UDC 327.5
DOI https://doi.org/10.20535/2308-5053.2022.2(54).264384

OVERVIEW OF NATO AND EU'S STRUGGLE AGAINST HYBRID THREATS

Ahmadly J.
Phd student
Baku State University
ORCID ID: 0000-0002-4195-9459
jeyhun.ahmadli9204@gmail.com

The main aim of the article is to analyze the main elements of the NATO and European Union strategy to combat Russian hybrid threats against Ukraine since 2014. It is noted that Russia since this period has put the issue of hybrid threats at the top of the international agenda.

Methods. To obtain exhaustive results, the method of comparative analysis was used. Also, the content analysis method was used to identify the fundamental points of the strategies of NATO and the EU to combat hybrid threats, as well as to determine the ratio of tools used by both organizations. This study also uses a strong empirical background and a descriptive research method.

The scientific novelty lies in the fact that the author tried to clarify the preparation of the West for a possible hybrid war. In particular, the author focuses on testing the resilience of the West against the backdrop of hybrid threats posed by Russia.

Conclusions. Summing up, the author notes that NATO and the European Union have created special institutions that develop a fundamental strategy to combat Russia's hybrid threats. It is emphasized that since the beginning of the Ukrainian crisis, one of the main topics at all NATO summits has been devoted to the development of a joint strategy to combat hybrid threats. In this context, serious steps have been taken to form a legal framework and identify practical steps. In general, the crisis in Ukraine has radically changed the security paradigm in Europe. It is also noted that against the backdrop of emerging hybrid threats, NATO and the EU have undergone functional and structural changes to form a new concept of security.

At the end of the article, the author notes that achieving a high level of preparedness is possible through regular monitoring and analysis to identify weaknesses (risks). Increasing civilian resilience and effective use of strategic communications are among the most important conditions in the fight against hybrid threats. As a result of this work, it can be said that the EU and NATO have very improved capabilities to defend against hybrid threats.

Key words: NATO, hybrid threats, hybrid war, military escalation, threat to the integrity of the state.

Introduction. As a defense bloc, NATO attaches great importance to combat hybrid threats for protecting member and partner states. The strategy of the Alliance is based on the three main principles: Prepare, deter, defend. These concepts are characterized as key milestones in NATO's strategy in combating hybrid threats. NATO's overall approach is that member states must be prepared at all times for hybrid threats from abroad. We can also characterize this stage as a regular study of the current situation. During the preparatory phase, the Alliance collects information that contains a hybrid threat element, exchanges it, and finally conducts relevant analysis to form a clear picture of the current situation. The main goal here is to be able to immediately identify a potential hybrid threat and take swift action against it. For example, one of the main activities of the Joint Intelligence and Security Directorate of NATO Headquarters is to conduct regular monitoring and analysis of hybrid threats. The Department's Hybrid Analysis Division provides decision makers with relevant information on potential hybrid threats. The department also carries out intelligence exchanges between member countries on hybrid threats. However, experience shows that the Alliance faces common challenges in the exchange of intelligence. Due to a lack of trust, some member

states are reluctant to share such information. Therefore, within NATO, cooperation in this area often takes place bilaterally or between a group of countries (Ballast, 2027).

The Alliance pays special attention to training in the preparatory phase of the fight against hybrid threats and the importance of appropriate education in this area. Since 2016, the organization's annual Crisis Management Training has included hybrid scenarios involving misinformation and "gray zone" situations (Martens Center, 2020). Live trainings are also organized under the names NRF*, VJTF*, Trident Juncture*, Brilliant Jump*, Noble Jump* to test the allies' ability and level of readiness against military hybrid threats. During these exercises, NATO forces become more professional in performing tasks, such as protecting critical infrastructure and combating irregular forces. In addition, the main mission of the NATO Cyber Defense Center, which specializes in hybrid threats, is to provide training and exercises in the field of cyber defense to member and partner countries, and to provide fundamental research in this area. Headquartered in Tallinn, Estonia, the Center has been organizing scientific-practical conferences, live trainings and exercises in the field of cyber defense and security every year since its establishment. The center, which analyzes and studies all aspects of information security and cyber defense, received the status of an International Military Organization on October 28, 2008.

