



Типологія протидії недержавним збройним акторам

Дмитро Ю. Горіленко^{1*} • Анастасія О. Хмель²

¹ Чорноморський національний університет імені Петра Могили (Україна). Здобувач другого (магістерського) рівня вищої освіти за спеціальністю Міжнародні відносини, суспільні комунікації та регіональні студії.

² Чорноморський національний університет імені Петра Могили (Україна). Доцент кафедри міжнародних відносин та зовнішньої політики, канд. іст. наук, доцент.

* Автор-кореспондент, e-mail: dgorilenko@gmail.com

СТАТТЯ	АНОТАЦІЯ
Дослідницька DOI: 10.70651/3041-2498/2025.5.19 Авторське право © 2025 авторів  Цей твір ліцензовано на умовах Ліцензії Creative Commons «Із Зазначенням Авторства – Некомерційна 4.0 Міжнародна» (CC BY-NC 4.0). 	У сучасному світовому безпековому контексті недержавні збройні актори (НЗА) стали домінуючою силою у конфліктах, що зумовлює потребу в ефективному та скоординованому підході до їх нейтралізації. На відміну від класичних міждержавних війн, сучасні загрози є гібридними за своєю природою й охоплюють військовий, інформаційний, правовий, гуманітарний та кібернетичний виміри. Метою цього дослідження є формулювання системи стратегічних моделей протидії НЗА та пояснення їхнього застосування в міжнародній практиці з акцентом на взаємодію різних інструментів. У статті запропоновано авторську типологію з шести стратегічних моделей: військова, правова, інформаційна, гуманітарна, кібер-розвідувальна та гібридна. Кожна з них проілюстрована реальними міжнародними прикладами. Військова модель розкривається через боротьбу з ІДІЛ та підтримку України; правова – через діяльність міжнародних судів і процедур притягнення до відповідальності; інформаційна – через кампанії контрпропаганди, зокрема дії Демократичних сил Сирії проти ІДІЛ; гуманітарна – через надання допомоги цивільному населенню в Сирії, Афганістані та африканських країнах; кібер-розвідувальна – через відстеження комунікацій терористів, як у випадку операції Пентагону “Glowing Symphony”; гібридна модель інтегрує всі зазначені інструменти і проявляється у спільних діях проти Талібану або в комплексній відповіді на агресію Росії проти України. Результати дослідження засвідчили, що жодна модель не є універсальною чи самодостатньою. Найефективнішою виявляється гібридна стратегія, здатна гнучко адаптуватися до складної природи сучасних загроз. Успіх заходів протидії НЗА залежить від рівня міжнародної координації, узгодженості політичних, військових і гуманітарних дій, а також урахування локальної специфіки конфліктів. У підсумку дослідження підкреслює, що ефективна протидія НЗА вимагає багаторівневої взаємодії держав, міжнародних організацій, приватного сектору та громадянського суспільства. З огляду на зростаючу тенденцію до нестандартного характеру конфліктів, саме гібридна модель, яка поєднує безпекові та соціогуманітарні елементи, є найперспективнішою основою для формування сталої політики безпеки.

КЛЮЧОВІ СЛОВА

недержавні збройні актори (НЗА), гібридна загроза, стратегія безпеки, військова протидія, правова відповідальність, боротьба з тероризмом.



e-ISSN 3041-2498

Public Management and Policy

<https://www.eu-scientists.com/index.php/pmap>


Typology of Countering Non-State Armed Actors

Dmytro Horilenko^{1*} • Anastasiia Khmel² 

¹ Petro Mohyla Black Sea National University (Ukraine). Second (Master's) Level Higher Education Degree in International Relations, Public Communications, and Regional Studies.

² Petro Mohyla Black Sea National University (Ukraine). Associate Professor at the Department of International Relations and Foreign Policy, PhD in History, Associate Professor.

* **Corresponding Author**, e-mail: dgorilenko@gmail.com

ARTICLE INFO

ABSTRACT

Research Article

DOI:

[10.70651/3041-2498/2025.5.19](https://doi.org/10.70651/3041-2498/2025.5.19)

Copyright © 2025
by authors



This is an open access journal and all published articles are licensed under a Creative Commons Attribution—NonCommercial 4.0 International (CC BY-NC 4.0)



In the security setup of today's world, the non-state armed actors (NSAAs) have become a prevailing force in the conflict, alarm for a workable and joint set of actions for their annihilation. Unlike usual wars between states, the present dangers are more of a carry-over type that involves military, information, legal, humanitarian, and cyber warfare aspects. The paper aims to establish a working system of definitions for tactics to stop NSAAs and to explain their application in global practice, focusing on the interplay of various tools. This study presents a novel class of six strategic models, namely military, legal, informational, humanitarian, cyber-intelligence, and hybrid. Each model is backed up with international examples. The military model is corroborated by the fight against ISIS and Ukrainian support operations; the legal model captures the representation of international courts and procedures; the informational model is characterized by the counter-propaganda of ISIS through Syrian Democratic Forces (SDF), the humanitarian model is showcased by the provision of aid to people in Syria, Afghanistan, and African countries, and the cyber-intelligence model is focused on the tracking of the terrorists' communications like the "Glowing Symphony" which is a Pentagon operation; and the hybrid model combines all possible instruments to have a tactical, as demonstrated in the use of joint forces against the Taliban or the case of the complex response to Russia's aggression against Ukraine. It is discovered from the results that no single model is good for all conditions and no one model is complete. The most productive course is the hybrid one, that is adaptable depending on complex issues of contemporary threats. The degree of success of the NSAA countermeasures is measured by the effectiveness of international cooperation, harmonizing political, military, and humanitarian intervention, and the ability to touch upon the peculiarities of each conflict in the area. Ultimately, the investigation underscores that, to prevent NSAA counter-strategies, we definitely need a multilevel approach between the state, international organizations, business, and the common people. Since the nature of conflicts that more often than not move beyond the traditional ways of war, the hybrid model that addresses both the safety, and socio-humanitarian issues is more optimistic as the way of developing a security policy to continue to be sustainable.

