ROMANIAN
MILITARY
THINKING

EU POLICIES FOR DEVELOPING CAPABILITIES TO COUNTER HYBRID THREATS

Colonel Marian ŞTEFAN

Defence Intelligence Training Centre, Ministry of National Defence

DOI: 10.55535/RMT.2023.1.9

Combating hybrid threats is one of the main dimensions of the European Union's policies expressed in the recently developed document, called "A Strategic Compass for Security and Defence", which guides the development of the Union's capabilities in the field of international security. The new document entails combining the tools developed since 2016 to combat hybrid threats in an "EU Hybrid Toolbox", which will also include new tools and modes of action. While the primary responsibility for countering hostile hybrid activity will continue to lie with member states, the EU aims to have a greater capacity to support and coordinate in order to prevent and respond adequately to new threats. The EU's approach focuses on non-military aspects and on the development of military capabilities to respond to hybrid crises, an aspect that implies increasing the importance of cooperation with NATO in this field.

Keywords: European Union; hybrid threats; policies; tools; resilience;

GENERAL ASPECTS REGARDING THE NEW EUROPEAN SECURITY PARADIGM

Living in an era of strategic competition and complex security threats involving the return of war in Europe, with Russia's unjustified and unprovoked aggression against Ukraine, as well as the current major geopolitical changes generated by China's ambitions, a series of challenges arise regarding the capacity of the European Union and implicitly of the member states to promote their vision and defend their interests. Confronted at the EU's borders and beyond with conflicts, military aggression and sources of instability, leading to humanitarian suffering and the forced displacement of millions of people, we find that hybrid threats have grown in both frequency and impact. The competition and political ambitions of some states generate increasing attempts at economic and energy coercion, and conflicts and instability are often exacerbated by the multiplier effect of climate change.

Confronted at the EU's borders and beyond with conflicts, military aggression and sources of instability, leading to humanitarian suffering and the forced displacement of millions of people, we find that hybrid threats have grown in both frequency and impact. The competition and political ambitions of some states generate increasing attempts at economic and energy coercion, and conflicts and instability are often exacerbated by the multiplier effect of climate change.

All these aspects lead to a general security landscape that has become more volatile, complex and fragmented than ever because of hybrid threats that involve the cumulative instrumentation of several coercive methods. The dynamics of local and regional instability, fuelled by dysfunctional governance and contestation of democratic values, existing in our neighbourhood, sometimes inflamed by inequality, religious and ethnic tensions, are increasingly impacted by the effects of unconventional and transnational threats as well as by geopolitical power rivalry. This erodes the capacity of the EU's multilateral system to prevent and mitigate risks and crises.

Since 2016, the EU has mobilized its resources and created new tools to combat hybrid threats. These actions are primarily the European Union's response to the destabilizing activities of Russia and China, as well as smaller states such as Belarus, Iran or North Korea, but also to the activities of non-state entities such as terrorist organizations and extremist groups. So far, the EU's efforts have focused on combating

disinformation and propaganda and strengthening the protection of critical infrastructure against cyber-attacks. In the current *"Strategic Compass"*, which was adopted by the EU Council on 21 March 2022, less than a month after the Russian invasion of Ukraine, the focus is on increasing the resilience of states and societies to information manipulation and interference in political processes, as well as on expanding the EU's capacity to support member states in responding to crises caused by hybrid methods, techniques and tactics. This is the aim of a new set of response and reaction tools called the *"EU Hybrid Toolbox"*, the final form of which will be developed by the EU in the coming months.

In the current "Strategic Compass", which was adopted by the EU Council on 21 March 2022, the focus is on increasing the resilience of states and societies to information manipulation and interference in political processes, as well as on expanding the EU's capacity to support member states in responding to crises caused by hybrid methods, techniques and tactics.