One of the key phases of NATO's defense strategy against hybrid threats is deterrence. The main goal here is to change the behavior of the enemy by intimidating it. At the 2016 Warsaw Summit, members of the Alliance unanimously stated that hybrid attacks could provide a basis for the implementation of Article 5 of the Charter. "NATO is ready to assist its ally at any stage of a hybrid campaign. In this case, guided by Article 5 of the Charter, a decision may be made to implement collective defense measures", the summit's final communiqué said (Warsaw Summit Communiqué, 2016). As a follow-up to this statement, in July 2018, NATO leaders agreed to form Counter-Hybrid Support Groups. According to the agreement, these groups can be activated at the request of one of the allied countries. This group, which consists mainly of civilian experts, is sent to member countries, if necessary, to identify the weaknesses of those countries during possible hybrid attacks and provide relevant advice. In 2019, such a group was sent to Montenegro for the first time. The goal was to protect the country's 2020 elections from Russian cyber-attacks (Rühle&Roberts, 2021). It should be noted that since 2016, various attempts at a coup d'etat have been organized in Montenegro through hybrid attacks (Lekic, 2019). NATO Secretary General Jens Stoltenberg later said, following a meeting of defense ministers of member states, that the alliance was completing the process of setting up task forces to defend against hybrid attacks. "We have made significant progress in the process of creating special teams to protect against hybrid threats. These groups will provide technical assistance to member states in repelling hybrid attacks", Stoltenberg said (Stoltenberq, 2018). Thus, referring to the documents adopted in recent years and the practical activities carried out, we can say that NATO's deterrence has increased significantly.

According to NATO's defense strategy against hybrid threats, if the deterrent policy does not force the aggressor to step back, the Alliance will begin to implement an effective defense plan. The steps to be taken for defense may vary depending on the type of threat. One of the main goals here is to prevent the hybrid conflict from escalating to a military level. It should be noted that NATO's advantage over hybrid threats of a military nature is largely due to its highly specialized Joint Task Force (VJTF). The main priority in combating non-military hybrid threats is cyber security. According to NATO officials, cyberattacks are one of the strengths of Russia's hybrid war strategy. When Stoltenberg defines hybrid warfare, he emphasizes its cyber size. Protection from cyber intrusion is one of the Alliance's number one security priorities (Stoltenberq, 2015).

NATO believes that establishing effective communication between collective defense, crisis management and cooperative security can significantly facilitate protection against hybrid threats. This necessitates the formation of a reliable network between states, organizations and individuals that can withstand the hybrid threat. In general, the overall approach prevailing in the West is that strategic communication is a key factor in the fight against hybrid threats. NATO adopted its strategic communication concept at the Strasbourg summit in 2009. The final declaration of the summit stated that strategic communication was an integral part of the Alliance's efforts to achieve its political and military goals (Kehl Summit Declaration, 2009). Russia's disinformation attacks on Ukraine since 2014 have led to a more fundamental study of strategic communication within NATO. The establishment of the Center for Strategic Communications in 2014 stemmed from this need. The Center's main mission is to make a significant contribution to the strategic communication capabilities of NATO institutions, NATO allies and NATO partners. The "heart" of the center is an international trainer, analyst and research team with military, political and academic careers.

One of the key features of NATO's strategy to combat hybrid threats is to strengthen the resilience of civil institutions and society. At the 2016 Warsaw Summit, it was decided to strengthen military resilience in addition to improving military capabilities against hybrid threats. The final declaration stated that civil training

was a key pillar of the Alliance's fight against hybrid threats (Warsaw Summit Communiqué, 2016, par. 73). In general, providing civilian training is a matter of national security for member states. The Alliance has set up expert groups to assess and advise its allies on the state of civil preparedness. In addition, issues related to civilian training have been included in NATO's Defense Planning Process.

