УДК 32:323:327.5:327.8

NATO'S COMMUNICATION STRATEGIES IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

КОМУНІКАЦІЙНІ СТРАТЕГІЇ НАТО В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Serhiy DANYLENKO
Doctor of political sciences (Dr.hab.), Professor, Head of the department of international media communications and communication technologies of the Institute of International Relations Taras Shevchenko National University of Kyiv
s_danylenko@ukr.net
ORCID ID 0000-0003-3435-2146

Zhanna PATSYORA
Postgraduate student of the educational and scientific program Doctor of Philosophy 291 "International Relations, Public Communications and Regional Studies" of the Educational and Scientific Institute of International Relations of Taras Shevchenko National University of Kyiv
e-mail: jpatsyora@gmail.com
ORCID ID 0009-0007-5388- 980X

Сергій ДАНИЛЕНКО
Доктор політичних наук, професор, завідувач кафедри міжнародних медіа комунікацій та комунікаційних технологій Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
s_danylenko@ukr.net
ORCID ID 0000-0003-3435-2146

Жанна ПАЦЬОРА
аспірантка освітньо-наукової програми доктора філософії 291 "Міжнародні відносини, суспільні комунікації та регіональні студії" Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
e-mail: jpatsyora@gmail.com
ORCID ID 0009-0007-5388- 980X

Abstract. *The article is devoted to the analysis of NATO's communication strategies in the context of the Russian-Ukrainian war. The dynamics and main objects of the communication policy of the Alliance are analyzed. Effective mechanisms for ensuring regional and international security within the framework of collective security and combining the efforts of allies have been determined. Ways of reaction of NATO member states to new challenges for the international security system have been studied: hybrid threats, cyber terrorism, disinformation, destructive informational influences. The key priorities of cooperation between Ukraine and NATO for countering aggression from the Russian Federation and restoring the territorial integrity of Ukraine are outlined.*

Keywords: *NATO, Ukraine, communication strategies, Russian-Ukrainian war, international security, information security, hybrid threats, cybersecurity, disinformation.*

Анотація. *Стаття присвячена аналізу комунікаційних стратегій НАТО в контексті російсько-української війни. Проаналізовано динаміку та головні об'єкти комунікаційної політики Альянсу. Визначено дієві механізми забезпечення регіональної та міжнародної безпеки в рамках колективної безпеки та об'єднання зусиль союзників. Досліджено шляхи реагування держав-учасниць НАТО на нові виклики для системи міжнародної безпеки: гібридні загрози, кібертероризм, дезінформація, деструктивні інформаційні впливи. Окреслені ключові пріоритети співробітництва між Україною та НАТО для протидії агресії з боку Російської Федерації та відновлення територіальної цілісності України.*

Ключові слова: *НАТО, Україна, комунікаційні стратегії, російсько-українська війна*, міжнародна безпека, інформаційна безпека, гібридні загрози, кібербезпека, дезінформація.

Introduction. The Russian-Ukrainian war has become a turning point in world history, changing the picture of the world. The war has destroyed the world order, called into question the world's perception of international security, jeopardized the independence of one of the largest

countries in Europe, brought back the ghost of nuclear confrontation, destroyed the global economy, and has already led to the deaths of hundreds of thousands of people. The Russian-Ukrainian war has demonstrated the ineffectiveness of modern mechanisms for preventing and resolving crises.

Actors of international relations realize the necessity of moving towards solving geopolitical problems, resolving international conflicts, and ensuring national interests using non-military methods and technologies. Modern technologies provide such a devastating capability to the actors of international relations that the use of "hard power" is potentially, with a high probability, to endanger the existence of humanity in large areas and in many regions of the world.

The concept of national resilience, the ability of the state and society to effectively counter threats, adapt to changes in the security environment and ensure stable functioning during crises, is becoming increasingly relevant. It means, first and foremost, the acquisition by states and organizations of a certain set of capabilities required for safe existence in the face of increased risks and crises, as well as for rapid recovery from a crisis. The current level of global interconnectedness necessitates the formation of an international coalition to combat information threats. The point is to share experience, information and support each other. It is necessary to jointly develop protection mechanisms, counteract threats, and adapt international standards of regulation in the media and cyberspace to new challenges without violating the principles of democracy. This is a challenge not only for individual states, but also for organizations, alliances and unions based on collective decision-making. Ukraine is making considerable efforts to create a set of measures to counteract real and information warfare by joining the process of international integration and cooperation, enhancing a wide-scale information policy based on the use of modern technologies and rapid response.

