

Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019).

Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2023. № 8.

DOI: <http://doi.org/10.32702/2307-2156.2023.8.8>

УДК 351

А. П. Хряпинський,

к. ю. н., м. Харків, Україна

ORCID ID: <https://orcid.org/0000-0002-2492-051X>

І. М. Хмиров,

д. держ. упр., доцент, старший науковий співробітник наукового відділу з проблем цивільного захисту та техногенно-екологічної безпеки науково-дослідного центру,

Національний університет цивільного захисту України, м. Харків, Україна

ORCID ID: <https://orcid.org/0000-0002-7958-463X>

**МЕХАНІЗМИ ФОРМУВАННЯ КОМПЛЕКСНИХ ЗАСАД ПРОТИДІЇ
ГІБРИДНИМ ЗАГРОЗАМ ТА ГІБРИДНІЙ ВІЙНІ У КОНТЕКСТІ
ВИЗНАЧЕННЯ ПРОБЛЕМАТИКИ «СІРИХ ЗОН»**

A. Khriapynskyi,

PhD in Law, Kharkiv, Ukraine

I. Khmyrov,

Doctor of Sciences in Public Administration, Associate Professor, Senior Researcher,

Scientific Department of Problems of Civil Protection and Technogenic and

Ecological Safety of the Scientific and Research Center,

National University of Civil Protection of Ukraine, Kharkiv, Ukraine

**MECHANISMS FOR THE FORMATION OF COMPLEX PRINCIPLES FOR
COUNTERING HYBRID THREATS AND HYBRID WAR IN THE
CONTEXT OF DEFINING THE PROBLEMS OF "GRAY ZONES"**

У даній статті здійснюється аналіз та доктринальний синтез концептуальних засад становлення механізмів формування комплексних засад протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон.

В результаті проведеного дослідження визначено аспекти концептуальних засад становлення механізмів формування алгоритмів та методів протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон. Констатовано, що виокремлення значення сірих зон є далеко не новим підходом та проблематикою, але усвідомлення та робота з включення його наслідків у політику, спроможність та реалізацію спроможності в західних демократіях набрали обертів в останні роки. Протягом останніх кількох років ряд європейських та міжнародних установ неодноразово отримували повідомлення засобів масової інформації про конкретні дії, наприклад, дезінформацію або операції зламування та витоку інформації, спрямовані на те, щоб змінити хід публічних дебатів або зменшити довіру до ключових суспільних акторів. У такому інформаційному середовищі легко потрапити в проблемно-орієнтоване відчуття безперервного шквалу загроз і втратити з поля зору більш витончені довгострокові події, які зміцнюють здатність реагувати та створювати стійкість до них. Безсумнівно, легше описати загрозу, спрямовану на конкретну подію чи ціль, окреслену в часі, ніж більш тонкі зміни в уряді чи суспільстві. Широкий огляд літератури щодо діяльності інформаційного впливу підкреслює, що до найбільш важливих методів протистояння гібридних загроз можна віднести: багатонаціональні організації та проекти, національні урядові організації та неурядові організації.

Аргументовано показано, що природа антагоністичних загроз нашим відкритим, демократичним суспільствам і процесам прийняття політичних рішень розширилася, а інтенсивність і потенційна шкода такого роду антагоністичної поведінки зростає. Протягом останніх років спостерігався швидкий розвиток досліджень і аналізу, а також практичних дій, природний

розвиток, враховуючи погіршення ситуації з розширення масштабів антагоністичних державних загроз, з якими ми стикаємося.

In this article, an analysis and doctrinal synthesis of the conceptual foundations of the formation of mechanisms for the formation of complex foundations for countering hybrid threats and hybrid war is carried out in the context of defining the problems of gray zones.

