Clío
Revista de Historia, Ciencias Humanas y Pensamiento Crítico
ISSN 2660-9037

Adscrita a:
Fundación Ediciones Clío
Academia de Historia del estado Zulia
Centro Zuliano de Investigaciones Genealógicas

Sección: **Artículo científico** | **2025**, julio-diciembre, año 5, No. 10, 2163-2191

Cooperation between the EU, NATO and the UN in addressing global security challenges: a critical analysis

Sergiy Lukin[1]
Correo: serge.lukin77@gmail.com
Orcid: https://orcid.org/0000-0001-6516-5605

Yevhenii Taran[2]
Correo: tarasiukyurii78@gmail.com
Orcid: https://orcid.org/0000-0002-1822-6978

Oleksander Tykhonenko[3]
Correo: Tikhonenko03@gmail.com
Orcid: https://orcid.org/0000-0002-5140-3737

DOI: https://doi.org/10.5281/zenodo.15659424

Abstract

The aim of the study is to analyse the cooperation of international organizations in shaping a global security strategy and countering modern threats. The research employed the following methods: graphical comparison, statistical and comparative analysis, and case study. The role of strategic documents and the role of international organizations in ensuring the security of member states is determined. The differences in resources between countries are identified, which emphasize the need for targeted capacity-building initiatives. Strategies for countering hybrid threats that combine conventional and unconventional tactics are investigated on the basis of 11 selected countries. The conclusion is made about the key role of international organizations in countering global security threats and the main focus of the UN, NATO and EU in performing their own

[1] Doctor of Science in Public Administration, Director, Associate Professor at the Regional Centre for Advanced Training in Kyiv Region, Kyiv, Ukraine
[2] PhD. in Political Science, Associate Professor of the the Global and National Security Department, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[3] PhD in Public Administration, Lecturer at the Regional Center for Advanced Training in Kyiv Region, Kyiv, Ukraine

Recibido: 2025-04-15 **Aceptado**: 2025-06-05

functions to ensure stability. Further efforts should focus on adaptive strategies and coherent policies to address the interconnected current security challenges.

Keywords: international cooperation, world order, global security, threats.

Cooperación entre la UE, la OTAN y la ONU para afrontar los retos de la seguridad mundial: Un análisis crítico

Resumen

El objetivo del estudio es analizar la cooperación de las organizaciones internacionales en la configuración de una estrategia de seguridad global y la lucha contra las amenazas modernas. La investigación emplea los siguientes métodos: comparación gráfica, análisis estadístico y comparativo, y estudio de casos. Se determina la función de los documentos estratégicos y el papel de las organizaciones internacionales a la hora de garantizar la seguridad de los Estados miembros. Se identifican las diferencias de recursos entre países, que ponen de relieve la necesidad de iniciativas específicas de capacitación. Las estrategias para contrarrestar las amenazas híbridas que combinan tácticas convencionales y no convencionales se investigan a partir de 11 países seleccionados. Se llega a la conclusión de que las organizaciones internacionales desempeñan un papel clave en la lucha contra las amenazas a la seguridad mundial y que la ONU, la OTAN y la UE se centran principalmente en el desempeño de sus propias funciones para garantizar la estabilidad. Los esfuerzos futuros deberían centrarse en estrategias adaptativas y políticas coherentes para hacer frente a los actuales retos de seguridad interconectados.

Palabras clave: cooperación internacional, orden mundial, seguridad global, amenazas.

Introduction

Security threats are becoming increasingly complex in the modern world, going beyond existing national borders and involving various groups of actors: from state-supported agencies to non-government organizations. This situation has accelerated changes in the implementation of global security measures, which are based on comprehensive strategic documents to address the problems of terrorism, cyber threats, economic instability, and environmental crises. In accordance with the identified threats, global international organizations, such as the United Nations (UN), the North Atlantic Treaty Organization (NATO) and the European Union (EU), and the Organization for Security and Co-operation in Europe (OSCE), together with regional alliances, perform key functions in coordinating security strategies.

Since the end of the World War II, a liberal order has taken shape in international relations, based on the principles of free trade, multilateral institutions, and the rule of law. The further fragmentation of the liberal order, marked by tensions between the United States and Russia and shifting alliances, complicates multilateral cooperation in the field of security. Revisionist regimes are on the rise, and strategic competition among leading powers is intensifying. Recent changes in U.S. policy, including the potential alignment with Russia under new leadership, may undermine coordination among NATO, the EU, and the UN, as evidenced by ongoing debates over burden-sharing.

As a result, the key mechanisms of collective security are losing their effectiveness, which necessitates a rethinking of the role of the UN, NATO, and the EU in the current context. Rapid technological progress and the strengthening of digital means have made cyber incidents a constant threat. Existing threats are directed at critical infrastructure, from power grids to financial systems, posing risks to economic stability and national security. The focus on cybersecurity as a key factor in global security strategies due to manifestations of cyberwarfare is a gradual adaptation of the activities of international organizations. It should be noted that the EU Cybersecurity Strategy for the Digital Decade focuses on building resilience against large-scale cyber incidents (European Commission, 2020, pp. 1-4). In addition, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) assists member states in strengthening cyber defence (Gargiulo et al., 2024, p. 8).

