on countering radicalisation, combating propaganda from terrorist organisations, and disinformation from Russia, China, Iran, or Turkey. All three teams are part of the Strategic Communications, Task Forces and Information Analysis Division of the EEAS (SG.STRAT.2), which supports EU institutions in planning policies, strategies, and strategic communication tools. It also provides support (e.g., in the form of analysis and instructions on how to combat disinformation) to EU diplomatic missions, operations, and missions within the Common Security and Defence Policy (CSDP). The unit also develops cooperation with partner countries, the G7, NGOs, civil society, and the private sector (e.g., on data acquisition using modern software and technology). The aim of these activities is to build public awareness and strengthen countries' resilience to disinformation in the EU neighbourhood.

In 2015, in response to Russian information and psychological operations, the East StratCom task force was established within the EEAS.

According to the EEAS, Russian disinformation poses the greatest threat to EU states because of its systemic nature. Russia has the resources to conduct disinformation campaigns as part of a long-term strategy to destabilise and disintegrate the Euro-Atlantic area. At the same time, the scale of Russian disinformation is incomparably greater in relation to other states emulating Russia in this area (e.g., China). One of the most sensitive and vulnerable areas of disinformation in the functioning of EU states is democratic political processes, such as elections and referendums. Between November 2016 and April 2019, Russian interference in political processes affected 16 out of 20 such cases worldwide (including in the UK, France, Germany, and Spain).[8] These primarily took the form of disinformation campaigns and

According to the EEAS, Russian disinformation poses the greatest threat to EU states because of its systemic nature.

[8] "Hacking democracies Cataloguing cyber-enabled attacks on elections," Australian Strategic Policy Institute, https://www.aspi.org.au.

cyberattacks, including hacking of websites and altering their content, attacks on electoral infrastructure, or stealing and publishing information (hack and leak) to manipulate public opinion.

To protect EU Member State voters from disinformation and cyber interference, the EU's CERT-EU set up a dedicated Social Media Assurance service to detect and remove accounts impersonating a real user. In September 2018, the Union also adopted the "Code of Practice" governing EU countries' cooperation with the private sector on obligations for online platforms and the advertising industry to improve transparency of political advertising, close fake accounts, and reduce incentives to spread disinformation. The Code has been adopted by, among others, major online service platforms such as Facebook, Google, Twitter, and Microsoft. They pledged to increase the transparency of political advertising and its funding and to block those responsible for disinformation. These measures were aimed at protecting the European Parliament elections in May 2019.

The Strategic Compass announced the creation of a new mechanism to increase situational awareness and the resilience of the EU against information manipulation and interference in political processes.

The Strategic Compass announced the creation (by 2023) of a new mechanism to increase situational awareness and the resilience of the EU, the Member States, and their societies, against information manipulation and interference in political processes (Foreign Information Manipulation and Interference Toolbox, FIMI). The new collaborative platform aims to standardise methods of data collection, analysis, and exchange (between Member State governments, the private sector, and civil society and international organisations) on the tactics, techniques, and procedures used by hybrid actors. This will enhance the EU's ability to identify and analyse disinformation campaigns early, facilitate the collection of evidence of external interference in democratic political processes, and standardise methods for reporting such incidents. An Information Analysis and Sharing Centre (ISAC) will most likely be established as part of the FIMI Toolbox.[9]

A breakthrough in the EU's approach to cybersecurity was the adoption of the "Directive on the Security of Network and Information Systems" (NIS Directive) in 2016.

Building the resilience of EU countries also concerns key sectors such as cybersecurity, critical infrastructure, energy, transport, defence, the financial system, maritime security, and space.[10] This effort is primarily oriented towards building the necessary legal instruments and capacities to respond to incidents and crises caused by hybrid methods (especially in cyberspace). A breakthrough in the EU's approach to cybersecurity was the adoption of the "Directive on the Security of Network and Information Systems" (NIS Directive) in 2016. It obliges the Member States to guarantee minimum common standards for cybersecurity, including through the adoption of national cybersecurity strategies or the creation of computer-incident response teams operating within the European CERT network. The EU has also made cyber-incident reporting mandatory for key service providers in the energy, transport, banking and finance, healthcare, water supply, and digital infrastructure sectors. In addition to regulatory activities, the EU, through the European Network and Information Security Agency (ENISA) and the European Cyber Security Organisation (ECSO), also supports research activities and public-private cooperation. The joint cyberdefence capabilities of the Member States are in turn developed through four PESCO Structured Cooperation Projects on information-sharing

[9] "2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division," 24 March 2022, https://www.eeas.europa.eu.