As a result of the conducted research, the aspects of the conceptual foundations of the formation of mechanisms for the formation of algorithms and methods of countering hybrid threats and hybrid war in the context of determining the problems of gray areas were determined. It has been established that highlighting the importance of gray areas is far from a new approach and problem, but awareness and work on including its consequences in policy, capacity, and implementation of capacity in Western democracies have gained momentum in recent years. Over the past few years, several European and international institutions have repeatedly received media reports of specific actions, such as disinformation or hacking and leaking operations, aimed at changing the course of public debate or undermining trust in key public actors. In such an information environment, it is easy to get caught up in a problem-oriented sense of a continuous barrage of threats and lose sight of the more subtle long-term developments that strengthen the ability to respond and build resilience to them. It is certainly easier to describe a threat directed at a specific event or target outlined in time than more subtle changes in government or society. A broad review of the literature on information influence activities emphasizes that the most important methods of countering hybrid threats include multinational organizations and projects, national governmental organizations, and non-governmental organizations.

It is argued that 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 worsening situation of expanding the scale of antagonistic state threats we face.

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

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

Постановка проблеми. В умовах воєнного стану в Україні та відкритої повномасштабної збройної агресії росії проти України, гібридні загрози, як явище та концепція, швидко опинились у центрі дискурсу політики безпеки ще у 2014 році. Природа антагоністичних загроз нашим відкритим, демократичним суспільствам і процесам прийняття політичних рішень розширилася, а інтенсивність і потенційна шкода такого роду антагоністичної поведінки зростає. 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.

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 концептуальних засад становлення механізмів формування комплексних засад протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон ще не отримали належного теоретико-прикладного обґрунтування та аналізу.

Внаслідок чого **метою** даної статті є наукове обґрунтування та дослідження проблематики концептуальних засад становлення механізмів формування комплексних засад протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон.

Виклад основного матеріалу. Останніми роками міжнародне середовище безпеки перетворилося на нестабільну та дедалі сірішу зону війни та миру. Виклики безпеці, які виникають через гібридні загрози та гібридну війну (надалі за текстом – «НТ&НВ»), сьогодні займають перше місце в порядку денному безпеки по всьому світу. Однак, незважаючи на увагу та зростаючий обсяг досліджень з конкретних питань, існує неминуча потреба в дослідженнях, які привертають увагу до того, як ці виклики можна вирішити, щоб розробити комплексний підхід до виявлення, аналізу та протидії НТ&НВ.

Як відомо, з плином часу сіра зона між миром і війною значно розширилася, що підкреслює необхідність розуміння гібридної війни та пов'язаних із нею загроз. Західні демократії – це не лише ті держави, які найчастіше підпадають під дію гібридних заходів, але й найбільш вразливі. Через те, що вони є відкритими, плюралістичними та ліберальними суспільствами зі свободою преси та верховенством права, західні демократії демонструють як притаманні слабкості, на які можна націлити, так і невід'ємні обмеження – зокрема через верховенство права та основні свободи – які обмежують можливості для оборонні дії. Західні уряди все більше визнають ці вразливі місця, які розробили низку організацій для їх вирішення, хоча координація в багатьох випадках залишається слабкою.

Сучасній науці щодо цих явищ бракує загального визначення, а

використання термінології залишається суперечливим. Насправді НТ&НВ – це лише два з безлічі різних, але збігаються, концепцій, які використовуються для опису подібного явища, де «асиметрична війна», «війна шостого покоління», «безконтактна війна», «сірі війни», «нова війна», «війна наступного покоління», «неоднозначна війна», «нерегулярна війна», «нелінійна війна», «конфлікт повного спектру» та «нетрадиційна війна» є прикладами більш-менш синонімічних термінів [1, с. 140-141].

Відтак, НТ&НВ – стиль двадцять першого століття – відрізняються від традиційних загроз і війни більше за інтенсивністю та масштабом, ніж за характером. Винятком є віртуальна або цифрова сфера, яка надає нові інструменти та знижує початкову вартість їх використання. НТ&НВ позначають супротивників або антагоністів, які прагнуть досягти результатів без війни, порушити, підірвати або завдати шкоди політичній системі та згуртованості об'єкта шляхом поєднання насильства, контролю, підривної діяльності, маніпуляції та поширення (дез)інформації. Таким чином, вони націлені на протилежні суспільства, а не комбатанти [2, с. 188].