International organizations are feeling the consequences of traditional and hybrid forms of warfare, including terrorism, which has remained a significant threat for many decades. Terrorist groups take advantage of the weakness of the governance system and the instability of individual regions, which makes coordinated international measures the only means of counteraction. The ability to resolve conflicts and promote peacebuilding initiatives is another area of the role of international organizations in maintaining global security. Preventing the escalation of conflicts can be considered the key goal of peacekeeping activities. Overcoming challenges posed by international organizations requires adaptive and flexible policies to ensure rapid responses to unexpected threats and the integration of current security paradigms. This article examines the role of international organizations in addressing four key security challenges (cybersecurity, terrorism, hybrid threats, and peacekeeping), analyzing their strategies and coordination mechanisms for countering these evolving threats.

So, the aim of the research is to analyse the role of international organizations in shaping a global security strategy and countering current threats. This study examines the hypothesis that international organizations strengthen global security through coordinated strategies, and that the ability to adapt is crucial for countering evolving threats. So, the aim involves the fulfilment of the following research objectives: (1) assess the coordination mechanisms between international organizations and member states in shaping global security policy based on key alliances; (2) determine the impact of current strategies (cybersecurity initiatives, anti-terrorism activities, and peacekeeping operations); (3) to identify promising avenues for enhancing multilateral cooperation aimed at strengthening the operational responsiveness and strategic adaptability of international organizations in the security sphere.

1. Literature review

The escalation of geopolitical tensions in recent years has deepened the manifestations of advanced persistent threats (APTs), which are becoming increasingly complex and widespread (World Economic Forum, 2023, p. 6). This state of affairs requires changes in international approaches, which require strict implementation and contexts of perception, which extends to the activities of all international institutions.

Numerous international institutions can state that they have effective tools to guarantee a peaceful life for their member states. Some of the features on the global stage related to conflict resolution and prevention is the absence of war as a means in international relations. However, critical analysis reveals a significant gap between the declared objectives and the actual outcomes. None of them, except for inter-organizational relations, such as in NATO and the EU, has been successfully implemented, except for obtaining the statutory principles, goals and objectives that were the basis and justification for the creation of these organizations (Kruglashov, 2023). One can partially agree with this opinion, given the events of recent years related to Russian military aggression as a means of military-political pressure.

A major weakness of the existing studies is that they often fail to account for contextual factors influencing the effectiveness of international cooperation. The events of recent years, related to Russian military aggression, expose substantial deficiencies in the collective security system, which remain insufficiently explored in academic literature.

National cybersecurity strategies demonstrate the state policy of the country, which emphasizes the leadership role in implementing cybersecurity. International organizations and conditional alliances are, of course, the most important driving forces of this penetration process (Kostyuk & Sidorova, 2024). The above thesis is confirmed by examples of the implementation of cyber defence measures, which involves active national actions combined with global interaction. Cybersecurity is a key area in the ongoing discussion about security, which is determined by fast technologies and digital interconnection. The importance of a common approach to cybersecurity is emphasized by the fact that the European Union Cybersecurity Strategy for the Digital Decade will contribute to increasing cyber resilience at the level of Member States (European Commission, 2020, p. 20).

International institutions are key arenas for sharing threat information and developing common cybersecurity standards, which are essential for maintaining system reliability. The new phase of the transatlantic partnership, implemented through the Trade and Technology Council, aims to align standards on artificial intelligence, cybersecurity, and the export control of critical technologies (Christou et al., 2025). This initiative could strengthen a joint strategy for protecting the digital infrastructure of NATO and EU countries, while minimizing national disparities. However, critical analysis reveals a significant shortcoming: most studies fail to examine the gap between technical capabilities and the organizational capacity to implement cybersecurity measures.

Joint oversight and cooperation deter destructive actions, making the world a safer place. Global institutions facilitate the formulation and implementation of counterterrorism measures, creating conditions for cooperation and partnership between country delegates, as well as providing platforms for discussing methods and tactics (Suprunova et al., 2024). We agree with the above opinion with a view to the global nature of threats and the need to unite for strengthening the resilience of security functions both internationally and locally. NATO has expanded its counterterrorism strategies by adopting new technologies to improve threat assessment and verification, thereby increasing the ability to detect and mitigate terrorist threats in advance (NATO, 2024a). We consider this statement correct because of the critical importance of advanced technological expertise of international organizations in countering innovative actions by groups or individuals seeking to disrupt security. A notable strength of NATO's approach lies in the adoption of new technologies to enhance threat assessment. Nevertheless, the majority of studies overlook the adaptability of terrorist organizations to emerging counter-technologies.

In the risk ranking, the state involvement in large-scale military conflicts significantly increases the occurrence of instability over the next two years. As the emphasis on importance by key states is focused on a few areas, the spread of conflict is a serious concern. Numerous conflict zones are prone to intensifying crises in the near term as a result of the dangers of spreading or increasing state instability (World Economic Forum, 2024, p. 6).

