СЕКЦІЯ 3
ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ
ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

ЕТИМОЛОГІЧНИЙ ВИМІР ВИЗНАЧЕННЯ ПОНЯТТЯ «ГІБРИДНИХ ЗАГРОЗ» (НА ПРИКЛАДІ ОКРЕМИХ ВИТОКІВ)

ETYMOLOGICAL DIMENSION OF THE DEFINITION OF THE CONCEPT OF "HYBRID THREATS" (ON THE EXAMPLE OF INDIVIDUAL LEAKS)

УДК 351
DOI https://doi.org/10.32782/pma2663-5240-2023.35.12

Хряпинський А.П.
к. юрид. наук

У статті здійснено комплексне наукове обґрунтування та дослідження проблематики визначення сутності та особливостей етимологічного змісту визначення поняття «гібридних загроз».
Акцентовано увагу на тому, що гібридні загрози, як явище та концепція, швидко опинились у центрі дискурсу політики безпеки після російської агресії проти України в 2014 році, з поважних причин. Природа антагоністичних загроз нашим відкритим, демократичним суспільствам і процесам прийняття політичних рішень розширилася, а інтенсивність і потенційна шкода такого роду антагоністичної поведінки зросла. Протягом останніх років спостерігався швидкий розвиток досліджень і аналізу, а також практичних дій, природний розвиток, враховуючи погіршення ситуації з політикою безпеки в Європі та розширення масштабів антагоністичних державних загроз, з якими ми стикаємося.
Аргументовано показано, що підвищення стійкості передбачає не лише зміцнення інфраструктури, фізичної чи соціальної; це також посилення когнітивної та правової стійкості. Нові модні слова, що постійно з'являються, – це підхід, що охоплює весь уряд і все суспільство. Очевидно, що приватний бізнес і громадянське суспільство відіграють важливу роль у протидії гібридним загрозам. Це особлива сила наших відкритих ліберальних демократій. Міжнародна співпраця та солідарність є важливими інструментами для посилення стримування, розуміння загрози та формування стійкості. Невипадково ЄС і НАТО розробили нові інструменти для протидії гібридним загрозам. Показано, що існує потреба краще зрозуміти це явище, щоб мати можливість виявити та ідентифікувати його, створити стійкість проти нього та, нарешті, протистояти йому. Зараз теорія і практика стрімко розвиваються рука об руку. Між аналітиками та практиками в цій галузі точаться жваві дебати. Не буде надмірним перебільшенням сказати, що зараз це є науковою межею політики безпеки. Ми знаходимося в процесі розробки нової спільної стратегічної культури, як на національному, так і на міжнародному рівнях, щодо того, як саме керувати цими антагоністичними загрозами в мирний час.

Ключові слова: *управління, гібридні загрози, протидія та превенція, інноваційний розвиток, протидія загрозам, превенція загрозам, гібридні загрози в управлінні.*

In the article, a comprehensive scientific substantiation and study of the problem of determining the essence and peculiarities of the etymological content of the definition of the concept of "hybrid threats" is carried out.
Attention is focused on the fact that hybrid threats, as a phenomenon and a concept, quickly found themselves at the center of the discourse of security policy after the Russian aggression against Ukraine in 2014, for good reasons. The nature of antagonistic threats to our open, democratic societies and political decision-making processes has expanded, and the intensity and potential harm of such antagonistic behavior has increased. Recent years have seen a rapid development of research and analysis as well as practical action, a natural development given the deterioration of the security policy situation in Europe and the expansion of the antagonistic state threats we face.
It is argued that increasing resilience involves not only strengthening infrastructure, physical or social; it is also a strengthening of cognitive and legal stability. New buzzwords that keep popping up are a whole-of-government, whole-of-society approach. It is clear that private business and civil society play an important role in countering hybrid threats. This is a particular strength of our open liberal democracies. International cooperation and solidarity are important tools for strengthening deterrence, understanding the threat, and building resilience. It is not by chance that the EU and NATO have developed new tools to counter hybrid threats. It is shown that there is a need to better understand this phenomenon in order to be able to detect and identify it, build resilience against it, and finally counter it. Now theory and practice are rapidly developing hand in hand. There is a lively debate between analysts and practitioners in this field. It is no exaggeration to say that this is now the scientific frontier of security policy. We are in the process of developing a new shared strategic culture, both nationally and internationally, about how exactly to manage these antagonistic threats in peacetime.