This study aims to define the current problems that European society is facing, to identify the cause of these security problems that generate a series of threats to political, economic, social, informational and military stability, and to analyse and briefly present the measures that the EU has adopted over the years to find an adapted formula of response in the key of a concept called resilience.

THE EUROPEAN APPROACH TO COUNTERING HYBRID THREATS

In 2016, in the document called *"The Common Framework for Countering Hybrid Threats"*, the EU defined the respective threats as a *"mixture of coercive and subversive activities, conventional and unconventional methods (diplomatic, military, economic, technological), which can be used in coordinated way by state or non-state actors to achieve specific objectives, being, at the same time, below the threshold of officially declared war"* (European Commission, 2016). These types of activities can be used to pursue a variety of strategic, operational and tactical objectives with the common denominator of destabilizing states and interfering in their political, social and economic processes, affecting both member states and the Community as a whole. The EU's broad approach to this issue derives from the specifics of the phenomenon itself, in particular the intricacy of hybrid actions, their complex nature and ambiguity. The response also reflects the different member states security perspectives and foreign policy priorities. This flexible approach makes it possible to take into account threats from the east (Russia, Belarus), from the south (Iran, terrorist organizations, mass illegal migration) and those with a global reach (China).

The catalogue of hybrid methods and tactics includes disinformation and propaganda activities, cyber attacks, interference in political processes (e.g. elections and referendums), economic pressure, instrumentalization of irregular migration, state support of armed groups and employment of mercenaries, subversive information operations, terrorist activities or the use of chemical, biological, radiological and nuclear (CBRN) agents. Hybrid methods can be used to different extents and intensities and can be freely combined by state or non-state aggressors whose *modus operandi* is not the same. In addition, the catalogue of hybrid instruments of war is *"open"* to any actions that may produce disruptive effects at the societal level. According to the EU institutions, the growing political rivalries with the Russian Federation (especially after the invasion of Ukraine) and China, the unstable situation in the EU's neighbourhood, the militarization of vital sectors (e.g. health security issues) and environmental issues and access to resources can constitute risk factors for the security of the community space. It is exemplified by Russian and Chinese vaccination disinformation campaigns during the COVID-19 pandemic. Similarly, issues such as environmental protection can be used to create social polarization and divisions within the EU. Climate change, in turn, may contribute to the destabilization of the Union's southern neighbourhood, migration crises and the emergence of terrorist organisations. The instrumentalization of these phenomena by external actors (e.g. the creation of routes for the illegal introduction of migrants or the support for radical formations or groups to commit terrorist attacks) represents a direct threat to EU states. The catalogue of hybrid threats is also expanded by emerging and disruptive technologies (EDT), including the development of artificial intelligence, providing advanced technical capabilities for disinformation and propaganda campaigns, as well as intelligence-gathering and subversion activities. These considerations make it much more difficult to develop response procedures to various hybrid attack scenarios, which, because of the cross-border and networked nature of hybrid threats, require a comprehensive and multi-dimensional approach to detection, early warning, countermeasures and emergency response.

The catalogue of hybrid methods and tactics includes disinformation and propaganda activities, cyber attacks, interference in political processes, economic pressure, instrumentalization of irregular migration, state support of armed groups and employment of mercenaries, subversive information operations, terrorist activities or the use of chemical, biological, radiological and nuclear (CBRN) agents.

Since 2016, the EU has set out to develop capabilities to counter hybrid threats starting from four essential areas: (1) situational awareness; (2) building and applying resilience policies; (3) countering

and responding to crises (including overcoming their effects); and (4) cooperation and coordination with partners and international organizations (mainly NATO). In this regard, the current *"Strategic 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 rests with national security institutions (e.g. intelligence, security services, police and military), which have the legal authority and executive powers to do so (under Article 4 paragraph (2) of the TEU). The Strategic Compass does not make changes in this area, instead the tools developed under the EU Hybrid Toolbox are intended to provide greater support in the national efforts to combat hybrid threats and to coordinate the joint actions of member states to achieve synergies and a more efficient response.