The combination of cyberattacks, conventional warfare, disinformation and economic distortions in hybrid threats presents a multifaceted dilemma that increasingly requires a coordinated global response. Hybrid threats manifest themselves as multidimensional attacks aimed at existing vulnerabilities in the digital and socio-political spheres (Bargués & Bourekba, 2022). This view in the context of security is correct, based on an analysis of the current proliferation of digital tools in both the social aspect and the political sphere of activity. A comprehensive approach based on the rules, structures, measures and capabilities of NATO and the EU is implemented through the developed strategies for countering hybrid threats. These strategies focus on cybersecurity, strategic communication and military mobility (Jacuch, 2020). We fully agree that the common approaches defined by the strategic documents have defined the framework for security activities, forming a certain common vision for common actions. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) promotes cooperation between member states and shares its own experience in preventing hybrid attacks (Ratsiborynska, 2022). However, a critical shortcoming lies in the limited empirical data available for assessing the long-term impact of its activities.

Global security challenges retain despite the creation of platforms for addressing them by international organizations. National sovereignty remains a significant obstacle, as countries may refuse to hand over control or share sensitive information that could undermine their security models. The varying levels of funding and skills in countries at different economic levels can make global security arrangements unreliable (China Institutes of Contemporary International Relations., 2024). Moreover, the organizational architecture of parameters within entities, such as the power to block in the UN Security Council, can hinder a rapid and unified response to emerging threats. A particularly pressing issue is the organizational architecture, especially the authority to veto within the United Nations Security Council. Existing research provides insufficient analysis of alternative mechanisms for overcoming these structural constraints. A significant limitation of the current literature is the lack of a comprehensive evaluation of the effectiveness of different models of international security cooperation. Existing approaches in the scholarly literature require further investigation into the interaction of international organizations in shaping global security strategies.

2. Materials and methods

2.1. Research design

Using the theory of collective security, this study analyzes indices and strategies for assessing institutional effectiveness in addressing cybersecurity, terrorism, hybrid threats, and peacekeeping.The research design consists of the following main stages: (1) analysis of the Global Peace Index (2024), the Fragile States Index (2024), and cybersecurity indicators of individual countries to identify key security trends; (2) review of key UN and NATO counterterrorism initiatives; (3) comparative analysis of NATO and EU hybrid threat strategies based on institutionalism, assessing how shared norms enhance cooperation; (4) review of specific UN and OSCE peacekeeping and preventive diplomacy efforts. Each stage complements the other, providing a multifaceted approach to examining the effectiveness of international organizations in shaping security strategy.

2.2. Sampling

In general, 8 European countries were selected from the total number of countries that are members of international organizations (27 EU member states and 32 NATO member states). They were Estonia, Germany, France, Great Britain, Lithuania, Poland, Spain, and Greece. The countries included in the sample cover geographically different European regions. They have different military potential, level of economic development, and also differ in experience in implementing security policy, which affected the specifics of security challenges and the dynamics of changes in indicators. The specified features of the selected countries allow for a sufficiently multi-vector study of several aspects of the implementation of security within the EU and NATO. The study uses data from various sources to analyse the scope of international activity in the field of security. The following global reports were used: key security indices, including the Global Peace Index (2024), the Global Cybersecurity Index (2020; 2024), and the Fragile States Index (2024). They provided a framework for assessing the relative stability, cybersecurity resilience, and vulnerability of different countries. The indices offer quantitative data that allows for cross-country comparisons of security dynamics and the impact of collective efforts on global security.

The study reviewed strategic policy documents and resolutions of international institutions such as NATO, the UN, and the EU. In particular, these are the NATO Strategy on Countering Hybrid Warfare (NATO , 2024b) and the EU Strategy on Cybersecurity and Disinformation (European Commission, 2020, p. 25). They helped to identify current priorities and identified security implementation measures. The documents were used within the scope of the study, which identifies modern security threats (hybrid warfare, cyber threats, and terrorism) and countermeasures. Global indicators (stability assessment, cyber resilience and the level of terrorism) were examined for individual countries that are part of joint security structures (for example, NATO or EU member states). The use of different approaches contributed to understanding the role of international organizations in global security.

2.3. Methods

The study used a combined approach to determine the role of international organizations in shaping global security strategies. The method of graphical comparison was used to compare the stability of the studied countries in order to determine the overall effectiveness of measures aimed at improving the security system. Statistical and comparative analysis made it possible to establish the impact of international cooperation on the stability indicator of countries and to clarify the effectiveness of the strategies of international organizations. The case study method made it possible to identify successful/partially successful practices of peacekeeping missions and to identify the main challenges facing international organizations.