Key words: *management, hybrid threats, counteraction and prevention, innovative development, countermeasures against threats, prevention of threats, hybrid threats in management.*

Постановка проблеми у загальному вигляді. Гібридні загрози, як явище та концепція, швидко опинились у центрі дискурсу політики безпеки після російської агресії проти України в 2014 році, з поважних причин. Природа антагоністичних загроз нашим відкритим, демократичним суспільствам і процесам прийняття політичних рішень розширилася, а інтенсивність і потенційна шкода такого роду антагоністичної поведінки зросла. Протягом останніх років спостерігався швидкий розвиток досліджень і аналізу, а також практичних дій, природний розвиток, враховуючи погіршення ситуації з політикою безпеки в Європі та розширення масштабів антагоністичних державних загроз, з якими ми стикаємося.

Існує потреба краще зрозуміти це явище, щоб мати можливість виявити та ідентифікувати його, створити стійкість проти нього та, нарешті, протистояти йому. Зараз теорія і практика стрімко розвиваються рука об руку. Між аналітиками та практиками в цій галузі точаться жваві дебати. Не буде надмірним перебільшенням сказати, що зараз це є науковою межею політики безпеки. Ми знаходимося в процесі розробки нової спільної стратегічної культури, як на національному, так і на міжнародному рівнях, щодо того, як саме керувати цими антагоністичними загрозами в мирний час.

Аналіз останніх досліджень і публікацій. Теоретико-прикладні аспекти дослідження внутрішніх загроз знайшли своє відображення у наукових працях багатьох вчених, зокрема таких як: Л. Акімова, Е. Бухвальд, З. Гбур, С. Лазаренко, В. Ліпкан, Н. Словацька. Водночас, питання пов'язані із комплексним науковим обґрунтуванням та дослідження сутності й етимологічного змісту визначення поняття «внутрішніх загроз» з урахуванням сучасних здобутків науки й методологічних підходів ще не отримали належного теоретико-прикладного обґрунтування та аналізу.

Внаслідок чого **метою** даної статті є наукове обґрунтування та дослідження проблематики етимологічного змісту визначення поняття «внутрішніх загроз».

Виклад основного матеріалу. Наші традиційні концептуальні відмінності між зовнішньою та внутрішньою безпекою, військовими та цивільними справами, а також між національними та міжнародними рішеннями, які керують нашим розумінням та бюрократією; організаційна структура здається менш придатною або може навіть заважати нам, коли ми підходимо до теми гібридних загроз. Іноді виникає питання, чи всі розмови (і дії) про гібридні загрози – це просто ажіотаж, просто переупакування чогось, що завжди існувало. Звичайно, методи та широкий інструментарій агресивних інструментів нав'язування своєї політичної волі іншим державам і суспільствам існували завжди. Тим не менш, відновлення уваги до цих питань після російської агресії проти України в 2014 році та в інших місцях є виправданим.

Під загрозою можна розуміти поєднання спроможності, наміру та можливості. Спроможність окремих держав скоординовано застосовувати широкий спектр антагоністичних інструментів, безумовно, зросла. Деякі з цих інструментів є новими або використовуються по-новому [1, с. 30]. Такий же намір: ми можемо спостерігати за діяльністю ворожої держави в обсязі, якого не бачили протягом тривалого часу. Протягом останнього десятиліття чи близько того деякі уряди явно зменшили свої обмеження на використання зловмисних і зловмисних дій. У той же час можливості, надані нашими власними вразливими місцями, зросли завдяки посиленню цифровізації та залежності, а також недостатнім інвестиціям у внутрішню та зовнішню безпеку. Тож так, гібридні загрози існують тут і зараз, і вони не збираються зникати. Гібридні загрози не є потенційним ризиком – те, що може статися. Вони є актуальною і теперішньою реальністю, з якою нам потрібно мати справу [2, с. 13].

Управління гібридними загрозами є предметом дискурсу, який швидко зростає на національному та міжнародному рівнях. Це вимагає від держав, суспільств і міжнародних організацій розуміння загрози, підвищення стійкості та набуття можливостей для протидії загрозі.