KEYWORDS

non-state armed actors (NSAs), hybrid threat, security strategy, military counteraction, legal responsibility, counterterrorism.

1. Вступ

Недержавні збройні актори (НЗА) представляють собою широкий спектр озброєних груп, що варіюються від повстанських рухів до терористичних організацій, і мають значний вплив на стабільність як окремих держав, так і міжнародного порядку. Ці групи, які здатні організовувати і здійснювати насильницькі дії для досягнення власних цілей, не інтегровані до офіційних структур державної влади, таких як армія або суспільна безпека. Зберігаючи самостійність у прийнятті політичних і військових рішень, їхня діяльність часто стає причиною підриву суверенітету держав, поширення насильства проти мирного населення та створення перешкод для мирного врегулювання конфліктів.

Особливістю НЗА є їх здатність діяти в умовах «сірої зони», що передбачає використання поєднання традиційних військових стратегій із невійськовими методами, включаючи активне залучення інструментів інформаційного простору та розроблення кіберзагроз. Відповідно, для ефективної боротьби з такими угрупованнями потрібен всеосяжний підхід, який би дозволив мобілізувати ресурси як національних урядів, так і міжнародних організацій.

На сучасному етапі формування колективних стратегій протидії НЗА стало нагальною потребою. Такий підхід передбачає налагодження міжурядової співпраці, інтеграцію зусиль міжнародних організацій, а також залучення інших зацікавлених сторін для координації дій з нейтралізації загроз, які виходять від цих груп. У рамках цього дослідження пропонується глибший аналіз типологічних особливостей стратегічних підходів до спільної боротьби з НЗА. Розглядаються ключові моделі взаємодії та оцінюються практичні приклади їхнього застосування як у межах окремих держав, так і на міжнародній арені.

2. Огляд літературних джерел

Останні наукові дослідження стосовно боротьби з недержавними збройними акторами (НЗА) спрямовані на інтеграцію військових, гібридних та правових стратегій.

В. Раута типологізує НЗА у контексті гібридної війни, виділяючи проксі, допоміжні сили і афілійовані сили (транснаціональні злочинні мережі). Він підкреслює, що характер взаємодії з державами визначає стратегічний вплив таких груп [1].

Д. Кілаллен переосмислює класичні підходи до контрповстанської боротьби (COIN). Він критикує традиційні методи оцінки успішності (знищення противника), наголошуючи на важливості населення як ключового суб'єкта безпеки [2].

Ю. Кайпер, Б.-О. Ліннер і Г. Шредер пропонують модель «гібридного управління», де інтегруються державні та недержавні актори, наприклад, у рамках кліматичної політики. Їхній підхід можна застосувати і в безпековій сфері для посилення прозорості та підзвітності через включення місцевих громад і недержавних груп у процес врегулювання конфліктів. Водночас вони застерігають від ризиків приватизації громадської безпеки [3].

Зокрема, М. Рюле та С. Робертс підкреслюють важливість гібридного виміру сучасних загроз, де сполучені ворожі дії державних та недержавних акторів потребують комбінованого підходу, що включає військові, інформаційні та інші засоби протидії [4]. С. Хендлер у аналітичному огляді для Атлантичної ради зазначає, що НЗА дедалі активніше освоюють кіберпростір, що вимагає нових кібернетичних та розвідувальних методів контрзаходів [5]. Дослідники М. Замір та К. Каунерт розробили модель стратегічних комунікацій для протидії радикалізації, акцентуючи роль інформаційних операцій та попереднього інформування населення [6]. К. Гофманн та У. Шнекенер узагальнюють підходи до взаємодії з НЗА, пропонуючи стратегії, що варіюються від суто каральних (силове придушення, санкції) до заохочувальних (інтеграція у владні структури, програми роззброєння, демобілізації та реінтеграції — DDR) [7].

В. Фелбаб-Браун зосереджується на взаємодії між НЗА та державами, підкреслюючи, що ефективна протидія вимагає комплексного підходу, який враховує політичні, соціальні та економічні аспекти [8]. А. Мамфорд зосереджується на проксі-війнах та контрповстанських операціях, аналізуючи, як держави використовують НЗА для досягнення своїх цілей. Він також досліджує вплив таких стратегій на міжнародну безпеку та стабільність [9]. Дж. Форест вивчає вплив соціальних медіа на сучасні конфлікти, підкреслюючи, що НЗА активно використовують цифрові платформи для вербування, пропаганди та координації дій. Він також аналізує, як держави можуть протидіяти цим загрозам [10].