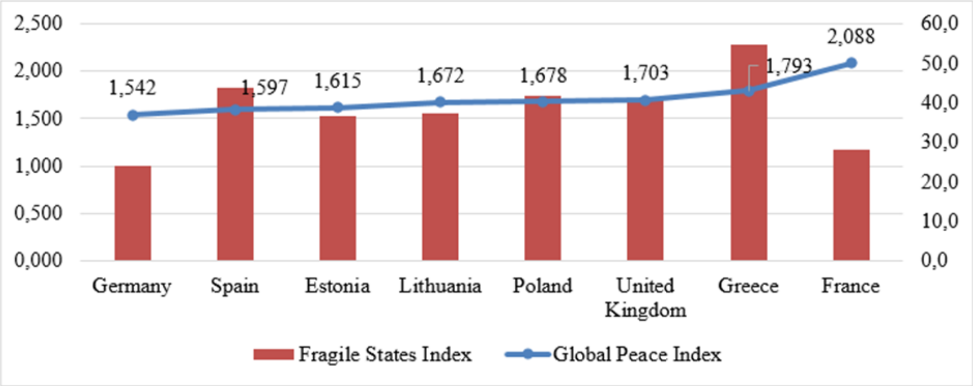
2.4. Instruments

Global indices (Global Peace Index, Fragile States Index, Global Cybersecurity Index), online platforms of international organizations (CCDCOE, Hybrid CoE, FATF), and strategic planning documents (EU Strategy on Cybersecurity and Disinformation, Strategy on Countering Hybrid Warfare) were used as tools.

3. Results

The results of the study demonstrate the definition by the international institutions (UN, NATO, EU) of their own approaches to global security. The results of quantitative analysis, the level of the Fragile States Index and the Global Peace Index, individual countries that are members of the EU and NATO, show fairly high stability indicators (Figure 1). Figure 1 shows high stability indicators for EU and NATO member states, indicating that coordinated strategies – such as NATO's cybersecurity initiatives and the harmonization of EU policies – contribute to improved security outcomes.

Figure 1. Global Peace Index and Fragile States Index



Source: developed by the authors based on data from Institute for Economics & Peace (2024, p. 2); The Fund for Peace (2024).

The EU and NATO have established different cybersecurity directions to protect member states from emerging cyber threats. The EU Cybersecurity Strategy for the Digital Decade and NATO’s CCDCOE initiatives are examples of how international organizations have promoted cyber resilience. Table 1 compares cybersecurity performance in individual EU and NATO countries, demonstrating the impact of joint cybersecurity structures. The higher cybersecurity indices in NATO/EU countries indicate a positive impact of joint programs, although other factors, such as national investments, may also contribute.

Table 1 illustrates the overall improvement in cyber defence performance among countries participating in EU or NATO cyber cooperation, demonstrating the positive impact of these joint cyber defence agencies. The data indicate that countries participating in EU and NATO cyber defence programmes have made significant progress, highlighting the contribution of dual ownership to strengthening defence. The results emphasize the benefits of a global partnership in digital defence, as partners can share assets, exchange intelligence, and apply common cyber standards.

Table 1. Cybersecurity performance of individual countries implementing cybersecurity measures

Country	Global Cybersecurity Index 2020	Global Cybersecurity Index 2024	Change (%)
Greece	93.98	97.11	+3.3
France	97.6	98.98	+1.41
Spain	98.52	99.74	+1.24
United Kingdom	99.54	100.0	+0.46
Poland	93.86	93.54	–0.34
Germany	97.41	93.84	–3.67
Estonia	99.48	95.04	–4.46
Lithuania	97.93	92.88	–5.16

Source: developed by the authors based on data from International Telecommunication Union (2021, p. 6; 2024, p. 1).

International organisations such as the UN and NATO play an important role in the fight against terrorism. The UN Counter-Terrorism Committee (CTC) strengthens political cooperation and intelligence sharing, while NATO's approach to counter-terrorism uses advanced technologies to proactively identify risks. Table 2 summarises the main UN and NATO counter-terrorism activities, outlining their objectives and key results.

Table 2. Overview of major UN and NATO counterterrorism initiatives

Organization	Measures	Objective	Key results
UN	Financial Action Task Force (FATF)	Blocking terrorist financing	Blocking financial assets involved in terrorist activities worldwide
UN	Counter-Terrorism Committee (CTC)	Shaping a common policy and exchanging information between member states	Developed standardized protocols for intelligence sharing between member states
NATO	Joint Counter-Terrorism Task Force	Improving operational coordination	Joint counter-terrorism exercises involving member states
NATO	Advanced Data Analysis Programmes	Using artificial intelligence (AI) and data analytics to detect threats	Increased number of potential threats identified in NATO countries

Source: developed by the authors based on data from United Nations Security Council Counter-Terrorism Committee (2024, p. 7); Financial Action Task Force (2023, p. 10); Lucarelli et al. (2021); NATO (2024c).

Table 2 shows the importance of global combined efforts to combat terrorism. NATO is using AI to rapidly understand potential threats. At the same time, the UN's global response has strengthened its capacity to disrupt the financial support of violent groups by standardizing fiscal rules and procedures. Global institutions are thus effectively addressing the various aspects of terrorism. The UN focuses on political and legal measures, while NATO prioritizes technical and tactical elements.

Hybrid threats, characterized by the combination of regular and irregular methods such as digital attacks, deception, and economic influence, have emerged as a major challenge to global security. Both NATO and the EU have implemented targeted plans to address hybrid challenges, including the NATO Strategy on Hybrid Threats and the establishment of the EU's European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Table 3 compares key elements of NATO and EU strategies to counter hybrid threats, focusing on their objectives and methods.