The burden of responsibility for countering hybrid threats rests with national security institutions which have the legal authority and executive powers to do so. The Strategic Compass does not make changes in this area, instead the tools developed under the EU Hybrid Toolbox are intended to provide greater support in the national efforts to combat hybrid threats and to coordinate the joint actions of member states to achieve synergies and a more efficient response.

THE IMPORTANCE OF JOINT ACTIONS

The *Strategic Compass* underlines the importance of continuing to strengthen the EU's intelligence capabilities to provide situational awareness and threat forecasting capabilities. The creation of hybrid threat intelligence sharing mechanisms is of particular importance to identify in the first place a *modus operandi* of foreign intelligence services that are instrumental in such actions. Improving the awareness of EU institutions and member states in this area will enhance the EU's ability to detect and respond in a prompt and adaptive manner to crises caused by hybrid methods of hostile vectors. It will also improve the coordination of actions taken by individual member states. Activities in this field were initiated in 2016 with the creation of the Hybrid Fusion Cell within the EU Intelligence and Situation Centre (EU INTCENT). It is made up of civilian and military analysts (from the Intelligence Directorate of the EU Military Staff, EUMS) responsible for producing reports, briefings and analyses within the Single Intelligence Analysis Capacity (SIAC) on hybrid threats that are identified at the level of EU countries and its neighbourhood. The studies are carried out on the basis of information from open and classified sources provided by the intelligence and security services of the member states, EU agencies (e.g. European Cybercrime Centre, European Counter-Terrorism Centre or Frontex) and partner countries (e.g. USA, Canada, Norway).

As regards cyber threat intelligence, the work of the Hybrid Fusion Cell is supported by representatives of the EU Institutions Cyber Emergency Response Team (CERT-EU). The exchange of sensitive information regarding, for example, technical details of accounts, administrators, software or infrastructure used to carry out a disinformation operation, is crucial in order to be able to assign responsibility for these actions to a specific entity and impose sanctions on it (Kaca, 2021).

The Hybrid Fusion Cell is the main institution responsible for providing situational awareness to the EU institutions and member states. Its creation has helped to increase the EU's ability to detect crises induced by hybrid threats at an early stage, as well as to speed up and coordinate the joint response of member states. An example in this regard is the EU's response (including in the form of effective strategic communication) to the migration crisis supported by Belarus in mid-2021 (with the support of the Russian Federation), which lasted for several months at the borders with Poland, Lithuania and Latvia (Dyner, 2022). Despite Belarusian-Russian disinformation activities aimed at creating disruptions regarding the interpretation and understanding of the situation at the border, the EU remained consistent and considered it a hybrid attack (Council of Europe, 2021).

The Hybrid Fusion Cell is the main institution responsible for providing situational awareness to the EU institutions and member states. Its creation has helped to increase the EU's ability to detect crises induced by hybrid threats at an early stage, as well as to speed up and coordinate the joint response of member states.

To raise situational awareness of hostile information manipulation, in March 2019, the EU established the Disinformation Rapid Alert System. The exchange of information within this system takes place through contact points established in each country of the Union. The system was used in 2020 during the COVID-19 pandemic, when the information space was flooded with a wave of Russian and Chinese disinformation, undermining trust in Western vaccines, EU institutions and vaccination strategies and fuelling anti-vaccination movements and protests (Ștefan, 2020). The main target of media attacks at the time was the European Medicines Agency. The system was used to exchange information between EU institutions and member states, representatives of the private sector and members of the G7 and NATO. Despite all the mechanisms and coordinated actions to combat disinformation, the wave of conspiracy theories spread by pro-Russia and pro-China news channels (including *"troll factories"*) has generated distortions of perception and mistrust among public opinion.

