ISSN 2415–881X Politology Bulletin, Issue 100, №2 (2026)
UDC 327.7 + 341.215.2 DOI 10.17721/2415-881X.2026.100.2.334–344

Anna Taranenko
Candidate of Political Science (PhD),
Associate Professor Department of International Relations
National University of "Kyiv-Mohyla Academy" (Kyiv, Ukraine)
https://orcid.org/0000-0003-2588-4941
e-mail: taranenkoann@yahoo.com

INFORMATION RESILIENCE IN UKRAINE AND THE BALTIC SEA REGION

Abstract

The article provides a comprehensive analysis of contemporary challenges to information security in Ukraine and the Baltic Sea region in the context of hybrid confrontation. It substantiates that information security has transformed into an independent strategic component of national and international security, while information influence has become an important instrument for destabilizing democratic societies. The study identifies the main forms of contemporary information threats, including disinformation, manipulative narratives, fake news, and technologies of information influence aimed at undermining public trust and intensifying political polarization.

The peculiarities of the Russian Federation's use of information and psychological operations against Ukraine and the Baltic region states are analyzed. The article reveals the specific features of Russian disinformation narratives targeting Ukraine, Latvia, Lithuania, Estonia, and Sweden, and outlines the key socio-political vulnerabilities exploited for destabilizing influence. It is demonstrated that a common feature of such information attacks is their focus on historical traumas, linguistic and cultural contradictions, and crises of public trust.

Special attention is paid to the concept of information resilience as a fundamental mechanism for countering hybrid threats. It is emphasized that the development of information resilience involves not only the state's ability to respond to information attacks, but also the formation of long-term mechanisms for protecting the democratic information space. The necessity of a multi-level approach to ensuring information security is substantiated,

encompassing cooperation among state institutions, security structures, civil society, educational programs, and strategic communications centers.

The article concludes that effective counteraction to contemporary information threats requires regional coordination, strengthened international cooperation, and the establishment of a common system of information resilience for Ukraine and the Baltic Sea states in the context of growing hybrid challenges

Keywords: information resilience; Ukraine; Baltic Sea Region; information threats; hybrid threats; disinformation; fake news; propaganda

Introduction

The notion of information security as a crucial dimension of national and international security has become especially salient lately due to numerous information threats to democracies worldwide, including disinformation, obscurantism and fake news. In the post-Cold War period nations enjoyed an unprecedented luxury of not expecting, at least in the near future, the menace of a large-scale war between the great powers of international politics [1, p.15]. Yet, at the present moment, it is increasingly more difficult to draw a precise line between war and peace in conflicts of the globalizing world in view of hybrid warfare usage and to clearly understand who an adversary is and what their goals might be.

Information threats are often utilized as a part of hybrid warfare. Thereby, disinformation can be defined, as false information that is intentionally meant to mislead audiences — intentionally misstating the facts to baffle and confuse [2, p.1]. One can single out, particularly, three distinct factors or motivators: to make money; to gain political influence, either foreign or domestic; or to cause trouble and harm for the sake of it [3, p.1].

Information threats are frequently categorized as part of hybrid warfare aimed at creating uncertainty, blur the line between conflicting parties and thus confuse an adversary. Hybrid warfare can be defined as warfare that includes a multiplicity of actors, blurs the traditional divide between sorts of armed conflict, and even between the notions of war and peace [4, p.7]. In recent years, the Russian Federation has been notorious in terms of involvement in a series of hybrid operation and disinformation spreading campaigns worldwide. Thereby, although hybrid warfare is a Western, not Russian term, all kinds of recent Russian hostile activities — from the covert use of special forces to interference in elections and economic coercion — have been defined as hybrid and caused growing disturbance in the Western security sector [4, p.7].

It should be noted that these hybrid threats stemming from authoritarian regimes, including the Russian Federation, have been of particular concern lately for the countries of the wider Baltic Sea Region, including Ukraine. Therefore, it is necessary to determine key characteristics of information resilience in Ukraine

and the wider Baltic Sea Region in view of the current threat of spreading fake news and obscurantism, particularly stemming from authoritarian regimes.