Table 3. Comparison of NATO and EU strategies to counter hybrid threats

Institution	Strategic document	Goals	Methods
NATO	Hybrid Warfare Resilience Programme	Strengthening national resilience	Military exercises, joint cyber operations, crisis management simulations
NATO	Counter Hybrid Threat Strategy	Preventing, detecting and responding to hybrid threats	Intelligence sharing, rapid response teams, information activities
EU	EU Cybersecurity and Disinformation Strategy	Countering disinformation and cyberattacks	Legal reforms, cybersecurity protocols, cooperation with the private sector
EU	Council of Europe Hybrid Initiative	Increasing resilience to hybrid threats	Training and capacity-building programmes, policy recommendations, research and analysis

Source: developed by the authors based on data from NATO (2024b); Lasoen (2022, p. 10); Jungwirth et al. (2023); European Commission (2020).

Table 3 highlights NATO's emphasis on rapid response (enhanced intelligence sharing) and the EU's focus on resilience (public awareness campaigns), which together form a solid foundation for countering hybrid threats (e.g., reducing the impact of disinformation). The results suggest that a harmonized approach that combines NATO's rapid response capabilities with EU resilience strategies is particularly powerful in countering hybrid threats. Uneven improvement in cyber resilience among resource-constrained countries (such as Lithuania and Estonia) indicates a gap in technical capabilities and funding. This highlights the need for targeted support to less developed states and the establishment of mechanisms for redistributing technological resources within the NATO–EU framework.

The UN and the OSCE primarily help to maintain peace in regions seized by ongoing wars. Peacekeeping missions contribute to stabilization in dangerous regions where people may be fighting, help governments to function properly, and ensure the safety of the people who live there. The OSCE aims to reduce tensions before they arise and to monitor any political problems in countries in eastern Europe. Table 4 provides some information on the peacekeeping and preventive diplomacy implemented by the UN and the OSCE.

Table 4 illustrates that efforts by the UN and OSCE, such as the protection of civilians by UNMISS in South Sudan, demonstrate significant capability, but the challenges in Mali highlight limitations due to resource constraints and political complexities. For instance, UNMISS reduced the number of civilian casualties, while MINUSMA faced higher rates of attacks. The OSCE role in Kosovo emphasizes the need for preventive mediation, despite protracted disputes such as those in Ukraine. This emphasizes the limitations of negotiations in the face of active warfare. The EU-NATO partnership has improved the state of cybersecurity. It is easier to stop cyberattacks in case of cooperation of countries, where they share critical data and respond quickly to threats. The UN and NATO have made significant progress in the fight against terrorism, although through different methods. The UN's emphasis on policy coordination and funding freezes complements NATO's technological approach to identifying risks and preparing for action.

Table 4. Summary of UN and OSCE peacekeeping and preventive diplomacy efforts

Organization	Mission/Operation	Region	Objectives	Results
OSCE	United Nations Interim Administration Mission in Kosovo, UNMIK	Kosovo	Political stabilization, protection of human rights	Maintaining political stability, supporting judicial reforms and protecting human rights
UN	United Nations Multidimensional Integrated Stabilization Mission in Mali, MINUSMA	Mali	Regional stabilization, fight against terrorism	Protecting regions, challenging high levels of resistance
UN	United Nations Mission in South Sudan, UNMISS	South Sudan	Maintaining the peace process, protection of civilians	Reducing civilian casualties, supporting the formation of a transitional government

Source: developed by the authors based on data from Day et al. (2019); Boutellis (2024); Organization for Security and Co-operation in Europe (2024).

NATO's prompt countermeasures and EU resilience programmes help to counter hybrid threats. The EU's emphasis on public awareness and policy review, together with NATO's armed readiness, provide a comprehensive strategy to counter complex multi-aspect threats. The combined efforts of the UN and OSCE in maintaining peace in conflict zones demonstrate both the capacity and limitations of global organizations in ensuring the security of individual territories.

In general, the findings show that international organizations are crucial to security worldwide, although their success depends on the specific threat and geographical location. Keeping security in the world requires quick actions in the face of threats, developing common policies, using new technologies, and building resilience. Proposed actions should aim to strengthen interactions between economic actors, expand cooperation between the public and private sectors (Kruhlov et al., 2019), and increase regulatory flexibility to better respond to threats.

4. Discussion

Positive indicators of cybersecurity development of countries participating in NATO and EU initiatives indicate the advantages of jointly created cybersecurity agencies. The research results confirm that coordinated strategies, such as cooperation between NATO and the EU in the field of cybersecurity (Table 1), improve security outcomes, while adaptability, as seen in the evolution of UN counterterrorism measures (Table 2), remains important. Our results are consistent with Radanliev (2024), whose analysis of CCDCOE protocols emphasizes improved threat detection based on the large volume of data from member states.