3. Постановка завдання

Метою дослідження є обґрунтування ефективності колективної багатовимірної відповіді на дії недержавних збройних акторів шляхом систематизації стратегічних підходів до їх протидії. У межах роботи пропонується здійснити глибокий аналіз семи основних стратегій: військової, правової, політичної, інформаційної, гуманітарної, кібер-розвідувальної та гібридної. Основна увага приділяється узагальненій класифікації цих підходів у рамках цілісної системи. Для кожного зі стратегічних підходів пропонується визначити ключові характеристики, опираючись на конкретні приклади з практики, як-от військові операції, укладання мирних угод чи проведення інформаційних кампаній. Важливо розглянути їхні сильні та слабкі сторони, а також оцінити роль кооперації та колективної взаємодії у досягненні бажаних результатів. Результати порівняння дозволяють зробити висновки щодо ефективності застосування гібридного підходу як інтеграційної стратегії.

4. Методи та матеріали

Методологічна основа дослідження базується на поєднанні кількох теоретичних та емпіричних підходів, що забезпечують системне і глибоке розуміння сучасних стратегій протидії недержавним збройним акторам (НЗА). Ключовими методами у рамках дослідження виступають порівняльний аналіз стратегій, кейс-стаді та аналіз нормативно-правових і політичних джерел.

Порівняльний аналіз стратегій використовується для систематизації та оцінки ефективності основних моделей протидії НЗА. Він дає змогу порівняти військові, політико-дипломатичні, правові, інформаційні, гуманітарні та гібридні стратегії за такими критеріями: досягнення безпекових цілей, легітимність дій, рівень міжнародної залученості, вплив на цивільне населення, стійкість результатів тощо. Це дозволяє виявити структурні сильні та слабкі сторони кожного підходу і визначити умови, за яких їх використання є найбільш ефективним.

Метод контент-аналізу застосовується для обробки великого обсягу документальних матеріалів, зокрема резолюцій ООН, звітів міжнародних організацій, аналітичних досліджень та статей у профільних академічних виданнях. Завдяки цьому методу вдається визначити частоту згадувань окремих стратегій у міжнародному дискурсі, підкреслити ключові акценти в підходах до НЗА та відстежити зміни у риторичі щодо їхньої ролі в конфліктах.

Індуктивно-дедуктивний метод використовується при створенні типології підходів до протидії НЗА. Зокрема, через узагальнення емпіричних кейсів (індукція) формуються загальні висновки про ефективність інтегрованих стратегій (дедукція). Це сприяє розкриттю логіки функціонування кожної стратегії та формулюванню аналітичних висновків щодо доцільності їхньої сумісності та інтеграції.

Метод системного аналізу дозволяє досліджувати взаємозв'язки між різними інструментами протидії — військовими, правовими, гуманітарними, інформаційними — як частинами єдиної гібридної стратегії. Значна увага приділяється взаємодії між компонентами, наприклад, як військові операції впливають на гуманітарні потреби чи як правові заходи впливають на легітимність військових дій. Аналіз нормативно-правових і політико-інституційних джерел став основою для дослідження інституційного забезпечення стратегій протидії НЗА.

5. Результати та обговорення

В умовах зростаючої ролі недержавних збройних акторів (НЗА) у сучасних збройних конфліктах розробка ефективних стратегій їх нейтралізації стала нагальною потребою. Спираючись на всебічний аналіз нормативних, аналітичних та емпіричних джерел, це дослідження пропонує оригінальну типологію стратегічних підходів до колективної протидії НЗА. Типологія охоплює сім концептуальних моделей: військову, правову, політичну, інформаційну, гуманітарну, кібер-розвідувальну та гібридну. Кожна з моделей характеризується переважним використанням певного інструментарію — від силових до дипломатичних чи цифрових засобів. Водночас дослідження підтверджує, що жоден із підходів не є ефективним сам

по собі; лише інтегроване застосування кількох моделей забезпечує сталі й результативні результати.

Військовий підхід

Військова модель передбачає пріоритетне використання сили з метою нейтралізації НЗА. Ґрунтуючись на класичній доктрині безпеки, цей підхід передбачає розгортання військових засобів — сухопутних військ, авіаційної підтримки та підрозділів спеціального призначення — окремими державами або коаліціями для знищення оперативного потенціалу недержавних груп, усунення їхнього керівництва та відновлення контролю над територіями. Яскравим прикладом цієї моделі є Глобальна коаліція проти «Ісламської держави» (ІДІЛ), створена у 2014 році під керівництвом США. До коаліції увійшли понад 70 держав (зокрема всі країни НАТО та більшість членів ЄС), які брали участь у бойових операціях в Іраку (за згодою іракського уряду) та в Сирії (без згоди режиму Асада) [11]. Згідно з офіційними звітами Коаліції, до кінця 2017 року ці дії дозволили звільнити приблизно 7,5 мільйонів осіб і суттєво зменшити територіальний контроль ІДІЛ [11].

Іншим показовим прикладом є Міжнародні сили сприяння безпеці (ISAF) в Афганістані — операція під проводом НАТО, що тривала з 2001 до 2014 року. Понад 40 країн взяли участь у спільній боротьбі проти «Талібану» та пов'язаних з ним груп. Ці приклади демонструють переваги військового підходу: швидке знешкодження ворожих груп, стримування подальшої агресії та демонстрація рішучості міжнародної спільноти. Водночас ця модель має суттєві обмеження. Збройні інтервенції часто призводять до значних жертв серед цивільного населення та руйнування інфраструктури, що може спричинити гуманітарні кризи і сприяти подальшій радикалізації місцевого населення. Тому успіх військових операцій тісно пов'язаний із паралельними зусиллями у сфері миробудування та стабілізації постконфліктних територій.