In the light of the current Russian-Ukrainian war, many models of international security have proven to be inefficient, failed, and ineffective. For instance, the system of international law and the activities of the United Nations concerning sustainable peace and security have been criticized. The system of collective security and the unification of allied efforts has proven to be one of the most effective mechanisms for ensuring regional and international security. At present, there is a progressive advance of strengthening and consolidation of the “collective West”, strengthening the Euro-Atlantic system of international security.

The North Atlantic Treaty Organization (NATO) supports the inalienable right of independent states to individual or collective defence (*The North Atlantic* 1949). Considering the changes in the international security system, the violation of the territorial integrity of one of the European countries, the deployment of a full-scale Russian-Ukrainian war, and the emergence of new methods of hybrid confrontation, it is important to study the changes and directions of NATO's communication strategy in the field of regional and international security.

Analysis of recent research and publications. The Ukrainian school of research on the use of information and psychological influences is represented by the works of Voloshenko I., Makarenko E.A., Marchuk E.K., Meleshchenko T., Pavliuk V.V., Perepelytsia H.M., Polovnyk P.M., Polyakov O.M., Sydoruk T.V., Shpura M.I., etc. In their works, Ukrainian researchers mainly cover the issues of intensification of cooperation in the field of regional and international security between Ukraine and NATO, prospects and problems of Ukraine's European integration aspirations, the main trends in the transformation of the North Atlantic Treaty Organization, NATO enlargement as a false pretext to justify Russia's aggression against Ukraine, strengthening the Alliance's capabilities in countering hybrid threats and cyberterrorism.

The aim of the article. The article studies features and directions of NATO's communication strategies in the context of the Russian-Ukrainian war.

Presentation of the main research material. The necessity to combine the functions of defence sufficiency and international security has challenged the Alliance to strengthen political structures, introduce information and analytical monitoring of conflict situations in Europe, apply predictive decision-making methods, extend the competence of activities beyond the Organization, and provide information means for the perception of NATO's foreign policy doctrine. This has determined NATO's task of responding to new security challenges through information programs, policy initiatives, preventive diplomacy, strategic communications, and information operations. NATO's information strategies are designed to provide access to the organization's sources, to use

communication tools via the Internet, to provide an opportunity to disseminate position papers, to respond to public inquiries, to ensure media relations, and to ensure cybersecurity of the Alliance's activities (Makarenko Ye. et al., 2023).

NATO has always paid great attention to communication strategies as part of its international security policy. The North Atlantic Treaty Organization has an extensive system of communication units such as the NATO Communication and Information Systems Services Agency, the NATO Headquarters Information Systems Service, the NATO Information and Press Service, the NATO Situation Room, the NATO Electronic Warfare Advisory Committee, the NATO Subcommittee on Radio Frequency Management, and the NATO Communications and Information Systems School. These services and structures carry out joint projects on the implementation of the concept of information security, information support for political consultations and negotiations during crises and in the post-conflict period, management of information flows and databases in war zones, protection of computer networks and systems from possible use of information weapons.

The processes of shaping the international security system and transforming NATO are permanent, but it is the Russian influence factor and the Russian-Ukrainian war that have become the determining factors of change over the past decade. The annexation of Crimea by the Russian Federation in 2014, the undeclared war in the East of Ukraine, and the rise of hybrid threats like disinformation and cyberattacks have forced NATO to also respond and adapt its communication strategies to counter these new challenges. Since 2014, the Alliance has introduced the largest collective defence reinforcement in a generation, with an increase in the number of high-readiness military forces and additional troops deployed to Allied territories.

While NATO unequivocally condemned Russia's aggression against Ukraine, the Alliance's initial reaction was relatively restrained. It primarily involved urging member states to aid Ukraine on a bilateral basis, considering NATO allies' responsibility to avoid direct conflict with a nuclear power (Dopovid Tsentru Razumkova, 2022). NATO and its Member states provide Ukraine with substantial financial assistance, assistance in equipping the Armed Forces of Ukraine with the necessary weapons, training and education of personnel, instructors, academic staff, and provide the necessary humanitarian aid.