The results of the study, based on Table 2, indicate progress in the fight against terrorism through UN financial regulations and NATO's technological advancements, although success depends on the region and requires continuous evaluation. This result is supported by the study on the fight against terrorist financing. In global financial networks, the UN and the Financial Action Task Force (FATF) have implemented standardized measures to combat money laundering and terrorist financing (Gaviyau & Sibindi, 2023). Similarly, in other research on the application of new technologies in NATO operations, such as the AI use for threat detection (Araya & King, 2022). This coincides with the findings of our study on the development of technology that enables very rapid detection of new threats, thereby expanding the tactical capabilities of its member states.

The study of Kalniete and Pildegovičs (2021) confirms the results of our study, namely: the appropriateness of a common and unified approach to countering hybrid threats and disinformation. It focuses on the need for EU leadership in the security system with a view to institutional and regulatory factors. The main conclusions of this study are confirmed in the study of Gheciu and Von Hlatky (2024), which notes the importance of NATO's resilience to external threats. Despite certain difficulties in international unification, collective security is focused on dynamic threats, which include military, hybrid or terrorist threats. The article of Usewicz and Keplin (2023), which emphasizes the need to coordinate security aspects in both NATO and the EU, also confirms the key theses of the study. This should involve expanding cooperation between the two international organizations and between member states with the purpose of countering hybrid threats by the EU and NATO.

Our research shows that the approaches to managing hybrid threats used by NATO and EU provide a comprehensive response. NATO focuses on rapid response and troop readiness, while the EU enhances resilience through public information and legal reform. Our approach is consistent with the findings of

Bajarūnas (2020), who views hybrid threats as complex and evolving challenges that require a coordinated response that includes both defensive resilience and proactive measures.

At the same time, some studies suggest a different view on the application of existing improvements than those presented in our study. Despite all their achievements, the EU and NATO cannot fully realize their goal of more resilient cybersecurity. This is explained by the fact that there are gaps in the resources and technical knowledge of their member states that hinder this process. States with a lower level of cyber infrastructure face protocols imposed by the aforementioned organizations, noting the need to further support and strengthen cybersecurity capabilities in all member states (International Telecommunication Union, 2024, p. 1). On the other hand, some analysts (Moncrieff et al., 2024) disagree with the views stated in the presented work. They argue that NATO's reliance on technology-focused counterterrorism strategies may weaken local intelligence gathering efforts, which are important for understanding the specifics of regional dynamics in terrorist organizations.

Several implications of the study are crucial for policy-making within international organizations. The differences in the resource base of member states emphasize the need for more targeted capacity-building initiatives to support countries with lower levels of technical infrastructure. Therefore, technical support and increased funding for these countries should be a priority. At the same time, NATO's latest approaches to threat identification will accelerate their work, and the integration of local intelligence sources will ensure more accurate processing of the context.

Hybrid threats remain unpredictable, so there is a need to shape security strategies based on adaptive approaches. Standardized protocols may, in turn, fail to respond to the changing hybrid threats, which often benefit from specific local vulnerabilities. Therefore, international organizations must adopt response strategies that are more flexible to vulnerabilities and can dynamically adapt to the rapid changes in hybrid attacks.

Russia’s growing activity within the Eurasian context is creating an alternative network that often competes with liberal institutions. Russia employs specific structures to undermine NATO’s influence along the eastern borders of the European Union, while simultaneously expanding its sphere of political and economic dominance. Analyzing these processes offers deeper insight into the challenges facing global institutions.

The study aimed to determine the role of international organizations in creating global security plans and countering modern challenges. In general, the obtained results are consistent with the set goals: the importance of global institutions in strengthening joint efforts in the field of security is proven, the advantages and disadvantages of current approaches are recognized, and the main directions for further expansion of cooperation are identified. The obtained results can be applied in the development of global security strategies and improving cooperation mechanisms of international organizations. They can also be used to implement approaches to the development of standards in the field of security and cybersecurity, as well as in the process of training specialists who perform relevant functions.

4.1. Limitations

Despite the significant amount of analysed data, there are still some limitations. Significant differences in the availability of information between countries lead to differences in the methods of comparison (for example, the Global Peace Index or the Fragile States Index). The scope and detail of the analysis are determined by the lack of available data, in particular on secret military tactics or publicized intelligence agreements. Besides, the assessment does not take into account political differences of different countries, which can potentially affect the application of uniform approaches. This issue reduces the likelihood that the obtained results will be applied universally and will be effective for shaping public policy in areas related to ensuring security.

4.2. Recommendations

The obtained results give grounds to provide some recommendations. It is appropriate to increase the level of interaction between the UN, the EU and NATO on the basis of joint programmes and activities (harmonization of strategic documents, unified communication platforms). Given the existing disparities in cybersecurity progress, it is recommended to provide technical support for less developed countries (expert, technical, financial assistance). Given the need for additional resources, it is necessary to develop innovative forms of interaction based on public-private partnership models and the use of artificial intelligence for threat detection. Further development of information exchange mechanisms and increased transparency in the field of security standards also remains an important factor.

The United Nations Security Council should establish a mechanism for the temporary suspension of the veto power in cases of critical cyber incidents, in order to ensure swift and effective responses. Within the European Commission, it is necessary to expand the mandate of the Trade and Technology Council to include the protection of critical resource supply chains. NATO should initiate a program to guarantee the rapid exchange of intelligence data.