[10] A. Kozioł, "Strategic Compass: Towards EU Space Strategy for Security and Defence," *PISM Policy Paper*, No. 1, 2022, www.pism.pl.

on cyber incidents, coordination of activities, support, and joint response, as well as research and training.[11]

In December 2020, the Union adopted a new cybersecurity strategy that aims to increase Member States' resilience to cyberattacks and better protect their critical infrastructure.

In December 2020, the Union adopted a new cybersecurity strategy[12] that aims to increase Member States' resilience to cyberattacks and better protect their critical infrastructure. An example of sectoral action in this area is the EU Cyber Diplomacy toolbox, which has measures that act as a deterrent to potential cyber-attackers. In May 2019, the model created a sanctions regime to respond to cyberattacks perpetrated against the Member States from outside the EU or using infrastructure located outside the Community. Blacklisted entities responsible for or supporting cyberattacks against EU states will be sanctioned by being banned from entering the EU and/or by having their assets frozen. A similar sanctions regime has been introduced against countries using chemical weapons (the classified list contains 20 substances), which is the EU's direct response to the use of the paralytic-convulsive Novichok agent on UK territory by Russian special services. Between 2019 and 2022, the EU also provided financial support, to the tune of €11.6 million, to the Organisation for the Prohibition of Chemical Weapons (OPCW) to counter the development and use of chemical weapons.

Preventing and Responding to Crises

The EU announced the creation of Rapid Hybrid Response Teams (EURHRTs) by the end of 2024 to support Member States in situations with hybrid attacks.

The EU Strategic Compass highlights the importance of strengthening the Union's capacity to respond to hybrid crisis. The EU announced the creation of Rapid Hybrid Response Teams (EURHRTs) by the end of 2024 to support Member States in situations with hybrid attacks. These teams are also likely to be able to be used for EU missions and operations, as well as to provide assistance to partner countries. Although work on the establishment of EURHRTs is in the conceptual phase, they most likely will be formed along the lines of the NATO Counter-Hybrid Support Teams (CHSTs) established in 2018.[13] The teams are mainly composed of civilian experts in strategic communications, cybersecurity, counterintelligence, energy security, and critical infrastructure protection. They also can be augmented with military advisors if necessary. In a crisis, they can be deployed to a Member State (at its request), or act as an advisory team to set up national defence structures to counter hybrid threats.

Importance of Cooperation with NATO

The Strategic Compass emphasises the importance of cooperation in combating hybrid threats with partners, including the G7, the UN, and NATO. The Union attributes a key role in this regard to its relations with the Alliance. In 2015, NATO adopted the "counter-hybrid strategy", which has three

[11] P. Szymański, "Towards greater resilience: NATO and the EU on hybrid threats," *OSW Commentary*, No. 328, 2020, www.osw.waw.pl

[12] "The EU's Cybersecurity Strategy for the Digital Decade," European Commission, 16 December 2020, https://digital-strategy.ec.europa.eu.

[13] CHSTs are NATO's instrument for responding to hybrid threats below the North Atlantic Treaty's Article 5 threshold of collective defence. So far, CHSTs have been used twice: first in 2019 in Montenegro in relation to cyberattacks and disinformation during the election period, and in 2021 in Lithuania in relation to the Belarus state-sponsored migration crisis on the border.

components: (1) be prepared for hybrid attacks by enhancing reconnaissance and early warning capabilities, strengthen critical infrastructure protection or test decision-making processes within the Alliance; (2) deter a potential aggressor by imposing sanctions, and keeping uncertainty about the nature of the response, and (3) defend allies in the event of hybrid aggression (especially attempts using military means).[14]

In joint declarations from 2016 and 2018, the EU and NATO developed a list of 74 joint actions in the security dimension, more than 20 of which can be related to countering hybrid threats.

In joint declarations from 2016 and 2018, the EU and NATO developed a list of 74 joint actions in the security dimension, more than 20 of which can be related to countering hybrid threats. The focus is primarily on recognising the phenomenon, raising situational awareness, building societal resilience, protecting critical infrastructure, and responding to hybrid emergencies. Both organisations work to implement joint initiatives based on systemic—informal—staff-to-staff cooperation mechanisms at three interrelated levels: 1) expert, 2) intermediate (within the EU-NATO Core Group), and 3) strategic (EU-NATO Steering Group). Through informal cooperation, the organisations developed a common operational protocol (playbook) for sharing knowledge on hybrid operations and coordinating the responses of both institutions. The common framework set the unequivocal ambition to make combating hybrid threats an EU priority.

