Сьогодні у більшості держав з республіканською формою правління традиційна зброя не входить до номенклатури символів верховної влади. Втім еквівалентом звичаєвого використання зброї у якості владної регалії можна розглядати інавгураційний ритуал передачі контролю над ядерною зброєю, що є прийнятим у країнах ядерного клубу. Нажаль, зараз ми стаємо свідками того, як ядерна зброя перетворюється із маркера політичної могутності держави на знаряддя військово шантажу. Будемо сподіватися, що у людства вистачить розуму залишити її лише у арсеналі символічного протистояння.

***Список використаних джерел:***


1. Tresidder J. (1998). Dictionary of Symbols: An Illustrated Guide to Traditional Images, Icons, and Emblems. San Francisco : Chronicle Books.
2. Lurker M. (1973). Wörterbuch biblischer Bilder und Symbole. München : Kösel.
3. Oakeshott E. (2017). The Archaeology of Weapons: Arms and Armour from Prehistory to the Age of Chivalry. Suffolk : Boydell Press; New Ed edition.
4. Stone G. C. (1999). The Glossary of the Construction, decoration and Use of Arms and Armor of all Countries and in all Times. New York : Dover Publications.



**Ключові слова:** семіотика, зброя, символ, політичне панування, війна.
**Key words:** semiotics, weapons, symbol, political domination, war.



***СЕМЕНЮК ОЛЕКСАНДР ГЕОРГІЙОВИЧ***

*Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, перший заступник керівника, доктор юридичних наук*

***ВЄДЄНЄЄВ ДМИТРО ВАЛЕРІЙОВИЧ***

*Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, головний науковий співробітник, доктор історичних наук, професор*


## ІНФРАСТРУКТУРА УЗАГАЛЬНЕННЯ ДОСВІДУ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

10 грудня 2019 р. Рада міністрів ЄС із загальних справ у річищі реалізації «Стратегічного порядку денного ЄС на 2019–2024 роки» ухвалила резолюцію із визначення пріоритетних напрямків протидії гібридним загрозам (ГЗ) та «підвищення стійкості країн-членів» [1]. Метою передбачених документом заходів визначено «розвиток співпраці з міжнародними організаціями та країнами-партнерами для посилення стійкості

та протидії гібридним загрозам, зокрема, співробітництво між ЄС і НАТО і співпрацю з країнами-сусідами Євросоюзу». При цьому ГЗ інтерпретуються як «широкий спектр скоординованих методів та дій, що використовуються ворожими державами та недержавними акторами з метою ураження вразливих демократичних держав та інституцій, не переступаючи межу формального розв'язання військових дій». Прикладами таких дій названі кібернетичні атаки, втручання у вибори, кампанії дезінформації, включаючи ті, що здійснюються у соціальних медіа.

Проводяться заходи із посилення блокової взаємодії, серед них – проведений за участю штабу Сил спецоперацій НАТО у квітні 2018 р. семінар із взаємодії між країнами Північної Європи та Прибалтики. Обговорюється створення «Координаційного комітету високого рівня для розробки стратегій та контрстратегій гібридних загроз та вивчення вразливостей» (координатора дослідницької та навчальної діяльності з протидії ГЗ, створення багатонаціональних мереж експертів, роботи із громадською свідомістю тощо).

Показові пріоритетні позиції, котрі (на думку профільних органів ЄС) є найбільш потенційно вразливими для ГЗ та потребують посиленого захисту: сфера «чутливих технологій» (штучний інтелект, засоби обробки та аналізу великих інформаційних масивів тощо); захист національної та загальноєвропейської критичної інфраструктури, від якої залежить належне функціонування держави, економіки та суспільства, їх фінансового та приватного секторів; протидія дезінформації на основі імплементації «Плану дій ЄС проти дезінформації» тощо.

У порядку денному міждержавних заходів вищого рівня країн ЄС відведене поважне місце тематиці несилових дій та гібридних загроз. У трьох пострадянських республіках Балтії та у Фінляндії діють *Центри передового досвіду із узагальнення даних про гібридні загрози й тактику гібридної війни*, працює *Центр кібероперацій при штабі ОЗС НАТО* у Монсі (Бельгія). Зі згаданими установами взаємодіють Центр передового досвіду НАТО з кіберзахисту (Таллінн), *Центр передового досвіду НАТО з протидії тероризму* (Анкара). У Польщі та Румунії розгорнуті *контррозвідувальні Центри НАТО з протидії розвідці як різновиду гібридних загроз* (NATO Counter Intelligence Centre of Excellence – NATO CI COE). При штабквартирі НАТО створені групи сприяння у боротьбі з гібридними загрозами. Спільна тематика досліджень цих установ та відповідних центрів у США охоплює широке коло проблематики гібридних конфліктів, розробку базових засад ведення сучасних війн та конфліктів.