The problem of this research study is the need to define characteristics of information resilience in Ukraine and the wider Baltic Sea Region in view of the current threat of spreading fake news and obscurantism. The goal of this research study is to define key characteristics of information resilience in Ukraine and the wider Baltic Sea Region in view of the current threat of spreading fake news and obscurantism.

The topics of hybrid threats, information security and information resilience have become particularly salient in recent years. Thereby hybrid threats are frequently characterized as anything happening in non-conventional wars, for instance, Russia-Chechnya wars, actions of ISIS, confrontation in Afghanistan [5, p.124]. Aggressor states have been using a wide range of hybrid techniques in order to reach their foreign policy goals.

There are various approaches to the term of "hybrid warfare". The term "hybrid warfare" was used to simply describe the concurrent use of conventional and irregular forces in the same military campaign — for instance, Peter R. Mansoor characterized hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, terrorists, among others), which could include both state and nonstate actors, aimed at achieving a common political purpose [6, p.7].

Democracy has a unique relation to the notions of hybrid warfare and information threats. It should be noted that when the founders of the United Nations drafted the United Nations Charter 80 years ago, they did not include the word "democracy", because in 1945, still more than today, many of the United Nations' Member States did not espouse democracy as a system — others laid claim to it, but did not practise it [7, p.1.]. Yet, the United Nations as an institution has done a lot to support democracy around the world — from fostering good governance to monitoring elections, from supporting civil society to strengthening democratic institutions, to assisting the drafting of new constitutions in nations post-conflict [7, p.1].

Another important term to analyze is the notion of resilience. Resilience refers to the ability to successfully adapt to stressors, maintaining psychological well-being in the face of adversity [8, p.1]. It is the ability to "bounce back" from difficult experiences, and it involves thoughts and actions that can be further learned and fine-tuned [8, p.1].

A wide range of tactics was elaborated and employed by democratic states, in particular, to withstand information threats. An important notion connected with this process is information resilience. Information resilience

can be defined as the process of reducing vulnerability of information to threats during its lifespan [9, p.1].

Developing and enhancing information resilience is especially urgent for Ukraine in view of the ongoing Russia-Ukraine war, and for the wider Baltic Sea Region, many of whose countries border on the Russian Federation and become the target of numerous disinformation threats and attacks. Among common myths spread by the Russian Federation about Ukraine, in particular, is that Ukraine is a failed state and not a democracy [10, p. 2]. It can be concluded that the above-mentioned terms and concepts are highly important for further approaching the topic of information resilience to current hybrid threats in Ukraine and the wider Baltic Sea Region countries.

Methods of Research

It is planned to utilize qualitative methodology in the research study. In particular, the selected method is qualitative case study. Researchers using qualitative methodology immerse themselves in a culture by observing its people and their interactions, often participating in activities, taking life histories, constructing case studies, and analyzing existing documents or other artefacts [11, p.1433]. The qualitative researcher's goal is to attain an insider's view of the group under study, which makes qualitative research methodology a bit different from the quantitative research methodology with respect to the type of qualitative research, the research design, sample size, instruments and methods of data collection and analysis [11, p.1433].

The research question of the present research study is, as follows, RQ. What are the key characteristics of information resilience in Ukraine and the wider Baltic Sea Region in view of the current threat of spreading fake news and obscurantism?

Results of Research

Since Ukraine and the wider Baltic Sea Region are in the focus of this research, it is also important to define the Baltic Sea Region and Ukraine's place in it for the present research study. It should be noted that the wider Baltic Sea Region includes Ukraine in its boundaries. One should note that there is a multitude of approaches to defining the Baltic Sea Region in view of various geographical, political, social, economic, linguistic and cultural factors. The region can be defined within wider or narrower terms. Moraczewska [12, p.16] notes that a region can be defined as a geographical area with its specific natural features, the appearance of shared norms and rules which are considered by a group of entities as well as a common initiative implemented by countries at local or central levels in planning policy, economy, social and cultural issues, and while dealing with a maritime region it is often the sea that becomes the most important factor stimulating the region-building processes. According to