The first joint EU-NATO initiative on countering hybrid threats was the establishment of the European Centre of Excellence (Hybrid CoE) in Helsinki (2016).

The first joint EU-NATO initiative on countering hybrid threats was the establishment of the European Centre of Excellence (Hybrid CoE) in Helsinki (2016). It acts as a think-tank, expert and advisory support, and a platform for sharing experience and information on hybrid threats. The Helsinki centre primarily contributes to the situational awareness of both organisations, as does the EU Hybrid Fusion Cell, or its counterpart the NATO Hybrid Analysis Branch operating in the Joint Intelligence and Security Division (JISD). Both structures have well-established working relationships through monthly staff exchanges. The EU and NATO Hybrid Threat Analysis Cells also prepare joint threat assessments (Parallel and Coordinated Assessments). Similar cooperation is also being developed between the East StratCom Task Force and the NATO Centre of Excellence for Strategic Communications (StratCom CoE) in Riga, developing joint training materials, disinformation response courses, and other tools for EU and NATO staff.

On a practical level, the Helsinki centre is responsible for organising workshops, seminars, and exercises, which include simulations of North Atlantic Council (NAC) and Political and Security Committee (PSC) meetings during hybrid attacks. Since 2017, the EU and NATO have been conducting the EU *Integrated Resolve* exercise and the NATO *Crisis Management Exercise* (CMX) in the Parallel and Coordinated Exercises (PACE) format to test the ability to respond to crises (including hybrid events) through a common operational protocol. Each year, the exercise changes the lead organisation: in 2022, it will be the EU, and in 2023, NATO. The organisations also seek opportunities for joint (complementary) responses to threats in cyberspace, facilitated by joint training and exercises (e.g., *Cyber Phalanx*, *Locked Shields*, or the NATO Cyber Coalition), exchange of information and doctrinal documents, regular working contacts, educational projects, and others. This cooperation takes place through the European Defence Agency (EDA) and the NATO Centre of Excellence for Cyber Defence in Tallinn, among others. An important element of it is cooperation in the technological dimension, including the exchange of experience

The Helsinki centre is responsible for organising workshops, seminars, and exercises, which include simulations of North Atlantic Council (NAC) and Political and Security Committee (PSC) meetings during hybrid attacks.

[14] "NATO's response to hybrid threats," NATO, 16 March 2021, www.nato.int.

and practices between CERT-EU and the NATO Computer Incident Response Capability (NCIRC) at the Supreme Command of Allied Powers in Europe (SHAPE).

Weaknesses in the EU Approach to Countering Hybrid Threats

The decision to integrate the Union's counter-hybrid tools into the EU Hybrid Toolbox is a step in the right direction, especially given the anticipated increase in hybrid activity from Russia, China, and other actors. However, the EU Hybrid Toolbox does not solve all the Union's problems and weaknesses in this area. First of all, the Strategic Compass does not explicitly indicate the possibility of invoking the solidarity clause (Article 222 of the Treaty on the Functioning of the European Union, TFEU) or the mutual defence clause (Article 42(7) of the Treaty on European Union, TEU) in the event of a hybrid attack against a Member State. Since an aggressor in a crisis will seek to break down the cohesion of the EU and NATO and paralyse their decision-making processes, more discussion, simulations, and exercises on the use of both clauses are needed to reduce the risk of such a scenario.

The Strategic Compass does not explicitly indicate the possibility of invoking the solidarity clause or the mutual defence clause in the event of a hybrid attack against a Member State.

Currently, EU states can invoke the solidarity clause, obliging other members of the community to provide assistance in the event of a terrorist attack or natural or man-made disaster. They can do so by requesting support directly from the presidency of the Council and the president of the European Commission through the Emergency Response Coordination Centre (ERCC), but only after they have exhausted national and EU response capacities and they are found to be insufficient to deal with the crisis. It is then up to the individual Member States to decide the nature of the assistance and the extent of the support they will provide. This assistance should be based on the principles of coherence and complementarity and on the EU Integrated Political Crisis Response (ICPR) system. It is coordinated by the Council in cooperation with and taking into account the competences of the EC, the EEAS, and the High Representative (HR). Existing sectoral response instruments (political, financial, and operational) adopted, for example, for counterterrorism, protection of critical infrastructure, or cyberspace, can be applied in response to cyberattacks or externally inspired sabotage and subversive activities, among others.