Conclusion

Unprecedented security challenges focused on digital threats, terrorist acts, and hybrid threats require a multi-aspect strategy for addressing them. In threat scenarios, international organizations (NATO, EU and UN) become key actors in promoting and implementing unified defence strategies. Their role is to help states to cooperate, coordinate policies, and strengthen defence against modern threats. Although the EU and NATO strategies are focused on Europe, the EU-NATO strategies align with the efforts of the UN in Africa (peacekeeping activities in Mali). A broader application to Asia or the Middle East requires further examination. A significant problem with existing approaches is the uncritical perception of international organizations as "key players." Although NATO, the EU, and the UN are indeed involved in shaping security strategies, the available data on their actual effectiveness remains controversial. The main results of the study are the following:

1. Coordination between international actors implies that NATO focuses on technological solutions (artificial intelligence, cybersecurity). The EU ensures policy harmonization and increases resilience, while the UN implements peacekeeping initiatives and the fight against terrorism. The mentioned actions

have demonstrated high effectiveness in the fields of cybersecurity and countering hybrid threats, but only under the conditions of fair resource allocation and the provision of technical assistance.

2. The increasing level of digitalisation has made cyber threats a global issue. The EU Cybersecurity Strategy for the Digital Decade and NATO initiatives demonstrate a positive impact on the resilience of Member States, but resource disparities between countries pose challenges.

3. International organisations are demonstrating progress in the fight against terrorism and cyber threats. This includes UN efforts to standardise procedures and block the financing of terrorist networks, ensuring NATO's operational readiness and introducing modern technologies to identify threats. At the same time, the EU is focusing on strengthening resilience and regulatory reforms.

4. Inadequate resources and national sovereignty limit the effectiveness of international cooperation. Further approaches to security should include the adaptability of policy frameworks, the use of public-private partnerships, and the integration of lessons learned into global strategies.

5. The EU Cybersecurity Strategy and NATO initiatives correlate with improving resilience in member states, but it is necessary to separate their impact from factors such as national policies or informational campaigns.

A general assessment of the available data reveals a significant gap between ambitious theoretical constructs and empirical realities. While international organizations indeed play a role in shaping the security discourse, their practical effectiveness remains questionable. Without a critical reconsideration of the foundational assumptions regarding the nature of international security cooperation, further research risks remaining within the boundaries of normative aspirations rather than achieving an analytical understanding of actual processes. The obtained results can be used in the development of global security strategies and the improvement of the system of interaction of international organizations. They can also contribute to the implementation of approaches to the creation of security and cybersecurity standards, as well as training specialists who perform relevant functions. In general, an integrative approach to global security is required, which includes regulatory harmonization, technological development, and cooperation between states. Further research can be aimed at analysing the mechanisms of response to hybrid threats.

References

Araya, D., & King, M. (2022). The impact of artificial intelligence on military defence and security. *CIGI Papers, 263,* 1–19. https://www.cigionline.org/static/documents/no.263.pdf

Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View, 19*(1), 62–70. https://doi.org/10.1177/1781685820912041

Bargués, P., & Bourekba, M. (2022). War by all means: The rise of hybrid warfare. In: Bargués, P., Moussa, B., & Colomina, C. (eds.), *Hybrid threats, a vulnerable order: CIDOB report* (pp. 9-13). Barcelona: CIDOB. https://shre.ink/eTNw

Boutellis, A. (2024). *The UN stabilization mission in Mali (MINUSMA), twenty-first century perspectives on war, peace, and human conflict*. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-66466-3

China Institutes of Contemporary International Relations (CICIR). (2024). *Global strategic and security risks*. https://shre.ink/eTEr

Christou, G., Meyer, T., & Fanni, R. (2025). The European Union: Assessing global leadership through actorness in artificial intelligence. *Journal of European Integration 47*(3), 383-401. https://doi.org/10.1080/07036337.2024.2377200

Day, A., Hunt, Ch. T., Yin, H., & Kumalo, L. (2019). *Assessing the effectiveness of the UN mission in South Sudan (UNMISS): EPON report (no. 2).* Norwegian Institute of International Affairs. https://collections.unu.edu/eserv/UNU:7595/EPON-UNMISS-Report-LOWRES.pdf

European Commission. (December 14, 2020). *The EU's cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Financial Action Task Force (FATF). (2023). *International standards on combating money laundering and the financing of terrorism & proliferation*. https://shre.ink/eTEe

Gargiulo, P., Giovannelli, D., & Sciacovelli, A. L. (eds.). (2024). *Cybersecurity governance and normative frameworks: Non-Western countries and international organizations perspectives.* Napoli: Editoriale Scientifica. https://goo.su/XRAfimv

Gaviyau, W., & Sibindi, A. B. (2023). Global anti-money laundering and combating terrorism financing regulatory framework: A critique. *Journal of Risk and Financial Management, 16*(7), 313. https://doi.org/10.3390/jrfm16070313