Розуміння загрози включає розвиток усвідомлення своєї вразливості; розуміння мотивів і способів дій антагоністичного стану; а також виявлення та ідентифікація загрози, завдання, яке вимагає розширеного усвідомлення ситуації. Гібридні загрози – це скоординовані та синхронізовані дії, які можуть проявлятися різними способами та у багатьох секторах. Нам потрібно з'єднати всі крапки, часто з датчиків, які не обов'язково підключалися раніше, і припустити цілісний підхід. Наші супротивники, звичайно, так [3, с. 44].

Побудова стійкості означає зменшення потенційних переваг антагоністичної держави, так зване стримування запереченням. Ні розуміння загрози, ні формування стійкості не є «ракетною наукою», хоча обидва вимагають цілеспрямованих зусиль і скоординованого підходу всього уряду.

Однак протидія гібридним загрозам частково означає вихід на незвідану та складну територію. «Протидію» можна розділити на застосування контрзаходів проти триваючих антагоністичних дій і створення стримування потенційних атак шляхом зміни аналізу витрат і вигод антагоністичного стану, так зване стримування покаранням. Гібридні загрози за своєю природою створені для створення плутанини та обману, і їх важко виявити та приписати. Вони складаються з великої кількості можливих антагоністичних засобів, які використовуються скоординовано, деякі з яких, наприклад дезінформація, не обов'язково повинні бути незаконними чи суперечити міжнародному праву. Симетричні відповіді «око за око» рідко можливі або бажані. Слід дотримуватись міжнародного права. Ми займаємося захистом наших відкритих, демократичних суспільств і міжнародного порядку, заснованого на правилах [4, с. 229].

Як правило, антагоністична держава – це авторитарний уряд або диктатура, яка мало перешкоджає агресивній поведінці та має високо централізовані, швидкі та скоординовані структури прийняття рішень. Антагоністичні, зловмисні дії розглядаються – і використовуються – як політичний інструмент для досягнення стратегічних цілей, засіб досягнення мети. Ця мета може полягати в тому, щоб вплинути на прийняття наших рішень або підірвати наші суспільства, завдати шкоди [5, с. 61].

Інформаційне середовище та величезний потенціал для його використання у зловмисних діях вже певний час тому привернули значну увагу фахівців у сфері гібридних загроз та гібридної війни. З початку тисячоліття використання операцій впливу як державними, так і недержавними акторами стає все більш очевидним як для тих, хто приймає рішення, так і для пересічного населення. Цифрова революція, що впливає на розповсюдження інформації та соціальний обмін у наших суспільствах і спільнотах, а також посилення зв'язаності ключових суспільних систем та інфраструктури відкрила не лише нові можливості, а також і вразливі місця. Крім того, зміни на ринках праці та у демографічному складі багатьох суспільств розширили можливості та горизонти для частини суспільства, але залишили інших невпевненими у своєму місці чи представленості їхніх інтересів у традиційних ЗМІ чи політичній сфері. Це мало прямий вплив як на національну публічну політику, так і на міжнародні відносини, не в останню чергу пов'язане з різними референдумами та виборами, наприклад, у Великій Британії та Сполучених Штатах у 2016 році та у Франції у 2017 році.

Протидія гібридним загрозам, виходячи за рамки створення стійкості, є стрімко зростаючим і поглибленим політичним та інтелектуальним пошуком. Це складна частина переосмислення та редизайну політики безпеки. Міжнародна співпраця та обміни між державними органами, аналітичними центрами та академічними колами відіграють важливу роль у цьому [6, с. 74].

Діяльність, що стоїть за гібридними загрозами, здійснюється, як правило, акторами з більш-менш авторитарними або тоталітарними поглядами на владу. Мета полягає в тому, щоб націлитися на системну вразливість демократій, використовуючи всі інструменти, які є в розпорядженні авторитарної держави. Демократичні держави також можуть, зіткнувшись з ворожим втручанням, здійснювати відповідні гібридні контрзаходи, але існують значні відмінності порівняно з діями, вжитими авторитарними державами.

У багатьох поясненнях і визначеннях, що стосуються концепції гібридних загроз, як державні, так і недержавні актори згадуються як суб'єкти, які беруть участь у реалізації гібридних загроз з метою втручання у внутрішній простір інших держав для посилення своїх власних стратегічних інтересів, у тому числі шляхом насильства. Використання гібридних загроз як механізму підтримки різних політик для просування власних стратегічних інтересів характерно для таких держав, як росія, Китай, Іран і Північна Корея, недержавних акторів, таких як Хезболла, Аль-Каїда та ІДІЛ, а також для декількох проксі-акторів – транснаціональних організованих злочинних синдикатів, ідеологічних рухів і прибуткових «незалежних» акторів.