Спеціалісти відзначають важливу комунікаційну роль у протидії ГЗ між ЄС та НАТО *«Європейського центру передового досвіду»* (ЄЦПД, офіційно відкритий у Хельсінкі 2 жовтня 2017 р., робочий орган – Секретаріат у столиці Фінляндії, до складу якого безпосередньо відрядили своїх співробітників шість країн) [2]. У його діяльності беруть участь до 20 країн, річний бюджет станом на 2021 р. становить 2,9 млн євро. В основу роботи Центру покладено т.зв. «фінську модель комплексної безпеки» (скоординована діяльність сукупності різнопрофільних

органів влади і відомств, які разом забезпечують необхідний масштаб і поширення заходів з протидії гібридним загрозам), а також розроблену ЄЦПД концепцію трьох «Зацікавлених спільнот» (COI), котрі передбачають розвиток мережевої організації та технологій, аналітичну діяльність, тренування і навчання учасників, накопичення інформації про стратегічну обстановку, удосконалення сил і засобів реагування на ГЗ в країнах-учасницях. Згодом додано четверту складову – із вивчення стратегічного розуміння гібридної війни [3].

Відтак структуру ЄЦПД утворили такі органи як: Комітет гібридного впливу (лідер – Велика Британія); Комітет недержавних акторів гібридної війни (Швеція); Комітет вразливості й протидії (Фінляндія); Комітет стратегії і оборони (Німеччина, створений у серпні 2018 р. для вироблення розуміння комплексу проблем протидії неконвенційним загрозам на стратегічному рівні). Усі країни-учасниці роблять значні внески в роботу Центру. Чотири країни взяли на себе провідну роль в Зацікавлених спільнотах Центру, а шість з них підтримують роботу Центру, відрядивши своїх співробітників до Секретаріату в Гельсінкі. Конкретним прикладом національного внеску є тренувальний захід з питань комплексної безпеки, який Центр організував разом з Фінськими силами оборони. Цей тижневий захід розрахований на країни – члени НАТО і ряд країн-партнерів з метою допомогти їм розробити комплексні підходи або об'єднані доктрини задля протидії гібридним загрозам.

ЄЦПД проводить в країнах ЄС, США і Канаді семінари з широкої проблематики – з правової протидії нестандартним безпековим загрозам, забезпечення безпеки на морі, на стратегічних комунікаціях і у виборчій системі, з захисту енергетичної сфери, кібербезпеки, із захисту супутникових навігаційних систем тощо. Розглядаються і певні інноваційні проблеми. В останні роки спостерігається прагнення Євросоюзу (передовсім – країн «старої Європи» – континентальних конкурентів США) посилити самостійність та пошуки власної моделі бачення ознак/протидії гібридним загрозам. У першу чергу, йдеться про протистояння ГЗ у сфері кібернетичної безпеки, дезінформації, протидії розвідувально-підривній діяльності, посилення готовності до застосування противником ядерної, хімічної, біологічної зброї.

Одним із інструментів взаємодії країн ЄС у згаданій царині вважається створений в Європейській системі зовнішніх дій «Об'єднаний гібридний осередок» (Hybrid Fusion Cell) з аналізу інформації щодо ГЗ, включаючи такі напрями моніторингу та аналізу як ядерний, хімічний, біологічний, контррозвідувальний та кібернетичний (зокрема, шляхом створення «Плану дій із посилення готовності та стійкості до ризиків безпеки у відповідних сферах»);

розвиток спільних стратегічних комунікаційних можливостей ЄС (як от «онлайн-платформа з дезінформації») із протидії деструктивним технологіям ІПСО, втручанням у вибори тощо;

захист кібернетичної сфери КБ шляхом створення спільної бази сертифікації кіберзагроз, розробка засад діяльності «Агентства кібербезпеки ЄС», впровадження досягнень в області цифрових технологій для

безпечного зв'язку між державами – членами ЄС, розробці засобів кібердипломатії, технологій відсічі кібератак. Створюється «спецплатформа з кібербезпеки» для навчання персоналу, з лютого 2020 р. впроваджено спільні навчання НАТО і ЄС «Кіберкоаліція»;

зміцнення потенціалу країн ЄС із протидії ворожій розвідувальній діяльності у порозумінні із США, НАТО та іншими міжнародними організаціями. Згаданий «Об'єднаний гібридний осередок» буде залучати досвідчених контррозвідників. Передбачена «Спільна рамкова програма з протидії гібридним загрозам» (22 основні заходи, включаючи обмін інформацією, зміцнення імунітету суспільства до екстремізму та тероризму, захист критичної інфраструктури, кіберсфери – у межах «Плану дій із видалення з Інтернету матеріалів терористичних організацій» тощо) [4].

Поряд з цим, європейські спеціалісти з проблем сучасної конфліктності в цілому ґрунтують свої концепції на постулаті апріорної воєнно-технічної переваги Заходу. Відповідно, у розробках із тематики ГЗ чільне місце приділяється проблемам використання у військовій справі штучного інтелекту, робототехніки, суперкомп'ютерів, систем кібернетичної війни, високоточної далекобійної зброї, повітряно-космічних сил, безпілотних авіаційних систем, сил спеціальних операцій тощо.

***Список використаних джерел:***


1. Countering hybrid threats: Council calls for enhanced common action. URL: https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/ (дата звернення 12 грудня 2021).
2. The European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi/about-us/ (дата звернення 18 січня 2022).
3. Хагельстам А. Співпраця заради протидії гібридним загрозам. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (дата звернення 10 січня 2022).
4. The European Commission and the High Representative adopted today a Joint Framework to counter hybrid threats URL: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 (дата звернення 11 січня 2022).



**Ключові слова:** європейська безпека, безпекове співробітництво, гібридні загрози, аналітична діяльність, стратегічні комунікації.

**Key words:** European security, security cooperation, hybrid threats, analytical activities, strategic communications.