the Baltic Development Forum (2018) approach, the Baltic Sea Region consists of eleven nations [13, p.1]. Per European Union Strategy for the Baltic Sea Region (EUSBSR), it includes 12 countries [14, p.1]. Rydén [15, p.10] notes that the Baltic Sea drainage basin includes wholly or partly the territory of fourteen countries, including Ukraine. The Baltic Sea drainage basin includes the territory of fourteen countries in total with some 85 million inhabitants — in addition to the nine coastal states — Sweden, Finland, Latvia, Lithuania, Poland, Germany, Denmark, Estonia and Russia — one can also find Belarus and smaller parts from Ukraine, Czech and Slovak republics draining through Poland in the south, and very small parts of Norway draining through Sweden in the west [15, p.10]. The author of the present research study will follow this wider and more inclusive definition of the Baltic Sea Region, with fourteen countries, including Ukraine.

In terms of threats to information security, the Russian Federation has long been one of the most serious antagonists for the wider Baltic Sea Region, including Ukraine. Concept of the Russian Foreign Policy (2023) contains such provisions, as "strategic foreign policy goals of the Russian Federation are achieved through performing the following main tasks… — develop ties with compatriots living abroad and render them full support in exercising their rights, ensuring protection of their interests and preserving all-Russian cultural identity [16, p. 9]. Thereby, one should also note the so-called new "securitization" of Europe — return to previously rejected realist concept of great powers in international relations, particularly after annexation of the Crimea [17, p.127].

In utilizing hybrid warfare, the Russian Federation continues to search, identify and exploit vulnerabilities of other states, particularly, of democratic states. For example, among vulnerabilities of Germany exploited by the Russian Federation were, in particular, the issues of migrants [17, p.130]. Among vulnerabilities of Sweden exploited by the Russian Federation was the case of the former Ministry of Defense Mr. Peter Hultqvist, a well-known critic of the Russian Federation, who was blamed for writing letters on providing weapons to Ukraine [17, p.130].

The Russian Federation has also been exploiting vulnerabilities of the Baltic Sea region states — former republics of the Soviet Union — Latvia, Lithuania and Estonia. Particularly, in Latvia, among the exploited vulnerabilities, there were such aspects, as "oppressing" linguistic rights of Russian-language speakers in Latvia and limiting rights of "non-citizens" [17, p.144]. As to Ukraine, the goal of the Russian Federation with regard to international audiences was to discredit the Ukrainian government and diminish the support provided to Ukraine by democratic allies [18, p.2]. Thus, it can be concluded that countries of the wider Baltic Sea Region, including Ukraine, have long been targets of Russian disinformation and propaganda, and have continued efforts on withstanding these threats and further developing their information resilience.

Fighting hybrid threats, disinformation and developing information resilience further continues in the wider Baltic Sea Region, including Ukraine. Regarding the Ukrainian case, in the opinion of E. Channell-Justice, phenomenon of self-organization is key: when a certain step needs to be taken, and people have the appropriate capabilities in Ukraine, they just go ahead and do it [19, p.27]. For instance, the basis of the Revolution of Dignity was self-organization, and the relevant political experience accumulated by the society during the months of confrontation was very useful for Ukrainians in their further political struggle in the following years [19, p.27]. The gained skills and expertise became especially vital after the start of the full-scale invasion of Ukraine by the Russian Federation on 24 February 2022. Other crucial elements of efficient responding to hybrid threats are civil society — government cooperation, efficient usage of track I and track II diplomacy, synergy among different societal groups, government and private companies.

The Baltic Sea Region states have exceled in finding comprehensive responses to hybrid threats emanating from the Russian Federation, in particular. These countries have made an all-of-society approach to disinformation a priority — in Lithuania, for instance, the Civic Resilience Initiative uses online and offline tools to help young people tackle disinformation head on [20, p.1]. Attracting people to take disinformation seriously is an urgent task in the Baltic Sea Region states — these relatively small, European Union countries have borders with the Russian Federation and know first-hand that the latter's regime will use trade, cyber-warfare, energy, food and any available mechanisms to pressure its neighbours into toeing the Kremlin line [20, p.1].