Більше того, хоча військовий підхід може бути необхідним для оперативного придушення загроз, сам по собі він не гарантує довготривалого миру. Знищення бойовиків не усуває першопричин виникнення НЗА і часто, навпаки, сприяє їхній адаптації та еволюції. Наприклад, після масштабних військових операцій армії Нігерії у 2015–2016 роках, угруповання «Боко Харам» втратило контроль над значними територіями. Проте вже до кінця 2018 року воно перейшло до партизанської та терористичної тактики, і кількість атак знову зросла [12]. Подібно до цього, попри територіальну поразку, ІДІЛ продовжувала діяти як децентралізована терористична мережа, що надихала й координувала атаки по всьому світу.

Більшість військових аналітиків сходяться на думці, що виключно силове придушення повстанських рухів не здатне забезпечити стійке політичне врегулювання. Отже, військову складову слід розглядати лише як один із елементів ширшої стратегічної рамки, яка обов'язково має включати також правові, політичні та інші інструменти.

У багатьох державах було ухвалено спеціальні закони, спрямовані на покарання терористичної та повстанської діяльності, визначення відповідальності за участь у таких організаціях, розширення повноважень правоохоронних органів у протидії загрозам, що походять від цих груп, та інші подібні заходи. Наприклад, Закон України «Про боротьбу з тероризмом» № 638-IV, ратифікований 20 березня 2003 року, визначає правові та організаційні засади боротьби з тероризмом, створює Антитерористичний центр при Службі безпеки України (СБУ), а також регламентує проведення антитерористичних операцій і координацію між суб'єктами боротьби з тероризмом [13]. На підставі цього закону була розпочата спеціальна військова операція проти незаконних збройних формувань на сході України — Антитерористична операція (АТО). Законодавства багатьох інших держав мають схожі положення. Так, після терактів 11 вересня 2001 року Конгрес США ухвалив низку законодавчих актів (зокрема Patriot Act), які фактично розширили повноваження уряду у виявленні та запобіганні терористичній діяльності. Серед інших національних правових інструментів — заборона екстремістських організацій, заморожування їхніх активів, спрощені процедури екстрадиції осіб, причетних до тероризму тощо. Суть цих заходів полягає в їхній скоординованості: коли більшість або всі держави впроваджують подібні норми, представники недержавних збройних угруповань втрачають можливість укриватися в країнах із лояльною юрисдикцією.

На глобальному рівні головна увага приділяється діяльності Ради Безпеки ООН через її резолюції, міжнародні договори та санкційні механізми. Поштовхом до активізації зусиль стало

ухвалення Резолюції РБ ООН 1373 (2001) невдовзі після подій 11 вересня. Прийнята на підставі Глави VII Статуту ООН, вона зобов'язала всі держави-члени криміналізувати фінансування тероризму та інші форми його підтримки, заморожувати відповідні активи, не надавати притулок терористам, а також активно співпрацювати в обміні розвідувальною інформацією та притягненні терористів до відповідальності [14]. На виконання положень цієї резолюції держави гармонізували своє законодавство, а при Раді Безпеки було створено Комітет з боротьби з тероризмом для моніторингу імплементації.

ООН також запровадила адресні санкції проти окремих недержавних акторів. Початком стало ухвалення Резолюції 1267 (1999), якою були запроваджені санкції проти руху «Талібан», а згодом — проти мережі «Аль-Каїда» та пов'язаних з нею осіб і структур. Санкційний комітет, спочатку відомий як Комітет 1267, згодом був розширений відповідно до Резолюцій 1989 (2011) та 2253 (2015), і веде консолідований список осіб та організацій, пов'язаних з терористичною діяльністю, щодо яких застосовуються такі заходи: замороження активів, заборона на подорожі та ембарго на постачання зброї [15].

До глобальних правових заходів належать і численні міжнародні конвенції, зокрема: Міжнародна конвенція про боротьбу з фінансуванням тероризму (1999), Конвенція проти захоплення заручників (1979), Конвенція ООН проти транснаціональної організованої злочинності (2000) тощо. Ці договори формують єдині правові стандарти, яких зобов'язані дотримуватися держави-учасниці, включно з криміналізацією терористичних дій та співпрацею в екстрадиції правопорушників.

Особливої уваги в контексті недержавних збройних акторів заслуговує міжнародне гуманітарне право (МГП). На відміну від контртерористичних заходів, МГП має на меті обмеження жорстокості під час збройних конфліктів, навіть якщо в них беруть участь недержавні суб'єкти. Додатковий протокол II (1977 року) до Женевських конвенцій 1949 року щодо захисту жертв міжнародних збройних конфліктів став першим міжнародно-правовим актом, що визначив зобов'язання для повстанців і НЗА, які беруть участь у внутрішніх конфліктах [16]. Протокол зобов'язує гуманно поводитися з особами, які більше не беруть участі в бойових діях (поранені, полонені, цивільні), та забороняє тортури, колективні покарання, захоплення заручників і терор щодо цивільного населення.

Попри те, що недержавні збройні актори не є рівноправними суб'єктами міжнародного права й не підписують Женевські конвенції, міжнародна правова практика визнає їх зобов'язаними дотримуватися основоположних гуманітарних норм. З метою заохочення дотримання цих норм міжнародні організації (наприклад, Міжнародний комітет Червоного Хреста) ведуть діалог із лідерами збройних груп. Паралельно діють і механізми притягнення до відповідальності: наприклад, Міжнародний кримінальний суд може судити осіб, винних у воєнних злочинах і злочинах проти людяності — незалежно від того, є вони представниками держави чи недержавного утворення.