НТ&НВ передбачає одночасну присутність ряду можливих засобів боротьби, від загроз війни до пропаганди та всього, що між ними. Таким чином, вони включають численні інструменти влади та впливу, хоча з наголосом на загрозах, як невійськових, так і військових, які діють за межами відкритої війни. Ідентифікація НТ&НВ не дозволяє провести чітке розмежування між різними формами акторів, державними чи недержавними; солдати чи цивільні особи; організоване насильство, терор, злочинність або війна в традиційному розумінні. Незалежно від суб'єкта, від якого походить загроза, для таких суб'єктів стало звичним комбінувати та пристосовувати поєднання звичайних і нерегулярних засобів для досягнення максимального ефекту. Таким чином, підвищена увага до НТ&НВ у сучасному західному стратегічному мисленні є передусім реакцією на інноваційну поведінку зовнішніх антагоністів. Таким чином, гібридна термінологія швидко набула популярності в західних громадських і політичних дебатах, де вона перетворилася на всеохоплюючий

погляд на міжнародну поведінку росії, пронизуючи стратегічний, оперативний і тактичний рівні. Тим часом Китай поступово став не лише економічною, а й військовою державою. Через асиметрію у військовій та економічній силі ці актори шукають способи та засоби кинути виклик Заходу, використовуючи вразливі місця в існуючих інститутах безпеки, а також у західних демократіях. Таким чином, НТ&НВ стали термінами, які зазвичай використовуються для опису стратегії противників глобальної гегемонії Заходу.

Проте, як зазначалося раніше, концепції НТ&НВ залишаються суперечливими. Крім того, стверджується, що групування різноманітних некінетичних засобів, включаючи економічні та інформаційні засоби, під заголовком гібридної війни, небезпечно розширює концепцію "війна". Проте інші критики вказують на те, що концепція гібридної війни стала надзвичайно розширеною, розширившись у межах, щоб охопити більшу частину агресивної політики. В той же час, визнаючи неоднозначність і слабкість НТ&НВ, а також інших концептуальних ярликів, ми зберігаємо його корисність у цілісному аналізі того, як низка акторів, державних і недержавних, стратегічно поєднує кінетичні та некінетичні засоби влади для реалізації інтересів. і досягати цілей у сучасному глобалізованому світі [3, с. 41].

Враховуючи притаманне розуміння того, що еволюція та привабливість ідеї НТ&НВ пов'язана з асиметрією влади та ресурсів, ця концептуалізація видається особливо корисною як основа для розуміння методів і поведінки тих, хто кидає виклик у глобальному чи регіональному масштабі, зокрема росія, Китай та Іран. Однак це аж ніяк не заважає західним демократіям поєднувати різні інструменти державного управління у спосіб, який можна охарактеризувати як гібридну війну [4, с. 45]. Дійсно, з усіма своїми недоліками та двозначностями, дебати про гібридну війну кинули виклик західному бінарному мисленню про війну та мир, а також про звичайну та нетрадиційну війну. Це сприяло більш повному розумінню того, як супротивники можуть інноваційно поєднувати низку інструментів зовнішньої політики, щоб націлити на конкретні вразливі місця західних суспільств і обійти їхні існуючі захисні

структури. І це підкреслило необхідність цілісного аналізу для розуміння та дій у сучасному середовищі безпеки. З точки зору розвідки, це також підкреслює необхідність поєднання розвідувальних даних військових і цивільних агенцій або навіть між розвідувальними і нерозвідувальними агенціями.

У 2014 році в Підсумковій декларації саміту НАТО в Уельсі описано «специфічні виклики, пов'язані з загрозами гібридної війни», і підкреслено важливість того, щоб альянс розробив «необхідні інструменти та процедури», щоб дати змогу реагувати на такі загрози. Вони також підкреслили, що для цього потрібен широкий спектр зусиль, пов'язаних із традиційними військовими можливостями, але також і поза ними. Того ж року було започатковано Центр передового досвіду НАТО StratCom у Ризі, Латвія. Він спрямований на підтримку «процесу розвитку спроможності НАТО, ефективності місії та оперативної сумісності шляхом надання всебічної та своєчасної експертизи у сфері стратегічних комунікацій». Крім того, Спільний центр передового досвіду кіберзахисту НАТО, створений у 2008 році, став ще одним важливим центром досліджень, навчання та навчань для альянсу з точки зору гібридних загроз. Одна стаття, яка ілюструє збіг між гібридними загрозами від CCD CoE, - це робота Бранджетто та Венендала «Кібероперації впливу: використання кібератак на підтримку операцій впливу», в якій досліджується, як вплив на поведінку цільової аудиторії стає основним ефектом кібероперації.