One of the important steps in the successful defense of hybrid threats is the deepening of relations between NATO and the European Union in this area. Both organizations are implementing Parallel and Coordinated Tasks (PACE*) to effectively combat hybrid threats. The European Center Against Hybrid Threats, established in 2016, is one of the initiatives that embodies the joint struggle of NATO and the European Union against hybrid threats (Rühle, 2019). The main task of the center is to develop the ability of member states to combat hybrid threats. Promoting government-society interaction in this area, the Center pays special attention to issues such as the exchange of experience, testing new ideas and approaches, and organizing relevant training courses and exercises. The Center also plays an important role as a platform for strategic discussions between NATO and the European Union, as well as for joint exercises. The Center, which brings together more than 1,200 practitioners and specialists, also organizes trainings and scientific discussions on hybrid threats for the private sector and academia (Arvonen, 2020).

The European Union is one of the international organizations with the best experience in combating hybrid threats. The EU can also be considered the organization with the most comprehensive legal framework in this area. Russia's large-scale disinformation attacks on Ukrainian and Western institutions since 2014 have prompted the European Union to develop a conceptual strategy to combat hybrid threats. On April 6, 2016, the Joint Communication on Countering Hybrid Threats was established within the European Union to ensure a coordinated fight against hybrid threats. The initiative was characterized as a timely step against the backdrop of dramatic changes in the EU's security environment and, in particular, calls for peace and stability in the Union's eastern and southern neighborhoods. Joint Communication interprets the concept of hybrid threat as "a mixture of violent and subversive activities in which traditional and non-traditional methods coordinated by governmental or non-governmental actors are used simultaneously (diplomatic, military, economic and technological) to achieve specific goals" (Document 52016JC0018, 2016). The Commonwealth encourages member countries to take steps in the following areas:

- Conduct continuous hybrid risk studies to identify security vulnerabilities;
- Development of strategic communication;
- Increased attention to the protection of critical infrastructure;
- Diversification of energy sources and continuous monitoring of threats to the economic sector;
- Raising public awareness of hybrid threats;
- Always keep the force financing hybrid attacks under sanctions;
- Increase resistance to radicalism and extremism, including violence;
- To cooperate with the third countries;
- Deepen cooperation with NATO;
- Ensuring effective management in crisis situations.

Ensuring security in cyberspace is central to the European Union's fight against hybrid threats. It is worthy to note that in 2017, two large-scale cyberattacks (WannaCry and NotPetya) revealed the EU's main weaknesses in this area. The attacks severely damaged the UK's healthcare system, large companies in Germany and France, as well as various Ukrainian government agencies. The adoption of the first EU cybersecurity legislation comes in 2016. The Network and Information Systems Security Guidelines (NIS Directive), adopted on 6 July of that year, have made great strides in increasing resistance and resilience to hybrid threats. Thus, the official Brussels has begun to develop a regulatory framework in the field of cyber security. The NIS Directive required member states to adopt their own cyber security strategies, form Computer Security Incident Response Teams (CSIRT) and a network of these commandos across Europe. One of the requirements of the NIS Directive was to ensure that the public and private sectors work together on cyber security issues.

In 2019, the Council of the European Union announced that severe sanctions will be imposed on the responsible countries and institutions in the event of cyberattacks against member states. The sanctions package includes a ban on entry into EU countries or the freezing of goods and property in EU member states. This precautionary step could greatly help neutralize future cyberattacks on EU countries. In addition, since 2017, a number of military cooperation projects in the field of cyber defense have been implemented in Europe. These projects include information exchange, effective coordination, development of rapid response capabilities in cyberspace, cyber education, innovations and etc.

In addition to taking effective protection measures in the field of cyber security, the European Union also supports the development of research programs and public-private partnerships. The EU Cyber Security Agency (ENISA) and the European Cyber Security Organization (established in 2016) play a special role here. The first is to develop recommendations and exchange experiences on cybersecurity, while the second is to deepen trilateral cooperation between the European Commission, member states and the business community.