BUILDING RESILIENCE POLICIES AND MECHANISMS

Strengthening the resilience of EU states and societies aims to reduce their vulnerability to disinformation and propaganda by hostile entities and to develop the protection of critical infrastructure against cyber-attacks, terrorism, subversion and sabotage. The *Strategic Compass* pays particular attention to strengthening the EU's resilience against information manipulation and interference in political processes. The EU's approach to combating information manipulation consists of four elements adopted by the European Council in December 2018 in the *"Disinformation Action Plan"* and aims to: increase the capacity of EU institutions to detect, analyse and expose disinformation, strengthen coordinated and collective responses to disinformation, mobilize private sector to combat disinformation and raise awareness and improve public resilience by supporting independent journalism, fact-checking initiatives and promoting media education.

In 2015, in response to the information and psychological operations carried out by the Russian Federation to mask the actions carried out in Ukraine and in other areas of strategic interest, the East StratCom task force was established at the EU level within the European External Action Service (EEAS) to monitor, analyse and respond to Russian propaganda and disinformation campaigns across the spectrum of hybrid threats.

In 2015, in response to the information and psychological operations carried out by the Russian Federation to mask the actions carried out in Ukraine and in other areas of strategic interest, the East StratCom task force was established at the EU level within the European External Action Service (EEAS) to monitor, analyse and respond to Russian propaganda and disinformation campaigns across the spectrum of hybrid threats. East StratCom currently monitors informational messages published in over 20 languages. By mid-May of 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 courses for staff from partner countries as well as activities to strengthen independent journalism and promotes awareness of the EU and its policies in Eastern Partnership countries. Similar tasks are carried out by the teams 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 radicalization, countering the propaganda of terrorist organizations and disinformation from Russia, China, Iran or Turkey. All three teams are part of the EEAS Division for Strategic Communication, Taskforces and Intelligence Analysis (SG.STRAT.2), which supports the EU institutions in planning strategic communication policies, strategies and tools. It also provides support (e.g. in the form of analysis and guidance on how to counter disinformation)

to EU missions, operations and diplomatic missions under the Common Security and Defence Policy (CSDP), also developing 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 raise public awareness and strengthen the resilience of countries in the EU's neighbourhood to disinformation.

According to the EEAS, Russian disinformation poses the biggest threat to EU states due to its systemic nature. Russia has the resources to conduct disinformation campaigns as part of a long-term strategy to destabilize and disintegrate the Euro-Atlantic area. One of the most sensitive and vulnerable areas of disinformation in the functioning of EU states concerns 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 the UK, France, Germany and Spain) (Australian Strategic Policy Institute, 2020). They mainly took the form of disinformation campaigns and cyber-attacks, including hacking websites and modifying their content, attacks on electoral infrastructure or hacking and leaking to manipulate public opinion.

To protect EU member states' voters from disinformation and cyber interference, CERT-EU has created 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 in terms of obligations for online platforms and the advertising industry with the aim of improving the transparency of political advertising, closing down fake accounts and reducing incentives to spread misinformation. The code has been adopted, among others, by major online service platforms such as Facebook, Google, Twitter and Microsoft. They have pledged to increase the transparency of political advertising and its financing and to block those responsible for disinformation. These measures were aimed at protecting the elections for the European Parliament in May 2019.

In September 2018, the Union also adopted the "Code of Practice" governing EU countries' cooperation with the private sector in terms of obligations for online platforms and the advertising industry with the aim of improving the transparency of political advertising, closing down fake accounts and reducing incentives to spread misinformation.

The *Strategic Compass* announced the creation (until 2023) of a new mechanism to increase situational awareness and resilience of the EU, its member states and their societies against information manipulation and interference in political processes (Foreign Information Manipulation and Interference Toolbox, FIMI). The new collaboration platform

aims to standardize the methods of data collection, analysis and exchange (among member states' governments, private sector and civil society and international organisations) on the tactics, techniques and procedures used by actors who implement hybrid threats. This approach will increase the EU's ability to identify and analyse disinformation campaigns early, facilitate the collection of evidence of external interference in democratic political processes and standardize the methods of reporting such incidents. An Information Sharing and Analysis Centre (ISAC) will most likely be established as part of the FIMI Toolkit (StratCom activity report/Strategic Communication Task Forces and Information Analysis Division).