Even though the formation and the establishment of relations between Ukraine and NATO began from the very beginning of Ukraine's independence in 1991, it was the aggressive and brutal actions of the Russian Federation in 2014 that necessitated the search for more effective mechanisms and guarantees of Ukraine's independence, sovereignty and territorial integrity. A key stage was the support by the Verkhovna Rada in December 2014 of the draft law on Ukraine's refusal of non-aligned status. Since then, cooperation has intensified significantly and taken on new forms. Since the beginning of the conflict in Ukraine, NATO's communications strategy has also evolved significantly. There is an obvious intensification of interconnections within the Alliance and increased cooperation and engagement between NATO and Ukraine, which is reflected in communications through an emphasis on military support, exercises, and consultations. This was a response to Russia's aggressive actions and a demonstration of international support for Ukraine. NATO's communications strategy has become more severe regarding Russia. NATO strongly condemned Russia's actions in Ukraine as a violation of international law. The Alliance's communication efforts were aimed at highlighting Russia's criminal actions and emphasizing the importance of international order and rules. (Joint press point with NATO Secretary General Jens Stoltenberg and the Prime Minister of Romania, Nicolae Ciucă, 2022).

The increasing utilization of hybrid warfare methods represents a perilous trend. Such threats are flexible, multi-actor, complex, and multi-subjective. At the same time, in combination with the means of information warfare and cyberwarfare, large-scale spread of disinformation, propaganda and fakes through global media, information and psychological operations, hybrid warfare methods achieve a high level of efficiency in achieving the goals of aggression, avoiding the large-scale use of conventional weapons (Kuchmii O., Frolova O, 2023). Hybrid wars are a new form of global confrontation in the modern international security system. Hybrid wars have gained particular significance since the beginning of Russia's open military aggression against Ukraine in February 2022, although they have been actively waged since 2014. Not only traditional media, but also social media have become a source of spreading Russian propaganda narratives, disinformation, and fakes.

NATO is actively utilizing online platforms, including social media, for providing operational information and engaging with the public. This involves the use of infographics, videos, and other visuals to present complex information in an accessible manner, as well as podcasts, webinars, and other multimedia formats to reach diverse audiences.

In the media space of NATO member states, attention was focused on Russian propaganda and disinformation, with the aim of warning and persuading the public to be cautious about information coming from Russian sources. Since the beginning of the Russian-Ukrainian war, many states have prohibited the broadcasting of the propaganda channel Russia Today on their territories. NATO is also actively working with international partners and the media to counter disinformation and propaganda. The Alliance urges that false stories be corrected or prevented from being broadcast or published. NATO has specialized teams monitoring disinformation and propaganda materials targeting the Alliance. The organization has mechanisms in place to promptly correct inaccurate information and provide accurate data. NATO is establishing cooperation with the media, providing journalists with reliable information and access to NATO experts to confirm facts. An important element of communication is the organization of trainings, seminars, and webinars to raise awareness of disinformation and how to detect and counter it.

Given that the party involved in the conflict, which predominantly implements the disinformation campaign, holds the initiative, NATO needs to act proactively, swiftly, and decisively to avert potentially devastating consequences. NATO has set up a website called "Setting the record straight" to counter and combat Russian fakes and disinformation. The website is a one-stop shop, a platform for documentaries, speeches, myth-busting videos, and photos, and is published in multiple languages, including Russian. Naturally, such measures cannot completely stop enemy destructive information influences, but they can identify propaganda and demonstrate it to the public. And crucially, by doing in this way, NATO is demonstrating that its own narrative is more accurate and truthful than that of its enemies. Countering disinformation can only be effective if it is supported by constant proactive communication. NATO's narrative must be known as much as the narratives of its adversary (Michael Rühle, Clare Roberts, 2021).

These elements of NATO's communications strategies help the Alliance to engage with the public, media, and other stakeholders in the face of the challenges posed by information warfare. And while the situation continues to develop, the basic principles and tools that NATO uses serve as an important means of ensuring clarity and transparency in complex circumstances.

The Russian-Ukrainian war made NATO revise its communication strategies regarding cybersecurity as a component of hybrid warfare. Apart from direct military threats and the threat of using "hard power," NATO has also identified cyberspace as an environment of information warfare, and cybersecurity has become an important area of its strategy. NATO advanced centres have been established in member states as multinational institutions to develop cybersecurity doctrine, implement theoretical developments in the practice of countering cyber threats, improve interstate cooperation and exchange of experience.