Despite all these effective measures, the measures taken by the EU in the field of cybersecurity have not fully yielded the expected results. For example, there were serious disagreements among all member states regarding the funding of the above-mentioned organizations. Another obstacle was the different cybersecurity strategies pursued by member countries. For instance, approaches to the application of Chinese technology in the development of 5G were not unanimously welcomed by some member states.

The European Union defines misinformation as "deliberate misinformation or misrepresentation for the purpose of deceiving the public or gaining economic benefits" (Tackling online disinformation, 2020). The general approach of Europe is that the fight against disinformation must always be at the forefront to protect democratic elections from foreign interference and manipulation. Terrorist propaganda is also one of the serious threats posed by disinformation in Europe. The European Union focuses on monitoring and disclosing such information in the fight against misinformation, as well as cooperating with online platforms.

Since 2015, the European Union has established a number of mechanisms to monitor and detect misinformation. First, the East StratCom Task Force was set up under the EU External Action Service to analyze disinformation trends from Russia. The Group has three main priorities: effective communication and promotion of the EU's Eastern Partnership policy; Strengthening the overall media environment within the Union and in the Eastern Partnership countries (especially media freedom and support for independent media); Strengthening the Union's capabilities in forecasting and responding to Russia's disinformation activities. According to official reports, the group has already analyzed and cataloged more than 4,500 Russian misinformation attempts. The main focus of the monitoring is the Eastern Partnership countries and Russia's local and international media. Later, similar groups were formed in the Western Balkans and the Southern Neighborhood. In addition, in connection with the 2019 European Parliament elections, the European Fact Checker Network and the Rapid Warning System against Online Misinformation have been established. In December 2018, the European Union's Action Plan against Misinformation was approved. This action plan focuses on strengthening coordination in the fight against misinformation, involving the private sector in the fight, as well as increasing society's resilience to misinformation.

One of the main approaches of the European Union is that the development of an independent media can play an important role in the fight against misinformation. In this regard, the European Commission supports investigative journalists and independent media for their contribution to exposing misinformation. The Commission is implementing a number of specific programs to support the development of the media, including financial assistance.

The European Union believes that misinformation undermines citizens' trust in democracy and democratic institutions. Misinformation leads to the polarization of public opinion and, consequently, complicates the democratic decision-making process. In short, misinformation can also be used to undermine the democratic European project. Therefore, it is imperative to take strong commitments and take swift steps to protect the democratic process and the trust of citizens in government. Protecting elections from foreign interference is a key EU priority: Citizens of EU member states must have the right to freely express their democratic choices in elections, without outside manipulation or interference.

One of the EU's ways to combat misinformation is to impose sanctions. Commission Vice President Vera Jourova announced in December 2020 that the European Union planned to impose sanctions on China and Russia in response to information provocations. In particular, the European Union considers it appropriate to take punitive measures against the manipulative steps of these countries aimed at creating confusion in the European information space about the COVID-19 virus. The European Commission has also announced that a new draft law on the transparency of political propaganda will be drafted from 2021. The organization has launched the following initiatives to combat misinformation: World standards of self-regulation called The Code of Practice on Disinformation have been established; The European Digital Media Observatory, which brings together fact-checkers, academics and other stakeholders to support political decision-makers, was established; An Action Plan was adopted to increase the EU's ability to combat misinformation and deepen cooperation between member states in this area.

Involvement of the private sector in the fight against misinformation is one of the activities supported by the European Union. The role of online media platforms and the advertising sector is noteworthy here. For example, online media platforms that have signed The Code of Practice on Disinformation have acted in line with their commitments during the 2019 European Parliament elections. According to the European Commission, in the run-up to the election, co-operated online platforms ensured the transparency of political advertisements, verified the source of sponsored shares with effective tools, closed fake accounts immediately and took action to identify automated bots. Under the agreement, online platforms should work with national audio-visual regulators, independent fact-checkers and researchers to detect misinformation campaigns and disseminate fact-based content more widely during elections. It is worthy to note that social media giants such as Facebook, Google and Twitter have also made some commitments to the European Commission (Action Plan against Disinformation, 2018). There are also reports that the commission will soon introduce

new rules that will allow it to better monitor the activities of large platforms in the fight against misinformation. This indicates the intention of the European Commission to strengthen control over the world's largest digital companies. The new rules also provide for sanctions against giant digital platforms, if necessary.