Таким чином, правовий підхід є багатоаспектним: він охоплює і каральні заходи (правосуддя, санкції), і превентивні (угоди про екстрадицію, контроль за фінансами), і нормативні (встановлення правил поведінки у конфліктах).

Політичний підхід

Політична модель є одним із підходів, який зосереджується переважно на мирних переговорах, укладанні угод та вирішенні політичних причин конфлікту. Ця стратегія ґрунтується на припущенні, що більшість недержавних збройних акторів (НЗА) мають політичні цілі або ідеології (наприклад, самоврядування, автономія, зміна режиму тощо), і що застосування лише військової сили без розв'язання цих вимог матиме незначний або зовсім нульовий ефект. Навпаки, залучення поміркованих лідерів НЗА до діалогу, реабілітація колишніх бійців через мирний політичний процес і публічне зобов'язання щодо дотримання демократичних принципів можуть сприяти трансформації конфлікту з військової у політичну площину.

Успішне застосування політичної стратегії продемонстроване в численних мирних процесах між урядами та повстанцями у різних частинах світу. Однією з найвідоміших подій є мирна угода 2016 року в Колумбії між урядом і Револьюційними збройними силами Колумбії (FARC), яка завершила майже 50-річний збройний конфлікт. Надання урядом гарантій для початку переговорного процесу дало керівництву FARC можливість скласти зброю, припинити збройну боротьбу та перетворитися на легальну політичну партію. Ця угода нейтралізувала

найбільше партизанське формування Західної півкулі: уряд Колумбії підтвердив, що понад 13 000 бійців FARC були роззброєні та демобілізовані [18]. Угода також вирішила структурні проблеми конфлікту, такі як розподіл землі та брак державного контролю в сільських регіонах, шляхом розширення сільської інфраструктури та політичного залучення колишніх повстанців. Вона інституціоналізувала колишніх бійців, тим самим ліквідуючи підґрунтя для збройного протистояння. Це типовий приклад ситуації, коли політичні рішення та поліпшення економічних умов можуть призвести до справедливого та мирного суспільства.

Політичний підхід до розв'язання конфліктів у різних умовах виявляється у формі домовленостей або перемир'їв. Наприклад, програми з роззброєння, демобілізації та реінтеграції (DDR) залишаються ключовими елементами мирних процесів у Сьєрра-Леоне, Ліберії, Афганістані та інших країнах. Міжнародні посередники, зокрема ООН або регіональні організації, зазвичай відіграють провідну роль у переговорах з НЗА, яких раніше вважали винятково терористами, наприклад, деякі угруповання Талібану до 2020 року.

Прикладом ефективної дипломатії є формат 6+1 для діалогу з Талібаном або зустрічі в Досі, які засвідчили, що потужний міжнародний тиск може змусити навіть радикальні рухи сісти за стіл переговорів. Однак кінцевий результат значною мірою залежить від щирості сторін і надійності гарантій. У випадку з Талібаном угода 2020 року з США сприяла виведенню військ, але мир виявився недовговічним: уряд Афганістану був недостатньо залучений, а Талібан, скориставшись нагодою, захопив владу у 2021 році. Експерти застерігають, що мирні переговори можуть перетворитися на «продовження війни іншими засобами», якщо угода лише відкладає новий виток насильства без усунення глибинних причин конфлікту [19].

Таким чином, політичний підхід є найефективнішим у поєднанні з іншими методами. З одного боку, військовий тиск змушує НЗА до переговорів; з іншого — юридичні гарантії, як-от амністії або, навпаки, загроза кримінального переслідування, стимулюють до компромісу. А підтримка міжнародної спільноти сприяє наданню ресурсів для повоєнного відновлення. Найбільшим викликом залишається політичний діалог з терористами, мотивованими радикальною ідеологією (як-от ІДІЛ або Аль-Каїда), оскільки з ними майже неможливо домовитися. Водночас, якщо першопричина конфлікту — політична (наприклад, автономія чи міжетнічне протистояння), єдиним рішенням є інклюзивні домовленості між спільнотами, представленими НЗА, що можуть призвести до сталого миру. Політична інтеграція колишніх бійців, перехід від війни до миру — основна мета цього підходу.

Інформаційний підхід

Інформаційна модель протидії зосереджується на впливі на суспільну свідомість і настрої – нейтралізації пропаганди НЗА, захисті населення від їхньої маніпулятивної дії та підтримці бойовиків шляхом руйнування їхніх ідеологічних наративів. У добу інформаційних технологій і соціальних мереж цей фронт боротьби набув надзвичайної ваги. Багато недержавних угруповань надають великого значення стратегії в медіа та ЗМІ. Яскравим прикладом є діяльність ІДІЛ, яка шокувала світ професійно змонтованими відео страт, онлайн-журналами та активністю у соцмережах, завдяки чому їм вдалося завербувати понад 20 000 іноземних бойовиків. ІДІЛ активно використовувала онлайн-платформи для просування своєї ідеології та залучення прибічників, ставши прикладом інформаційної війни [19]. Тому боротьба з НЗА неминує включати елементи контрпропаганди та стратегічних комунікацій.

На державному рівні реалізуються колективні зусилля у співпраці з приватним сектором і громадянським суспільством. У 2015 році було створено Глобальний центр протидії екстремістській ідеології за участі національних урядів і ІТ-компаній. Серед його завдань – моніторинг і видалення терористичного контенту з інтернету та просування альтернативних наративів. Такі платформи, як Facebook, Twitter та YouTube, у взаємодії з правоохоронними органами посилили модерацію, видаливши тисячі акаунтів ІДІЛ та Аль-Каїди, які поширювали заклики до насильства [20]. Одночасно були запущені кампанії контрнاراتивів: мусульманські громади за підтримки держав створювали ініціативи для спростування джихадистської ідеології на основі автентичного релігійного дискурсу. У регіонах, де діє Боко Харам, місцеві лідери думок і духовенство проводять роботу для дискредитації гасел бойовиків і проповіді мирних цінностей.