Due to the ambiguity of hybrid threats (e.g., difficulties in identifying the actor responsible for an attack), the assessment of the legitimacy of invoking the solidarity clause has been entrusted to the High Representative and the EC (in line with their respective competences), which prolongs the response time and gives an aggressor space to interfere in the decision-making process (e.g., through disinformation activities). Indicating explicitly that Member States can invoke the solidarity clause in the event of hybrid threats would have important political consequences and a deterrent function. It would also make it more difficult for an adversary to manipulate individual EU states' assessment of the situation.

To trigger the mutual defence clause (Article 42(7) TEU), obliging members to provide support to an EU state that is the victim of armed aggression, the hybrid actions would (most likely) have to be carried out using military means, or a series of them (e.g., cyberattacks on critical infrastructure) that have far-reaching consequences and give grounds for considering these actions together as

Hybrid actions by their nature are activities conducted below the threshold of war, which creates the risk of a non-universal interpretation, and consequent dilatory action or inaction.

armed aggression.[15] Hybrid actions by their nature are activities conducted below the threshold of war, which creates the risk of a non-universal interpretation, and consequent dilatory action or inaction. It is therefore unclear how the EU would react to, for example, a series of subversive and sabotage operations (e.g., against the arms sector providing weapons or systems to Ukraine) and whether such an event would be considered as armed aggression. However, it is worth noting that Article 42(7) TEU, for the first and only time in EU history, was invoked by France after the 2015 terrorist attacks. EU states unanimously backed France despite the fact that this was in response to an internal threat and not an externally derived armed aggression. The decision to invoke the mutual defence clause, rather than the solidarity clause, was primarily symbolic and political. It remains an open question whether the Union would have reacted similarly to a hybrid attack directed, for example, against a state of lesser potential and importance in the EU, and exactly what action would have been taken.[16]

The lines of work in the EU indicate that hybrid attacks of a non-kinetic nature (e.g., in cyberspace) may be grounds for triggering the mutual assistance clause. This is evidenced by, for example, the cyberattack response exercises conducted in the spirit of Article 42(7) TEU. The principles of cooperation between the Member States and individual EU institutions in this regard were formulated in the recommendation on the coordinated response to large-scale cyber incidents and crises. Among other things, it emphasises the crucial importance of situational awareness for effective coordination at the technical (strengthening the security of networks and information systems), operational (information-sharing), and strategic (political) levels.

Equally importantly, the Compass does not develop politico-military mechanisms for responding to a full-scale armed conflict preceded by hostile hybrid action, thus leaving the lead role to NATO to ensure collective defence capability. In a situation of external aggression using military hybrid methods, Article 42(7) TEU and Article 5 of the North Atlantic Treaty could be triggered simultaneously.

The Strategic Compass announced the creation of Rapid Deployment Capability (RDC).

As the anticipated NATO membership of Finland and Sweden will reduce the number of EU countries outside NATO structures to four (Austria, Cyprus, Ireland, Malta), there is likely to be a weakening of initiatives to develop EU collective defence capabilities in favour of the development of crisis-management tools. This should strengthen the "European pillar" of the Alliance and the complementarity of the two organisations in the security and defence dimension. The Strategic Compass announced the creation of Rapid Deployment Capability (RDC) of 5,000 troops by 2025, consisting of components dedicated to a specific EU mission or operation. Indeed, they will be primarily intended for tasks under Article 43 TEU, that is, disarmament operations, humanitarian and rescue missions, military advice and support, conflict prevention, peacekeeping or peace-making, and post-conflict stabilisation operations. RDCs should also be used to support partner states at risk of conflict or instability resulting from hostile hybrid action.

RDCs should also be used to support partner states at risk of conflict or instability resulting from hostile hybrid action.

[15] *Resolution on the mutual defence clause (Article 42(7) TEU)*, 2015/3034(RSP) - 21/01/2016, European Parliament, https://oeil.secure.europarl.europa.eu.

[16] In 2015, EU countries agreed to support counterterrorism operations in Syria, Iraq, and the Sahel.

Conclusions and Recommendations

The creation of the EU Hybrid Toolbox will strengthen the Union's capacity to counter and respond to hybrid threats.