Conclusion

The hybrid threat phenomenon has been on the agendas of NATO and European Union since 2014. Although 7 years is not a long time, the Alliance and EU has been able to develop an effective defense strategy against hybrid threats during this time. To this end, both organizations have managed to form a legal framework, as well as a kind of fundamental approach, focusing on research and training. The main approach of the both organizations is that effective protection against hybrid threats goes through the level of readiness of member countries. Achieving a high level of preparedness is possible through regular monitoring and analysis to identify weaknesses (risks). Strengthening resilience at the civilian level and the effective use of strategic communication are among the most important conditions in the fight against hybrid threats. As a result of this work, we can say that the EU and NATO`s have a very improved defense capabilities against hybrid threats.

Ахмадлі Дж. Огляд боротьби НАТО і ЄС проти гібридних загроз

Основна мета статті – аналіз основних елементів стратегії НАТО та Європейського Союзу по боротьбі з гібридними загрозами Росії проти України з 2014 року. Зазначається, що Росія з цього періоду поставила питання про гібридні загрози на перше місце у міжнародному порядку денному.

Методи. Для отримання вичерпних результатів використали метод порівняльного аналізу. Також метод контент-аналізу був використаний для виявлення принципових моментів стратегій НАТО та ЄС щодо боротьби з гібридними погрозами, а також для з'ясування співвідношення інструментів, які застосовуються обома організаціями. У цьому дослідженні також використовується сильний емпіричний фон та описовий метод дослідження.

Наукова новизна полягає в тому, що автор спробував прояснити підготовку Заходу до можливої гібридної війни. Зокрема, основна увага автора спрямована на перевірку стійкості Заходу на тлі гібридних загроз, які створюють Росія.

Висновки. Підсумовуючи, автор зазначає, що НАТО та Європейський Союз створив спеціальні інститути, які розробляють фундаментальну стратегію боротьби з гібридними загрозами Росії. Наголошується, що з початку української кризи одна з головних тем на всіх самітах НАТО була присвячена розробці спільної стратегії боротьби з гібридними загрозами. У цьому контексті були зроблені серйозні кроки щодо формування правової бази та визначення практичних кроків. Загалом криза в Україні радикально змінила парадигму безпеки в Європі. Також, зазначається, що на тлі гібридних загроз НАТО і ЄС, що виникають, зазнали функціональних і структурних змін для формування нової концепції безпеки.

Наприкінці статті автор зазначає, що досягнення високого рівня готовності можливе за рахунок регулярного моніторингу та аналізу для виявлення слабких місць (ризиків). Підвищення стійкості на цивільному рівні та ефективне використання стратегічного зв'язку є одними з найважливіших умов боротьби з гібридними загрозами. В результаті цієї роботи можна сказати, що ЄС і НАТО мають дуже покращені можливості захисту від гібридних загроз.

Ключові слова: НАТО, гібридні загрози, гібридна війна, військова ескалація, загроза цілісності держави.

Bibliography:

1. Ballast, J. (2017) 'Trust (in) NATO – The future of intelligence sharing within the Alliance', NATO Defense College, Research Paper, No. 140, September 2017, https://www.ndc.nato.int/news/news.php?icode=1085 (на англ.яз.)
2. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, European View 2020, Martens Center for European Studies, Vol. 19(1) 62–70. https://journals.sagepub.com/doi/pdf/10.1177/1781685820912041 (на англ.яз.)
3. Press Release 100 (2016), Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (на англ.яз.)
4. Michael Rühle, Clare Roberts (2021). Enlarging NATO's toolbox to counter hybrid threats, 19 March, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (на англ.яз.)