On May 16, 2023, the 15th anniversary of the NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Ukrainian flag was solemnly raised at the Centre’s headquarters in Tallinn, greeting Ukraine. For Ukraine, this is an opportunity to strengthen international cooperation in the field of cybersecurity and cyberdefence, deepen the exchange of experience, and participate in cyber defence exercises and training, as well as joint cybersecurity research. Ukraine's accession to NATO's Cooperative Cyber Defence Centre of Excellence will help to enhance the state's cyber resilience and effectively counteract aggression in cyberspace.

The strategic focus of NATO's activities is largely determined by the NATO Summits, where the Heads of State and Government of NATO Member states can meet and take joint coordinated decisions to address the current issues facing the Alliance. NATO summits are a highly efficient communication mechanism at the level of heads of state and government, meetings at the highest available level, where new policies are introduced, new significant initiatives are launched, new members are invited, and partnerships are strengthened (Warsaw Summit Communiqué, 2016).

In 2015, NATO foreign ministers adopted an updated strategy to counter hybrid threats. In July 2016, the NATO Summit reaffirmed NATO's defence mandate and recognized cyberspace as a field of military operations in which NATO must defend itself as efficiently as it does in the air, at

sea and on land. NATO has signed a Technical Arrangement on Cyber Defence with EU, including information sharing, personnel training, research, and exercises. According to NATO Secretary General J. Stoltenberg, the transatlantic cooperation organization supported the decision to strengthen cooperation between the EU and NATO, defined the dimensions of hybrid warfare and its threats to European security and drew attention to the crisis in Ukraine and further relations with Russia.

In 2017, NATO established the Joint Intelligence and Security Division, consisting of a specialized unit responsible for systematic analysis and monitoring of hybrid threats. This can be seen as a significant step forward in providing the Alliance's Allies with a comprehensive understanding of the situation. Recognizing that hybrid threats can have both internal and external aspects countries are increasingly focusing on sharing information about their internal developments.

To continue its policy of countering hybrid threats, in 2018 NATO leaders agreed to form Counter-Hybrid Support Teams to provide individualized, targeted assistance to Allies upon the request in preparing for and responding to hybrid activities. National cybersecurity units can be used to protect NATO member states during special operations. In 2019, NATO developed recommendations to strengthen the ability to effectively respond to cyberattacks, develop cooperation with the business environment in the development of cyber industry.

At the 2021 NATO Summit in Brussels, the Allies approved a Comprehensive Cyber Defence Policy that supports NATO's three primary tasks and its overall deterrence and defence posture. It reaffirmed the commitment to use the full range of capabilities to actively deter, defend against, and always counter the full range of cyber threats, including by considering a collective response. The response should be sustained and based on elements of NATO's full toolset, including political, diplomatic, and military instruments. The Allies also recognized that the impact of significant combined malicious cyber activity could, in certain circumstances, be considered an armed attack that could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty on a case-by-case basis (Brussels Summit, 2021).

The last NATO Summit was held in Vilnius on July 11-12, 2023. Support for Ukraine, which has been deterring Russia's large-scale aggression for 1.5 years, was a central theme of all discussions. NATO Allies agreed on a list of measures to bring Ukraine's membership in NATO closer. During Russia's illegal, unjustified, and aggressive war against Ukraine, NATO member states have strengthened the Alliance's deterrence and defence policy by adopting new regional plans to counter the two main threats to NATO's security, Russia and terrorism. NATO member states have pledged to spend at least 2% of their national gross domestic product on defence annually. Furthermore, an Action Plan was adopted to promote defence production, encourage investment, and increase production capacity. At the NATO Summit in 2023, Allies agreed on a new concept to strengthen the contribution of cyber defence to NATO's overall deterrence and defence posture. Additionally, they introduced the NATO Virtual Cyber Incident Support Capability to support national efforts to mitigate the consequences of criminal and dangerous cyber activities. The concept aims to better integrate NATO's three levels of cyber defence - political, military, and technical. Strengthening NATO's cyber resilience is one of the pillars of regional and international security. Ukraine was in the centre of attention of the summit participants, receiving another confirmation that the country will be able to become a NATO member when the conditions are completed. A long-term assistance program for Ukraine was approved, and the inaugural meeting of the NATO-Ukraine Council was held [9].