Ukrainians today have responded to Russia's onslaught with extraordinary resilience and unity. Thus, Yaholnyk notes that, in order to achieve a fair and lasting peace, Ukraine must elevate its successful and innovative counter-operations in order to reshape the strategic equation [21, p.1]. Organisation LetsData analysed the discourse of local Telegram channels in areas occupied after 24 October, 2022, as well as in frontline communities — in particular, they conducted a study featuring practical case studies and recommendations on how to counter propaganda and disinformation — various messages were communicated to local authorities, and they have been developing different policies and approaches, implementing certain measures — and the results so far have been quite positive [21, p.1]. Thus, it can be noted that Ukraine and the wider Baltic Region countries have demonstrated resilience and adaptability to the information threats coming from the Russian Federation.

Conclusions

It can be concluded that specific features of information resilience in Ukraine and the Baltic Sea Region are related to comprehensive approach to fighting disinformation and malicious propaganda. In particular, it is

establishment of research centers, think tanks, centers of excellence; fact-checking, myth-busting projects and agencies. In a strategic long-term perspective, it is implementation of education programs on critical thinking and media literacy. Respective measures also encompass efficient cooperation between civil society, government and private sector companies. Another important dimension of countering hybrid threats is the effective usage of track I and track II diplomacy.

The response to hybrid information threats needs to be multi-faceted and comprehensive. It can include civilian-military cooperation, synergy between government and civil society as an important mechanism for democracies, and enhancement of information resilience of a society. These efforts need to be undertaken tactically at the level of excellence centers for countering disinformation and penalizing perpetrators, as well as strategically at the level of academic programs and curricula. Information threats in the age of obscurantism, globalization and AI-driven risks and opportunities are constantly changing and evolving, therefore it is necessary to keep monitoring the situation, conducting proper risk assessment and adapting current tactics and strategies to the rapidly changing circumstances.

References

1. Dannreuther, R. (2014). International security: The contemporary agenda. John Wiley & Sons.
2. American Psychological Association. (n.d.). Misinformation and disinformation. https://www.apa.org/topics/journalism-facts/misinformation-disinformation
3. Northeastern University Libraries. (2025, August 22). Fake News/Misinformation/Disinformation: What is Fake News? https://subjectguides.lib.neu.edu/fakenews
4. Wither, J. K. (2020). Per Concordiam, 10(1). George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf
5. Bajarūnas, E., & Keršanskas, V. (2018). Hybrid threats: Analysis of content, challenges posed and measures to overcome. Lithuanian Annual Strategic Review, 16(1), 123-170. https://doi.org/10.2478/lasr-2018-0006
6. Wither, J. K. (2020). Per Concordiam, 10(1). George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf
7. United Nations. (n.d.). Democracy. https://www.un.org/en/sections/issues-depth/democracy/index.html

8. U.S. Department of State. (n.d.). What is resilience? https://2009-2017.state.gov/m/med/dsmp/c44950.htm
9. Centre for Digital Built Britain. (n.d.). Information Resilience — exploring ways to leverage data and information to deliver a digital built Britain. University of Cambridge. https://www.cdbb.cam.ac.uk/research/digital-infrastructure/information-resilience-exploring-ways-leverage-data-and-information
10. Taranenko, A. (2024). Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations. Social Sciences & Humanities Open, 10(1), Article 100987. https://doi.org/10.1016/j.ssaho.2024.100987
11. Ernest, N., Nkenganyi, F. M., Suh Abenwi, J., & Ibrahima. (2023). Qualitative research methodology in social sciences. International Journal of Scientific Research and Management (IJSRM), 11(09), 14311445. https://doi.org/10.18535/ijsrm/v11i09.sh01 (ijsrm.net)
12. Branka, T. (Ed.). (2023). Rethinking the Baltic Sea Region: Trends and challenges. Uppsala universitet. https://uu.diva-portal.org/smash/get/diva2:1786953/FULLTEXT02.pdf (uu.diva-portal.org)
13. Baltic Development Forum. (2018). Home [Website]. https://www.bdforum.org
14. European Commission. (2021). The EU strategy for the Baltic Sea Region (EUSBSR) — factsheet. Retrieved November 2, 2025, from https://ec.europa.eu/regional_policy/sources/cooperate/baltic/factsheet_eusbr_en.pdf
15. Maciejewski, W. (Ed.). (2002). The Baltic Sea region: Cultures, politics, societies. Baltic University Press.
16. Ministry of Foreign Affairs of the Russian Federation. (2023, March 31). The Concept of the Foreign Policy of the Russian Federation (Decree No. 229) [Unofficial translation]. https://theatrum-belli.com/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=https://theatrum-belli.com/wp-content/uploads/2023/04/2023_03_31_The-Concept-of-the-Foreign-Policy-of-the-Russian-Federation.pdf
17. Bajarūnas, E., & Keršanskas, V. (2018). Hybrid threats: Analysis of content, challenges posed and measures to overcome. Lithuanian Annual Strategic Review, 16(1), 123-170. https://doi.org/10.2478/lasr-2018-0006
18. Taranenko, A. (2024). Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations.