Ще один напрям інформаційної протидії – викриття дезінформації та воєнних злочинів НЗА. Наприклад, у 2022 році Державний департамент США опублікував звіт, що викриває участь

ПВК «Вагнер» у злочинах в Африці, спростовуючи російську пропаганду про їхню «миротворчу» роль [21]. Подібні дії дискредитують НЗА в очах міжнародної спільноти та унеможливають їх легітимізацію. У контексті гібридної агресії РФ проти України було створено Центр протидії дезінформації, що займається викриттям фейків, ворожої пропаганди й мови ворожнечі. НАТО й ЄС, усвідомлюючи ключову роль інформаційної безпеки, інвестують у підрозділи стратегічних комунікацій.

Головна мета інформаційного підходу – позбавити НЗА підтримки населення, зменшити приплив нових бойовиків і симпатиків, а також сформувати негативне сприйняття таких акторів. Це досягається не лише правдивим інформуванням про наслідки їхніх дій (теракти, насильство), а й поширенням позитивної альтернативи – миру, розвитку, а також «цифровою гігієною», тобто обмеженням доступу бойовиків до інформаційного простору. Звісно, обмеження в межах інформаційних кампаній не повинні суперечити свободі слова та правам людини. Але у випадку терористичних матеріалів у багатьох країнах передбачені жорсткіші заходи, як-от блокування сайтів або кримінальне покарання за публічне виправдання тероризму. На глобальному рівні важливо ділитися методиками та зібраними даними: у 2016 році, наприклад, спецслужби різних держав координували відстеження активності ІДІЛ в інтернеті, що допомогло запобігти низці атак. Водночас лише інформаційною кампанією перемогти екстремізм неможливо: необхідно супроводжувати військове визволення територій інформуванням населення про позитивні зміни та запобігати поверненню пропагандистів. Лише так перемога на полі бою буде закріплена й в інформаційній сфері.

Гуманітарний підхід

Один із методів протидії недержавним збройним акторам у межах гуманітарної моделі базується на комунікації з місцевим населенням і подоланні соціально-економічних причин конфлікту. Її основне твердження полягає в тому, що, позбавивши такі угруповання масової підтримки шляхом усунення страждань і потреб, які вони використовують для вербування, ситуація не загострюватиметься. Терористичні й повстанські рухи зазвичай виникають у регіонах, де бракує базових благ, порушується закон, існує міжобщинна ворожнеча, або де держава відсутня чи проводить дискримінаційну політику. Гуманітарна парадигма покликана заповнити цей вакуум – надати допомогу, захист і дружню альтернативу владі бойовиків.

Наприклад, практична реалізація цієї моделі включає створення різних форм підтримки (економічної, фінансової тощо) для жителів громад паралельно з військовими або поліцейськими операціями. Під час війни з ІДІЛ, зокрема, неурядові організації та деякі країни коаліції надавали мешканцям звільнених від бойовиків районів масштабну гуманітарну допомогу – воду, їжу, медичні послуги та відновлення інфраструктури, тобто задовольняли базові потреби людей. Це знижувало ймовірність того, що місцеві жителі розчаруються і почнуть симпатизувати екстремістам. У період місії НАТО в Афганістані зусилля були зосереджені на будівництві шкіл, підтримці фермерів та покращенні сільського життя – саме ці заходи сприяли зменшенню соціальної бази «Талібану». В Африці уряди за підтримки ООН реалізовували програми порятунку дітей-солдатів, навчання молоді та створення для них можливостей працевлаштування в районах, де діють угруповання Boko Haram або Аль-Шабаб, щоб не допустити втягування молоді у збройні формування.

Зазвичай гуманітарні зусилля здійснюються в партнерстві з міжнародними організаціями, такими як Червоний Хрест чи Всесвітня продовольча програма, які виступають як нейтральні сторони. Наприклад, Червоний Хрест вів перемовини з деякими НЗА щодо доступу до заручників чи вакцинації дітей у районах, контрольованих бойовиками. Такі дії мали гуманітарний характер і сприяли зниженню ворожнечі між сторонами.

Гуманітарна модель також передбачає соціальну реабілітацію колишніх бойовиків. У таких країнах, як Саудівська Аравія, Нігерія та Чад, були створені центри, де колишні учасники НЗА проходили ідеологічну переорієнтацію, отримували психологічну допомогу та професійну підготовку. За підтримки родин і громади багато з них успішно поверталися до мирного життя. Звісно, не всі програми реінтеграції є успішними, але сама готовність суспільства до прощення і прийняття є важливим сигналом і знижує привабливість насильницького екстремізму.

Гуманітарний підхід тісно пов'язаний із концепцією «відповідальність захищати»: якщо держава не здатна забезпечити безпеку своїм громадянам, міжнародна спільнота повинна взяти на себе відповідальність і надати допомогу. При цьому не варто вважати, що гуманітарними

заходами можна роззброїти бойовиків – це завдання силового реагування. Проте гуманітарні дії здатні підірвати соціальну базу підтримки екстремістів і зменшити потік новобранців.