The creation of the EU Hybrid Toolbox will strengthen the Union's capacity to counter and respond to hybrid threats. The comprehensive set of measures, which has been in development since 2016, is characterised by flexibility of response and openness to new hybrid methods and tactics used by both state and non-state actors. The burden of responding to hostile hybrid actions lies with the Member States (as per Article 4(2) TEU), while the Union's role is to support them and coordinate joint responses to crises. The implementation of new tools and *modus operandi* will increase, among other things, situational awareness and the resilience of EU institutions, the Member States, and their societies (especially against information manipulation and foreign interference in democratic processes).

The EU Hybrid Toolbox would be a more effective instrument if it was better integrated with the fragmented set of EU policy tools to combat hybrid threats.

However, the EU Hybrid Toolbox would be a more effective instrument if it was better integrated with the fragmented set of EU policy, operational, information, and financial tools to combat hybrid threats. To streamline their use by the Member States, the EU could adopt a single document (e.g., an updated joint framework or strategy) integrating and organising the counter-hybrid toolbox, and clearly defining the division of roles, tasks, and competences between EU institutions in this area. To strengthen the EU's response capacity, the Member States should also initiate a debate on the possibility of invoking the solidarity or mutual defence clause in the event of hybrid crises.

Thanks to multilateral intelligence cooperation, the establishment of the Hybrid Fusion Cell and the Disinformation Early Warning System, the Union has significantly improved its situational awareness.

Thanks to multilateral intelligence cooperation, the establishment of the Hybrid Fusion Cell and the Disinformation Early Warning System, the Union has significantly improved its situational awareness. The complexity of hybrid threats and the anticipated expansion of sectors susceptible to weaponisation (including health security, climate change, environmental protection, or new technologies) generate the need to strengthen the analytical capabilities of these structures by increasing personnel and financial resources. It is in Poland's interest to have Polish diplomats, soldiers, and officers in these structures (especially in leadership positions). This will make it possible to influence to a greater extent the shape of policy and doctrinal documents in the area of hybrid threats. At present, Polish representatives are heading the work of East StratCom and the Intelligence Directorate of the EU Military Staff, among others.

The planned creation of new instruments for identifying disinformation campaigns and interference in political processes (FIMI) or responding to hybrid crises (EURHRTs) is only at the conceptual stage. However, the Compass does not specify exactly what elements they will consist of and under what conditions they can be used. Poland should aim for EU EURHTRs to be prepared to support the Member States and EU missions and operations, and to strengthen the resilience of partner states exposed to hostile hybrid action. In the future, Poland could seek to deploy them in Bosnia and Herzegovina, Moldova, Georgia, and others.

The EU's approach to combating hybrid threats focuses only on their non-military dimension which is insufficient for developing a military response capability for the full spectrum of hybrid methods.

The EU's approach to combating hybrid threats focuses only on their non-military dimension (i.e., disinformation, propaganda, cyberattacks), which is insufficient for developing a military response capability for the full spectrum of hybrid methods (including military or paramilitary). The Union should consider the role of the

RDCs, now being created, in a hybrid crisis on the territory of one or more Member States (e.g., instrumentalisation of migration, terrorist or subversive/sabotage activities, or infiltration of territory by armed groups). Pre-emptive deployment of these tools (e.g., in a crisis on the EU's external border) would send a clear signal to an aggressor that further escalation of the situation would be met with a strong Union response. This action should be taken in consultation with NATO, building on the principle of complementarity between the two organisations and strengthening the "European pillar" of the Alliance.

The EU should also explicitly indicate the possibility of invoking the solidarity clause in the event of a large-scale and significant hybrid crisis or the mutual assistance clause in the event of the use of military or paramilitary hybrid methods.

The EU should also explicitly indicate the possibility of invoking the solidarity clause in the event of a large-scale and significant hybrid crisis or the mutual assistance clause in the event of the use of military or paramilitary hybrid methods. This would enhance the security of the Member States, which could count on simultaneous and coherent action by the Union and NATO. The ambiguity of hybrid action (e.g., the difficulty of attributing it to a specific actor) creates the risk of divergent interpretations of a crisis, prolonged decision-making in the EU, and thus slower or inadequate Union responses. These can be minimised by developing solutions through simulations and exercises both within the EU and in cooperation with NATO based on real hybrid crisis scenarios. They should also take into account possible future forms of attacks using new methods and tactics.