5. Lekic, Slobodan (2019), First NATO counter-hybrid warfare team to deploy to Montenegro, Stars and Stripes webpage, 8 November, https://www.stripes.com/news/first-nato-counter-hybrid-warfare-team-to-deploy-to-montenegro-1.606562 (на англ.яз.)
6. Stoltenberq (2018), *Stoltenberg [NATO prepares response to Russian hybrid threats],* NATO Rusiyanın hibrid təhdidlərinə cavab hazırlayır» – 05/10 https://azpolitika.info/?p=455828 (на азербайджанском яз.)
7. BBC News (2016), NATO to Counter 'Hybrid Warfare' from Russia, (May 14, 2015), retrieved September 12, from http://www.bbc.com/news/world-europe-32741688 (на англ.яз.)
8. NATO. Strasbourg (2009) / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl. April, https://www.nato.int/cps/en/natolive/news_52837.htm (на англ.яз.)
9. NATO Warsaw Summit Communiqué. (2016, 9 Jul). Available at https://www.nato.int/cps/en/natohq/official_texts_133169.htm (на англ.яз.)
10. Rühle, Michael (2019), NATO's Response to Hybrid Threats, https://www.realcleardefense.com/articles/2019/11/05/natos_response_to_hybrid_threats_114832.html (на англ.яз.)
11. What is Hybrid CoE (2020), https://www.hybridcoe.fi/who-what-and-how/
12. European Commission (2016). Joint framework on countering hybrid threats: A European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (на англ.яз.)
13. Tackling online disinformation (2020). https://digital-strategy.ec.europa.eu/en/policies/online-disinformation (на англ.яз.)
14. Action Plan against Disinformation (2018). European Commission contribution to the European Council, December 5, https://ec.europa.eu/info/sites/default/files/eu-communication-disinformation- euco-05122018_en.pdf (на англ.яз.)

References:

1. Ballast, J. (2017) 'Trust (in) NATO – The future of intelligence sharing within the Alliance', NATO Defense College, Research Paper, No. 140, September 2017, https://www.ndc.nato.int/news/news.php?icode=1085
2. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, European View 2020, Martens Center for European Studies, Vol. 19(1) 62–70. https://journals.sagepub.com/doi/pdf/10.1177/1781685820912041
3. Press Release 100 (2016), Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm
4. Michael Rühle, Clare Roberts (2021). Enlarging NATO's toolbox to counter hybrid threats, 19 March, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html
5. Lekic, Slobodan (2019), First NATO counter-hybrid warfare team to deploy to Montenegro, Stars and Stripes webpage, 8 November, https://www.stripes.com/news/first-nato-counter-hybrid-warfare-team-to-deploy-to-montenegro-1.606562
6. Stoltenberq (2018), *Stoltenberg [NATO prepares response to Russian hybrid threats],* NATO Rusiyanın hibrid təhdidlərinə cavab hazırlayır» – 05/10 https://azpolitika.info/?p=455828
7. BBC News (2016), NATO to Counter 'Hybrid Warfare' from Russia, (May 14, 2015), retrieved September 12, from http://www.bbc.com/news/world-europe-32741688
8. NATO. Strasbourg (2009) / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl. April, https://www.nato.int/cps/en/natolive/news_52837.htm
9. NATO Warsaw Summit Communiqué. (2016, 9 Jul). Available at https://www.nato.int/cps/en/natohq/official_texts_133169.htm
10. Rühle, Michael (2019), NATO's Response to Hybrid Threats, https://www.realcleardefense.com/articles/2019/11/05/natos_response_to_hybrid_threats_114832.html
11. What is Hybrid CoE (2020), https://www.hybridcoe.fi/who-what-and-how/
12. European Commission (2016). Joint framework on countering hybrid threats: A European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
13. Tackling online disinformation (2020). https://digital-strategy.ec.europa.eu/en/policies/online-disinformation
14. Action Plan against Disinformation (2018). European Commission contribution to the European Council, December 5, https://ec.europa.eu/info/sites/default/files/eu-communication-disinformation-euco-05122018_en.pdf

Стаття надійшла до редакції 17.05.2022
Стаття рекомендована до друку 08.06.2022