Social Sciences & Humanities Open, 10(1), Article 100987. https://doi.org/10.1016/j.ssaho.2024.100987

19. Channell-Justice, E. (2022). Without the state: Self-organization and political activism in Ukraine. University of Toronto Press.
20. Equal Times. (n.d.). In the existential fight [Article]. https://www.equaltimes.org/in-the-existential-fight-against
21. Yaholnyk, A. (2025, May 7). How Ukraine's civil society battles Russia in the information war. Ukraïner. https://www.ukrainer.net/en/how-ukraine-s-civil-society-battles-russia-in-the-information-war/

УДК 327.7 + 341.215.2 DOI 10.17721/2415-881X.2026.100.2.334–344

Тараненко Ганна Геннадіївна
Кандидат політичних наук, доцент кафедри міжнародних відносин
Національний університет «Києво-Могилянська академія» (м. Київ, Україна)
https://orcid.org/0000-0003-2588-4941
e-mail: taranenkoann@yahoo.com

ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ ТА РЕГІОНІ БАЛТІЙСЬКОГО МОРЯ

Резюме

У статті здійснено комплексний аналіз сучасних викликів інформаційній безпеці України та держав регіону Балтійського моря в умовах гібридного протиборства. Обґрунтовано, що інформаційна безпека трансформувалася у самостійний стратегічний компонент національної та міжнародної безпеки, а інформаційні впливи стали важливим інструментом дестабілізації демократичних суспільств. Визначено основні форми сучасних інформаційних загроз, серед яких дезінформація, маніпулятивні наративи, фейкові новини та технології інформаційного впливу, спрямовані на підрив суспільної довіри й посилення політичної поляризації.

Проаналізовано особливості використання Російською Федерацією інформаційно-психологічних операцій проти України та країн Балтійського регіону. Виявлено специфіку російських дезінформаційних наративів щодо України, Латвії, Литви, Естонії та Швеції, а також окреслено ключові суспільно-політичні вразливості, які використовуються для дестабілізаційного впливу. Доведено, що спільною рисою інформаційних атак є їх орієнтація на історичні травми, мовно-культурні суперечності та кризу суспільної довіри.

Особливу увагу приділено концепту інформаційної стійкості як базового механізму протидії гібридним загрозам. Підкреслено, що розвиток інформаційної стійкості передбачає не лише здатність держави реагувати на інформаційні атаки, а й формування довгострокових механізмів захисту демократичного інформаційного простору. Обґрунтовано необхідність багаторівневого підходу до забезпечення інформаційної безпеки, що охоплює

взаємодію державних інституцій, структур безпеки, громадянського суспільства, освітніх програм та центрів стратегічних комунікацій.

Зроблено висновок, що ефективна протидія сучасним інформаційним загрозам потребує регіональної координації, посилення міжнародної співпраці та формування спільної системи інформаційної стійкості України і держав Балтійського моря в умовах зростання гібридних викликів.

Ключові слова: інформаційна стійкість; Україна; Балтійський регіон; інформаційні загрози; гібридні загрози; дезінформація; фейкові новини; пропаганда.

Надійшла до редакції/ Received: 15.02.2026

Прорецензовано/ Revised: 04.03.2026

Прийнято до друку/ Accepted: 24.04.2026