Strengthening the resilience of EU countries also refers to key sectors such as cyber security, critical infrastructure, energy, transport, defence, financial system, maritime security and space. This effort is primarily geared toward building the legal tools and capabilities needed to respond to incidents and crises caused by hybrid threats (especially in cyberspace). A breakthrough in the EU's approach to cyber security was the adoption of the "Directive on the Security of Network and Information Systems".

Strengthening the resilience of EU countries also refers to key sectors such as cyber security, critical infrastructure, energy, transport, defence, financial system, maritime security and space (Kozioł, 2022). This effort is primarily geared toward building the legal tools and capabilities needed to respond to incidents and crises caused by hybrid threats (especially in cyberspace). A breakthrough in the EU's approach to cyber security was the adoption of the *"Directive on the Security of Network and Information Systems"* (NIS Directive) in 2016. It obliges member states to guarantee common minimum standards for cyber security, including by adopting national rules, cyber security 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 Organization (ECSO), also supports research activities and public-private cooperation. The common cyber defence capabilities of the member states are, in turn, developed through four PESCO structured cooperation projects on the exchange of information on cyber incidents, coordination of activities, joint support and response, as well as research and training (The Council of the European Union, 2019).

In December 2020, the Union adopted a new cyber security strategy, which aims to increase member states' resilience to cyber attacks and better protect their critical infrastructure (European

Commission, 2020). An example of sectoral action in this area is the EU cyber diplomacy toolkit, which contains measures that act as a deterrent to potential cyber attackers. Blacklisted entities responsible for cyber attacks or supporting cyber attacks against EU states will be sanctioned by being banned from entering the EU and/or 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-convulsant agent *"Novichok"* on UK soil by Russian special services. Between 2019 and 2022, the EU also provided €11.6 million in financial support to the Organization for the Prohibition of Chemical Weapons (OPCW) to counter the development and use of chemical weapons.

ROMANIAN MILITARY THINKING

The EU Strategic Compass underlines the importance of strengthening the Union's capabilities to respond to a crisis generated by an attack of a hybrid nature. The EU has announced the creation of Hybrid Rapid Response Teams (EURHRT) by the end of 2024 to support member states in situations of hybrid attacks. It is also possible for these teams to be used for EU missions and operations, as well as to provide assistance to partner countries.

CRISIS PREVENTION AND RESPONSE

The EU *Strategic Compass* underlines the importance of strengthening the Union's capabilities to respond to a crisis generated by an attack of a hybrid nature. The EU has announced the creation of Hybrid Rapid Response Teams (EURHRT) by the end of 2024 to support member states in situations of hybrid attacks. It is also possible for these teams to be used for EU missions and operations, as well as to provide assistance to partner countries. Although the work on the establishment of EURHRTs is in the conceptual phase, they will most likely be formed in line with NATO's Counter Hybrid Threat Teams (CHSTs) established in 2018. CHSTs represent NATO's hybrid threat response tool situated below the collective defence threshold provided for in Article 5 of the North Atlantic Treaty Organization. To date, CHSTs have been used twice: first in 2019 in Montenegro in relation to election-period cyber attacks and disinformation, and in 2021 in Lithuania in relation to the Belarusian-backed border migration crisis. The teams are composed primarily of civilian experts in strategic communication, cyber security, counterintelligence, energy security and critical infrastructure protection. They can also be supplemented with military advisors, if the situation requires such an approach. 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 (Rühle, Roberts, 2021).