Практика показала: там, де після військових дій швидко відновлюють нормальне життя та справедливість, недержавні збройні актори більше не повертаються. Навпаки, такі проблеми, як масове безробіття і міжрелігійні конфлікти, як у післявоєнному Іраку 2000-х років, призводили до нових хвиль насильства. Тому сучасні міжнародні миротворчі місії мають поєднувати військові й гуманітарно-розвиткові інструменти.

Один із головних принципів сучасної стратегії полягає в тому, що розвиток є невід’ємним елементом колективної безпеки – це два боки однієї медалі.

Кібер-розвідувальний підхід

Кібер-розвідувальна модель протидії недержавним збройним акторам (НЗА) базується на використанні можливостей кіберпростору та розвідувальних технологій для передбачення і ліквідації загроз. У цифрову епоху терористичні та повстанські мережі не лише адаптувалися до нових умов, але й активно використовують інтернет, шифрування, криптовалютні транзакції, дрони та інші передові технології. У відповідь держави спільно розробляють інструменти кіберборотьби: кібероперації проти інфраструктури НЗА, розвідка на основі великих масивів даних для виявлення змов, технічне спостереження та точкове знищення командних центрів бойовиків.

Яскравим прикладом стала секретна операція США 2016 року під назвою “Glowing Symphony” – перша масштабна наступальна кіберкампанія Пентагону проти ІДІЛ. Об’єднана група кібервійськ Joint Task Force ARES зламала сервери та акаунти, які відповідали за медіапропаганду ІДІЛ, видалила контент і порушила комунікації бойовиків [22]. У результаті онлайн-мережу ісламістів було паралізовано, що унеможливило координацію та вербування. Аналогічні дії здійснювали кіберпідрозділи армій провідних країн, націлюючись на фінансові канали терористів і відстежуючи переміщення коштів і зброї.

Розвідка залишається вирішальною складовою: технічні засоби (прослуховування, безпілотники, супутники) дають змогу виявляти табори НЗА та місцезнаходження їхніх лідерів. Спільні розвідувальні центри, як-от Коаліційний розвідувальний центр проти ІДІЛ у Йорданії, використовують дані з багатьох країн для створення повної картини діяльності терористичних мереж. Завдяки цьому за останні роки було проведено точкові удари, які призвели до ліквідації ключових фігур — від Усами бен Ладена (Аль-Каїда) до Абу Бакра аль-Багдаді (ІДІЛ) — з мінімальними супутніми втратами. Ключову роль у цих операціях відіграють кібер- та космічні технології.

Втім, кібер-розвідувальний підхід включає не лише наступальні дії, а й захист власної критичної інфраструктури від кібератак НЗА. Терористи можуть намагатися атакувати об’єкти інфраструктури (наприклад, енергетичні чи транспортні) через кіберпростір. У зв’язку з цим у межах колективної безпеки країни НАТО та ЄС створили механізми обміну інформацією про кіберзагрози та проводять спільні навчання з кіберзахисту. Зазвичай держави укладають угоди з приватними компаніями, які мають цінні масиви даних та експертизу.

Кібер-розвідувальна модель здебільшого застосовується конфіденційно, головним чином для запобігання терактам. Попри її неопублічність, її ефективність засвідчено численними випадками зірваних терактів. Наприклад, за даними уряду США, з 2001 року було попереджено понад 50 масштабних терактів завдяки глобальному моніторингу комунікацій терористів. У Європі після 2015 року саме завдяки стеженню за соціальними мережами вдалося оперативно виявити осередки ІДІЛ ще до того, як вони змогли реалізувати свої злочинні плани [23].

Ця модель допомагає зберегти баланс між безпекою та приватністю громадян і не перетинає межу, яка гарантує людям свободу від переслідувань. Однак щодо злочинних структур немає сумнівів: вони діють поза законом, а отже, держави мають повне право застосовувати кіберзасоби для їх нейтралізації.

Гібридний підхід

Гібридна модель є більш всеосяжним і широким підходом. Вона об’єднує всі раніше згадані інструменти в єдину стратегію колективної відповіді. Фактично, це підхід, що охоплює весь спектр діяльності з боку збройних сил, дипломатів, поліції, розвідки, гуманітарних організацій,

ЗМІ та інших суб'єктів як на національному, так і на міжнародному рівнях з метою досягнення спільної мети — нейтралізації недержавних збройних акторів (НЗА).

Подібна гібридна стратегія виникла у відповідь на гібридні загрози, в межах яких супротивники одночасно діють у військовій, інформаційній, юридичній та інших сферах. Відповідно, ефективна протидія цим загрозам також має бути багатовимірною та скоординованою.

На практиці елементи гібридної війни спостерігаються в багатьох сучасних операціях проти НЗА. Яскравим прикладом є діяльність Глобальної коаліції проти ІДІЛ, яка реалізовувала не лише військові дії, а й створювала спеціалізовані суди для злочинців ІДІЛ, проводила медіакампанії з делегітимації «халіфату», надавала гуманітарну допомогу звільненому населенню та здійснювала кібероперації для знищення пропагандистських ресурсів. Такий «всеохоплюючий підхід» дозволив не лише досягти військової перемоги, а й утримувати ситуацію під контролем.

Ще один приклад — спільна стратегія щодо Талібану, яка поєднувала 20-річну місію НАТО, політичні зусилля з розбудови державних інституцій, гуманітарну допомогу населенню та комунікаційні кампанії на підтримку прав жінок та освіти. Хоча очікування щодо Афганістану не справдилися, цей досвід наочно показав необхідність кращої координації дій і врахування локального контексту в гібридних стратегіях.