Gheciu, A., & von Hlatky, S. (2024). Irreconcilable differences? NATO's response to Russian aggression against Ukraine. *International Journal Canada S Journal of Global Policy Analysis, 79*(2), 275–96. https://doi.org/10.1177/00207020241255999

Institute for Economics & Peace. (2024). *Global Peace Index 2024: Measuring peace in a complex world*. https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf

International Telecommunication Union (ITU). (2021). *Global Cybersecurity Index 2020*. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024*, 5th ed. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Jacuch, A. (2020). Countering hybrid threats: Resilience in the EU and NATO's strategies. *The Copernicus Journal of Political Studies*, *1*, 5–26. https://doi.org/10.12775/cjps.2020.001

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., & Giannopoulos, G. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. Luxembourg: Publications Office of the European Union. https://doi.org/10.2760/37899

Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. *European View*, *20*(1), 23–33. https://doi.org/10.1177/17816858211004648

Kostyuk, N., & Sidorova, J. (2024). *Role of international organizations and formal alliances in the global diffusion of national cybersecurity strategies*. https://weis.utdallas.edu/files/2024/04/Kostyuk-Sidorova-WEIS-2024-9356574e1f44fb9b.pdf

Kruglashov, A. (2023). The reaction of international organizations to global security challenges. In: *Global public goods and sustainable development in the practice of international organizations* (chapter 3, pp. 59–84). Leiden: Brill. https://doi.org/10.1163/9789004687264_005

Kruhlov, V., Latynin, M., Horban, A., & Petrov, A. (2019). Public-private partnership in cybersecurity. *Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019), 2654*, paper 48. https://ceur-ws.org/Vol-2654/paper48.pdf

Lasoen, K. (2022). *Realising the EU hybrid toolbox: Opportunities and pitfalls: Clingendael policy brief.* Clingendael Institute (Netherlands Institute of International Relations). https://goo.su/mhy2

Lucarelli, S., Marrone, A., & Moro, F. N. (eds.). (2021). *NATO decision-making in the age of big data and artificial intelligence.* Brussels: University of Bologna and Istituto Affari Internazionali (IAI) of Rome. https://www.act.nato.int/wp-content/uploads/2024/07/20210301_AC-2020_Final-Report.pdf

Moncrieff, M., Kilibarda, P., & Gaggioli, G. (2024). Social network analysis and counterterrorism: A double-edged sword for international humanitarian law. *Journal of Conflict and Security Law, 29*(1), 165–83. https://doi.org/10.1093/jcsl/krae002

NATO. (Jule 25, 2024a). *Countering terrorism*. Retrieved December 20, 2024, https://www.nato.int/cps/uk/natohq/topics_77646.htm?selectedLocale=en

NATO. (Jule 25, 2024c). *NATO's policy guidelines on counter*-*terrorism. Aware, capable and engaged for a safer future.* https://www.nato.int/cps/en/natohq/official_texts_228154.htm

NATO. (May 07, 2024b). *Countering hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm

Organization for Security and Co-operation in Europe (OSCE). (2024). *25 years together*. *OSCE Mission in Kosovo.* https://goo.su/V26m8W

Radanliev, P. (2024). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, ioT, blockchains, and quantum computing. *Journal of Cyber Security Technology*, *9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671

Ratsiborynska, V. (2022). EU-NATO and the Eastern partnership countries against hybrid threats (2016–2021). *National Security and the Future, 23*(2), 89–121. https://doi.org/10.37458/nstf.23.2.3

Suprunova, I., Kovalchuk, V., Lytvynchuk, O., Levchenko, I., & Lysak, K. (2024). International organizations and their role in combating terrorism and terrorist financing. *Economic Affairs*, *69*(Special Issue), 179‒186. https://doi.org/10.46852/0424-2513.1.2024.20

The Fund for Peace. (2024). *Fragile States Index 2024 [Data set]*. https://fragilestatesindex.org/global-data/

United Nations Security Council Counter-Terrorism Committee (CTED). (2024). *Evolving trends in the financing of foreign terrorist fighters' activity, 2014–2024*. https://goo.su/xgXAU

Usewicz, T., & Keplin, J. (2023). Hybrid actions and their effect on EU maritime security. *Journal on Baltic Security, 9*(1), 32–68. https://doi.org/10.57767/jobs_2023_001

World Economic Forum. (2023). *The global risks report 2023, 18th ed.* https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Conflict of interest and originality declaration

As stipulated in the *Code of Ethics and Best Practices* published in *Clío Journal*, the authors, *Sergiy Lukin; Yevhenii Taran and Oleksandr Tykhonenko* declare that they have no real, potential or evident conflicts of interest, of an academic, financial, intellectual or intellectual property nature, related to the content of the article: *Cooperation between the EU, NATO and the UN in addressing global security challenges: a critical analysis*, in relation to its publication. Likewise, they declare that the work is original, has not been published partially or totally in another medium of dissemination, no ideas, formulations, citations or illustrations were used, extracted from different sources, without clearly and strictly mentioning their origin and without being duly referenced in the corresponding bibliography. They consent to the Editorial Board applying any plagiarism detection system to verify their originality.