THE IMPORTANCE OF COOPERATION WITH NATO

The *Strategic Compass* emphasizes the importance of cooperation in countering hybrid threats with partners such as the G7, the UN and NATO. The Union attributes a key role in this regard to its relations with the North Atlantic Alliance. In 2015, NATO adopted the *"Strategy against hybrid threats"*, which has three components: preparing for hybrid attacks by improving reconnaissance and early warning capabilities, strengthening critical infrastructure protection and testing the decision-making processes within the Alliance; deterring a potential aggressor by imposing sanctions and preserving uncertainty about the nature of the response and defending allies in the event of a hybrid aggression.

In 2015, NATO adopted the "Strategy against hybrid threats", which has three components: preparing for hybrid attacks by improving reconnaissance and early warning capabilities, strengthening critical infrastructure protection and testing the decision-making processes within the Alliance; deterring a potential aggressor by imposing sanctions and preserving uncertainty about the nature of the response and defending allies in the event of a hybrid aggression.

In the joint declarations of 2016 and 2018, the EU and NATO developed a list of 74 joint actions in the security dimension, of which more than 20 can be related to countering hybrid threats. The focus is primarily on recognizing the phenomenon, raising situational awareness, building societal resilience, protecting critical infrastructure, and responding to emergencies generated by hybrid threats. Both organizations work to implement joint initiatives based on systemic mechanisms of cooperation between their own staff, on three interdependent levels: expert, intermediate (within the EU-NATO core group) and strategic (EU-NATO Steering Group). Through informal cooperation, the organizations developed a common operational protocol for sharing knowledge on hybrid operations and coordinating the responses of both institutions. The Common Framework set out the unequivocal ambition to make countering 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). It acts as a think-tank, providing expertise and advisory support and a platform for sharing experience and information on hybrid threats. The Helsinki Centre primarily contributes to situational awareness for both organizations, as does the EU's Hybrid Fusion Cell or its counterpart NATO's Hybrid Analysis Branch operating within the Joint Intelligence and Security Division (JISD). Both structures have well-established working relationships through monthly staff exchanges. 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

Working Group and the NATO Centre of Excellence for Strategic Communications (StratComCoE) in Riga, developing joint training materials, disinformation response courses and other tools for EU and NATO personnel.

On a practical level, the Helsinki Hybrid CoE is responsible for organizing 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 EU *Integrated Resolve* 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 main organization: in 2022, it will be the EU, and in 2023, NATO. The organizations also seek opportunities for joint (complementary) responses to threats in cyberspace, facilitated by joint training and exercises (e.g. *Cyber Phalanx, Locked Shields or NATO Cyber Coalition*), exchange of information and doctrinal documents, regular contacts related to work, education, projects and others. The mentioned cooperation takes place through the European Defence Agency (EDA) and the NATO Cyber Defence Centre of Excellence in Tallinn, among others. One of its important elements is cooperation in the technological domain, including the exchange of experience and practices between CERT-EU and the NATO Computer Incident Response Capability (NCIRC) at the Supreme Allied Commander Europe (SHAPE).

ROMANIAN MILITARY THINKING

Since 2017, the EU and NATO have been conducting EU Integrated Resolve 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 main organization: in 2022, it will be the EU, and in 2023, NATO.

CONCLUSIONS

The creation of the EU toolkit for responding to hybrid threats will strengthen the Union's ability to counter and respond to these types of threats. The comprehensive set of measures, which has been under development since 2016, is characterized by response flexibility and openness to identifying new methods and hybrid tactics used by both state and non-state actors. The onus to respond to hostile hybrid actions is on the member states (in accordance with Article 4(2) TEU), while the Union's role is to support them and coordinate common responses to crises. The implementation of new tools and *modus operandi* will, among other things, increase the situational awareness and resilience of EU institutions, member states and their societies (especially against information manipulation and foreign interference in democratic processes).