Одним із головних викликів у протидії гібридним загрозам є те, що, з одного боку, ми стикаємося з традиційною проблемою безпеки та зовнішньої політики – зовнішнім антагоністичним державним суб'єктом, тобто зовнішньою загрозою – але з іншого боку, загрози часто проявляються у внутрішньому сферу безпеки, де також можна знайти багато можливих контрзаходів [7, с. 20]. Політична культура та бюрократичні структури західних держав часів холодної війни чи пост-холодної війни не обов'язково сприяють подоланню розриву між тим, що традиційно тлумачиться як «внутрішні» та «зовнішні» виклики безпеці. Нове гібридне середовище загроз означає, що концепція політики безпеки має бути розширена та частково переосмислена [8, с. 4].

Підвищення стійкості передбачає не лише зміцнення інфраструктури, фізичної чи соціальної; це також посилення когнітивної та правової стійкості. Нові модні слова, що постійно з'являються, – це підхід, що охоплює весь уряд і все суспільство [9, с. 303]. Очевидно, що приватний бізнес і громадянське суспільство відіграють важливу роль у протидії гібридним загрозам. Це особлива сила наших відкритих ліберальних демократій. Міжнародна співпраця та солідарність є важливими інструментами для посилення стримування, розуміння загрози та формування стійкості. Невипадково ЄС і НАТО розробили нові інструменти для протидії гібридним загрозам.

Висновки. Таким чином, можна зробити висновок, що вирішення цієї важливої, але складної проблеми щодо визначення сутності внутрішніх загроз має бути командною системою зусиль. Вченим, аналітикам і практикам є чому навчитися один у одного. Іноді ми використовуємо різні слова та концептуальні моделі для вирішення цих проблем. Існують різні погляди на інструментарій і те, як найкраще структурувати наші системи для боротьби із загрозами. І існують різні точки зору – національні/міжнародні, внутрішні/зовнішні, військові/цивільні – на цю тему. Нам є чому навчитися з цих різних точок зору, обмінюватися найкращими практиками та ідеями, які є безкоштовними та можуть покращити наш розум і дії, тоді як великий аналіз поглядів, заснований на глибоких знаннях і багаторічному досвіді, і є дуже бажаним і важливим внеском у подальшому шляху в боротьбі з гібридними загрозами та потребує подальшого науково-теоретичного пізнання.

ЛІТЕРАТУРА:

1. Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee and Madeline McCue, Addressing Hybrid Threats (Stockholm: Swedish Defence University, 2018), 10 fft.

2. Mark Galeotti, 'Hybrid, Ambiguous, and Non-Linear? How New Is Russia's "New Way of War"?', Small Wars & Insurgencies 27, no. 2 (2016): 7.

3. Michael Kofman and Matthew Rojansky, 'A Closer Look at Russia's "Hybrid War"', Kennan Cable 7 (Wilson Center: Kennan Institute, 2015).URL: https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

4. Timothy Thomas, 'The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation and New-Type Thinking', The Journal of Slavic Military Studies 29, no. 4 (2016): 557–9.

5. Foreign Policy Concept; Valery Gerasimov, 'Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy: Thoughts on Future Military Conflict-March 2018'. Translated by Dr Harold Orenstein. Army University Press, Military Review, January–February 2019. https://www.armyupress.army.mil/Journals/Military-Review/Eng lish-Edition-Archives/Jan-Feb-2019/Gerasimov-Future/; Sergey Glazyev, advisor to Russian president on issues of economic integration, quoted in RIA Novosti, 8 April 2015.

6. Alexander Lanozska, 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', International Affairs 92, no. 1 (2016): 178.

7. Pascal Brangetto and Matthijs A. Veenendaal, 'Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations', 8th International Conference on Cyber Conflict (CyCon), 31 May–3 June 2016, Tallinn, Estonia. https://ieeexplore.ieee.org/abstract/document/7529430

8. Martin Kragh and Sebastian Åsberg, 'Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case', Journal of Strategic Studies 40, no. 6 (2017): 35.

9. Edward Deverell, 'Att identifiera och motstå informationspåverkan: En jämförande studie av hur de nordiska länderna organiserar arbetet', Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift, no. 1 (2019): 31–54.