A significant consequence of the Russian-Ukrainian war for the transformation processes in NATO was its expansion and accession of new members. In April 2023, Finland became a new NATO member state. Sweden also applied for NATO membership in 2022. Sweden's membership is in the process of being approved, as all NATO member states have agreed on this decision, except for Turkey and Hungary.

Conclusion. NATO's communication strategies in the context of war demonstrate the alliance's adaptability and its ability to respond to dynamic changes in the geopolitical landscape. NATO constantly optimized its communication approaches throughout the conflict. NATO's communication strategies are quite restrained, measured, and cautious, aiming to avoid the escalation of the conflict with a party that possesses weapons of mass destruction. NATO emphasizes that it

provides only non-lethal aid to Ukraine. Lethal weapons are supplied to Kyiv only by the Member states of the Alliance, bilaterally or multilaterally.

Since the beginning of the conflict in Ukraine, NATO's communications strategy has undergone significant changes. The intensification of interconnections within the Alliance and the strengthening of cooperation and engagement between NATO and Ukraine are evident, reflected in communications through an emphasis on military support, exercises, and consultations. Equally important is information support for Ukraine, emphasizing its sovereignty and right to territorial integrity. Communications reaffirm NATO's position to reject aggressive actions and violations of international law. The main strength of the alliance is its ability to act collectively and coordinate communication among members. This has allowed NATO to act as a united front line, efficiently responding to threats and challenges that arose during the conflict.

In general, NATO's communication strategies have proven effective in the conflict, but need to be constantly adapted and modernized to face new information challenges. NATO should continue to invest in its communications efforts, developing the latest technologies and techniques to ensure that its messages are clear, transparent, and credible.

The Alliance is committed to a NATO-Ukraine partnership based on mutually beneficial cooperation and mutual reinforcement, shared values, and coordination and cooperation with other international alliances and organizations such as EU, UN, G7, OSCE and others.

The NATO Heads of State reaffirmed that Russia's war against Ukraine is a major challenge to the norms and values that have guaranteed the security and well-being of the European community. Russian aggression is a danger not only for Ukraine, but also for NATO Member states. NATO Allies have officially declared their intention to counter Russian aggression and help the government and people of Ukraine defend their independence and territorial integrity, since such actions are an integral part of countering threats and shaping the system of regional and international security

References

1. *The North Atlantic* (1949). The North Atlantic Treaty Washington D.C. - 4 April 1949 https://www.nato.int/cps/uk/natohq/official_texts_17120.htm?selectedLocale=en

2. *Makarenko Ye. et al.,* (2023). Міжнародна інформаційна безпека Підручник. [Mizhnarodna informatsiina bezpeka], Київ: ВАЕКС, 540 с.

3. Dopovid Tsentru Razumkova, (2022). Роль і місце України в перспективних європейській та євро-атлантичній системах безпеки. [Rol i mistse Ukrainy v perspektyvnykh yevropeiskii ta yevro-atlantychnii systemakh bezpeky.] Доповідь Центру Разумкова. Київ.

4. Joint press point with NATO Secretary General Jens Stoltenberg and the Prime Minister of Romania, Nicolae Ciucă, 2022, https://www.nato.int/cps/en/natohq/opinions_208592.htm.

5. *Kuchmii O., Frolova O.*, (2023). Використання соціальних медіа як інструменту сучасної гібридної війни [Vykorystannia sotsialnykh media yak instrumentu suchasnoi hibrydnoi viiny] «Acta de Historia & Politica: Saeculum XXI», Чорноморський національний університет імені Петра Могили, 2023 (спецвипуск), с.93-104 https://doi.org/10.26693/ahpsxxi2023.si.093

6. *Michael Rühle, Clare Roberts* (2021). Розширення інструментарію НАТО з протидії гібридним загрозам [Rozshyrennia instrumentariiu NATO z protydii hibrydnym zahrozam] https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennya-nstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html

7. *Warsaw Summit Communiqué*, (2016). Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. https://www.nato.int/cps/uk/natohq/official_texts_133169.htm?selectedLocale=en

8. *Brussels Summit,* (2021) On the Agenda Brussels Summit, 14 June 2021 https://www.nato.int/cps/uk/natohq/news_184633.htm

Samity NATO, (2024). https://www.nato.int/cps/uk/natolive/topics_50115.htm