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 of strategic interest (including health security, climate change, environmental protection or new technologies) generate the need to strengthen the analytical capabilities of these structures by increasing staff and financial resources. It is in Romania's interest, as an EU and NATO member state, to have representatives (diplomats, specialists, military, field experts) in these structures (especially in management positions). It will enable the synchronized development and greater implementation of policy and doctrinal documents in the field of hybrid threats.

It is in Romania's interest, as an EU and NATO member state, to have representatives (diplomats, specialists, military, field experts) in these structures (especially in management positions). It will enable the synchronized development and greater implementation of policy and doctrinal documents in the field of hybrid threats.

The planned creation of new tools to identify disinformation campaigns and interference in political processes (FIMI) or hybrid crisis response (EURHRT) is only at the conceptual stage. However, the EU *Strategic Compass* does not specify exactly what elements they will consist of and under what conditions they can be used. Therefore, Romania should ensure that the EURHTRs are prepared to support EU member states and EU missions and operations and strengthen the resilience of partner states exposed to hostile hybrid actions such as the Republic of Moldova, Georgia and others.

BIBLIOGRAPHY:

1. Dyner, A.M. (2002). *"The Border Crisis as an Example of Hybrid Warfare"*. In *PISM Strategic File*, no. 2, February, https://www.pism.pl/publications/the-border-crisis-as-an-example-of-hybrid-warfare, retrieved on 24 August 2022.
2. Kaca, *E. (2021). "Sancțiunile UE pentru campaniile de dezinformare: perspective și limite"*. In *Buletinul PISM*, no. 104, 26 May 2021, www.pism.pl., retrieved on 25 August 2022.
3. Kozioł, A. (2022). *"Strategic Compass: Towards EU Space Strategy for Security and Defense"*. In *Policy Paper PISM*, no. 1, https://www.pism.pl/publications/strategic-compass-towards-eu-space-strategy-for-security-and-defence, retrieved on 1 September 2022.
4. O'Connor, S., Hanson, F., Currey, E., Beattie, T. (2020). *"Cyber-enabled foreign interference in elections and referendums"*. Australian Strategic Policy Institute, 28 October 2020, https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums, retrieved on 1 September 2022.

5. Rühle, M., Roberts, C. (2021). *"Enlarging NATO's toolbox to counter hybrid threats"*, 19 March 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html, retrieved on 2 September 2022.
6. Ștefan, M. (2020). *"Intelligence versus fake news* în *contextul COVID 19".* In *INFOSFERA*, no. 2, ISSN 2065-3395, pp. 35-43.
7. *"Joint Framework on countering hybrid threats. A European Union response"* (2016). European Commission, 6 April 2016, https://eur-lex.europa.eu., retrieved on 8 August 2022.
8. *"Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions"* (2019). The Council of the European Union, 10 December 2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf., retrieved on 5 July 2022.
9. *"The Council of the European Union Conclusions on 21 and 22 October 2021"*. The Council of the European Union, https://www.consilium.europa.eu/media/52622/20211022-euco-conclusions-en.pdf., retrieved on 17 August 2022.
10. *"Resolution on the mutual defence clause (Article 42 (7) TEU)"*. European Parliament, https://oeil.secure.europarl.europa.eu., retrieved on 26 August 2022.
11. *"EU Cyber Defence Strategy for the digital age"* (2020). European Commission, 16 December 2020, https://digital-strategy.ec.europa.eu., retrieved on 12 May 2022.
12. *"2021 StratCom activity report – Strategic Communication Task Forces and Information Analysis Division"* (24 March 2022), https://www.eeas.europa.eu., retrieved on 27 April 2022.
13. https://euvsdisinfo.eu/ro/#, retrieved on 11 August 2022.
14. https://www.consilium.europa.eu/ro/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/, retrieved on 29 August 2022.
15. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232, retrieved on 28 August 2022.
16. https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf., retrieved on 28 August 2022.
17. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf, retrieved on 29 August 2022.
18. https://www.nato.int/cps/en/natohq/topics_156338.htm., retrieved on 22 August 2022.