Центр аналізу розвідувальних даних ЄС (INTCEN) є ще одним ключовим гравцем, здатним збирати розвіддані та порівнювати такі внески від держав-членів ЄС. Це призводить до аналізу та оцінки для того, щоб надати голові Європейської служби зовнішніх дій та керівництву ЄС ситуаційне уявлення. Таким чином, це має важливу функцію для забезпечення того, щоб низка сфер, що збігаються, таких як ті, що знаходяться в межах царство гібридних загроз, розуміються та відстежуються.

Крім того, Європейська Рада вирішила створити робочу групу EEAS East StratCom Task Force під час зустрічі на початку 2015 року.²⁴ Її завданням є розвиток комунікації для пояснення політики ЄС, а також підтримка медіа-

середовища в країнах Східного партнерства. Він також аналізує та готує звіти про тенденції та наративи дезінформації та активно працює над підвищенням обізнаності про таку діяльність з боку російської держави та пов'язаних з нею суб'єктів. Це включає підтримку широкого міжнародного співробітництва та співробітництва держав-членів для обміну найкращими практиками стратегічних комунікацій та забезпечення постійного доступу до об'єктивної інформації [5, с. 23].

Іншим проектом, який варто відзначити, є багатонаціональна кампанія з розвитку потенціалу протидії гібридній війні, спільні зусилля ЄС і ряду додаткових країн, що беруть участь у цьому. Він спрямований на інформування про національну та багатонаціональну політику, сприяння співпраці та надання концептуальних вказівок щодо безпеки та оборони [6, с. 108].

Значення НТ&НВ далеко не нове, але усвідомлення та робота з включення його наслідків у політику, спроможність та реалізацію спроможності в західних демократіях набрали обертів в останні роки. Протягом останніх кількох років ряд європейських та міжнародних установ неодноразово отримували повідомлення ЗМІ про конкретні дії, наприклад, дезінформацію або операції зламування та витоку інформації, спрямовані на те, щоб змінити хід публічних дебатів або зменшити довіру до ключових суспільних акторів [7, с. 202]. У такому інформаційному середовищі легко потрапити в проблемно-орієнтоване відчуття безперервного шквалу загроз і втратити з поля зору більш витончені довгострокові події, які зміцнюють здатність реагувати та створювати стійкість до них. Безсумнівно, легше описати загрозу, спрямовану на конкретну подію чи ціль, окреслену в часі, ніж більш тонкі зміни в уряді чи суспільстві. Широкий огляд літератури щодо діяльності інформаційного впливу підкреслює, що більше відомо про методи та проведення цієї діяльності, ніж про те, як їй протистояти. Отже, давайте окреслимо кілька прикладів можливостей, які нещодавно з'явилися та є актуальними, щоб зрозуміти або зменшити наслідки гібридних загроз проти Заходу. До них належать (1) багатонаціональні організації та проекти, (2) національні урядові організації та (3) неурядові

організації.

Загалом, низка організацій, створених на Заході для протидії НТ&НВ, відображає значно підвищену обізнаність про проблему в міжнародних, національних і внутрішніх умовах. Крім того, вони також підкреслюють появу численних кооперативних та інноваційних засобів для вирішення проблем незахищеності, пов'язаних із НТ&НВ. Дійсно, безліч відповідей свідчить про дедалі динамічніший характер нинішнього середовища безпеки, в якому Захід виявляється здатним не лише реагувати на виклики антагоністів, а й виявляти та усувати власні вразливі місця в цьому відношенні. як розробка інноваційних та креативних власних контрзаходів.

Висновки і пропозиції. Таким чином, в результаті проведеного дослідження визначено аспекти концептуальних засад становлення механізмів формування алгоритмів та методів протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон. Констатовано, що виокремлення значення сірих зон є далеко не новим підходом та проблематикою, але усвідомлення та робота з включення його наслідків у політику, спроможність та реалізацію спроможності в західних демократіях набрали обертів в останні роки. Протягом останніх кількох років ряд європейських та міжнародних установ неодноразово отримували повідомлення засобів масової інформації про конкретні дії, наприклад, дезінформацію або операції зламування та витоку інформації, спрямовані на те, щоб змінити хід публічних дебатів або зменшити довіру до ключових суспільних акторів. У такому інформаційному середовищі легко потрапити в проблемно-орієнтоване відчуття безперервного шквалу загроз і втратити з поля зору більш витончені довгострокові події, які зміцнюють здатність реагувати та створювати стійкість до них. Безсумнівно, легше описати загрозу, спрямовану на конкретну подію чи ціль, окреслену в часі, ніж більш тонкі зміни в уряді чи суспільстві. Широкий огляд літератури щодо діяльності інформаційного впливу підкреслює, що до найбільш важливих методів протистояння гібридних загроз можна віднести: багатонаціональні організації та проекти, національні урядові організації та

неурядові організації.

Перспективи подальших розвідок у даному напрямі стосуються формуванню та розробленню пропозицій методологічного інструментарію методів протидії гібридним загрозам та гібридній війні у контексті визначення проблематики сірих зон.

Література

1. Марчук Є. Україна: нова парадигма поступу : аналітичне дослідження. Київ : Аваллон, 2001. 215 с.
2. Михалевська Л. Б. Кадровий потенціал органів державної влади як об'єкт наукових досліджень. *Теорія та практика державного управління і місцевого самоврядування*. 2015. № 1. С. 187-191.
3. Пуліна Т. В., Ткачук О. Ю., Вафіна А. О. Розвиток кадрового потенціалу органу публічної служби. *Економічна наука*. 2018. № 2. С. 44-49.
4. Зубар І. В., Онищук Ю. В. Практика ЄС у децентралізації публічної влади та перспективи її застосування в Україні. *Публічне управління та митне адміністрування*. № 1 (32). 2022. С. 41-45.
5. Сабурова Г. Б. Основні напрями розвитку системи публічного управління в Україні. *Публічне управління і адміністрування в Україні*. 2021. № 21. С. 23-28.
6. Нижник Н.Р., Мосов С.П. Теоретичні аспекти державного управління : монографія. Чернівці : Технодрук, 2011. 248 с.
7. Скуратівський В. Соціальна безпека українського суспільства та шляхи її забезпечення. *Вісник НАДУ*. 2011. № 3. С. 194-204.

References

1. Marchuk, E. (2001), *Ukraine: nova paradigma postupu: analitichne doslidzhennya* [Ukraine: a new paradigm of progress: analytical research], Avallon, Kiev, Ukraine.
2. Mikhalevskaya, L. B. (2015), "Personnel potential of state authorities as

an object of scientific research”, *Theory and practice of public administration and local self-government*, vol. 1, pp. 187-191.

3. Pulina, T. V. Tkachuk, O. Yu. and Vafina, A. A. (2018), “ Development of the personnel potential of the public service body ”, *Economic science*, vol. 2, pp. 44-49.

4. Zubar, I. V. and Onyshchuk, Yu. V. (2022), “EU practice in decentralization of public power and prospects for its application in Ukraine”, *Publichne upravlinnia ta mytne administruvannia*, vol. 1 (32), pp. 41-45.

5. Saburova, G. B. (2021), “The main directions of the development of the public administration system in Ukraine”, *Publichne upravlinnia i administruvannia v Ukraini*, vol. 21, pp. 23-28.

6. Nyzhnyk, N.R. & Mosov, S.P. (2011), *Teoretychni aspekty derzhavnoho upravlinnia* [Theoretical aspects of public administration], Tekhnodruk, Chernivtsi, Ukraine.

7. Skurativskyi, V. (2011), “ Social security of Ukrainian society and ways of ensuring it ”, *Visnyk NADU*, vol. 3, pp.194-204.

Стаття надійшла до редакції 15.08.2023 р.