Для України гібридний підхід є надзвичайно актуальним. Російська агресія в Криму та на Донбасі потребувала не лише військової оборони, а й дипломатичного тиску на РФ, міжнародно-правових позовів, інформаційної боротьби з російською пропагандою та підтримки цивільного населення. Саме завдяки таким скоординованим зусиллям багатьох країн (включно з санкціями проти агресора, військовою допомогою Україні, резолюціями ООН про невизнання анексії тощо) вдалося стримати подальшу експансію.

Починаючи з 2015 року, НАТО ухвалило окрему стратегію протидії гібридним загрозам, і відтоді активно розширює свої інструменти реагування. Це означає, що у разі появи нового «гібридного» НЗА (наприклад, найманців, яких підтримує іноземна держава), Альянс зможе відповісти на загрозу гібридними засобами — від військового стримування до викриття зовнішнього спонсора на міжнародній арені [24].

Однією з ключових переваг гібридного підходу є його гнучкість та всеохопність. Він дозволяє чинити тиск на противника з різних напрямків: якщо не діє авіація — спрацьовує судовий позов або інформаційна кампанія. Більшість НЗА, які пристосовуються до одного типу загроз, виявляються вразливими до іншого. Наприклад, якщо бойовики ховаються серед цивільного населення, щоб уникнути ударів, їх все одно можна виявити завдяки фінансовій розвідці або ізолювати пропагандистськи.

Крім того, перевагою гібридної стратегії є ефективний розподіл ресурсів: вони спрямовуються туди, де потрібні найбільше саме в конкретний момент — надання гуманітарної допомоги під час перемир'я, або мобілізація військових сил у випадку ескалації.

6. Висновки

Дослідження доводить, що ефективна протидія недержавним збройним актором (НЗА) можлива лише за умови колективного і комплексного підходу, який інтегрує різні стратегічні моделі. Аналіз семи основних підходів – військового, правового, політичного, інформаційного, гуманітарного, кібер-розвідувального і гібридного – демонструє їхню значущість для загальної стратегії, але жоден окремо не забезпечує успіху.

Військовий підхід необхідний для фізичного усунення бойовиків, але без політичного вирішення конфлікт може поновитися. Правові заходи створюють механізми невідворотності покарання та міжнародної ізоляції терористів, хоча для їхньої реалізації потрібна підтримка силових структур. Політичні рішення дозволяють завершити затяжні війни через інтеграцію колишніх повстанців у мирне життя, однак вимагають гарантій безпеки та справедливості. Інформаційні методи знижують вплив екстремістської ідеології та захищають населення від пропаганди, але їхня ефективність залежить від поліпшення якості життя громадян. Гуманітарна допомога усуває причини суспільної підтримки НЗА, демонструючи турботу держави та міжнародних організацій, однак вона не може замінити силових заходів проти найрадикальніших елементів. Кібер-розвідка і застосування інноваційних технологій

дозволяють випереджати ворога і руйнувати його інфраструктуру, хоча їхня діяльність має бути узгоджена з правовими нормами, аби уникнути шкоди для цивільних.

Найбільш перспективним виявився гібридний підхід, що поєднує всі згадані елементи. Він враховує багатовимірність сучасних загроз і дозволяє досягати стійкого миру: коли воєнна перемога підкріплюється політичними домовленостями, правосуддям, відновленням інфраструктури та зміною суспільних настроїв.

Практична цінність дослідження полягає у формуванні типології стратегій безпеки, яка стає основою для розробки державної та міжнародної політики. Чітке розуміння ролі кожного компонента (силового, правового, дипломатичного тощо) дає змогу урядам та міжнародним організаціям ефективніше координувати дії у протидії тероризму й іншим видам нелегального насильства. Для України дослідження наголошує на необхідності продовжувати інтеграцію військових, правоохоронних та інформаційних зусиль у боротьбі з гібридними загрозами з боку російсько-сепаратистських угруповань як на національному рівні, так і за допомогою міжнародних партнерів.

Подальші дослідження мають бути спрямовані на оптимізацію структури та механізмів координації багаторівневої відповіді. Є потреба у визначенні найбільш доцільного розподілу ресурсів між різними напрямками протидії для досягнення максимального ефекту з мінімальними витратами та ризиками. Корисним буде більш детальне вивчення невдалих або частково успішних прикладів стратегій: виявлення ключових факторів провалу, таких як: суперечності між союзниками, брак мандатів у міжнародних організаціях чи інформаційні помилки. Загалом висновки підтверджують важливість єдиної і координованої протидії сучасним НЗА. Коли світова спільнота діє спільно і комплексно, навіть найсерйозніші терористичні чи повстанські угруповання можуть бути нейтралізовані, а регіони повернуті до мирного розвитку.

References

1. Rauta, V. (2019). Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs*, 33(6), 868–887. <https://doi.org/10.1080/09557571.2019.1656600>
2. Kilcullen, D. (2014). Counterinsurgency: theory and reality. *E-International Relations*. <https://www.e-ir.info/2014/02/26/review-counterinsurgency/>
3. Kuyper, J. W., Linnér, B. O., & Schroeder, H. (2018). Non-state actors in hybrid global climate governance: Justice, legitimacy, and effectiveness in a post-Paris era. *Environmental Politics*. <https://docslib.org/download/3209190/non-state-actors-in-hybrid-global-climate-governance-justice-legitimacy-and-effectiveness-in-a-post-paris-era>
4. Rühle, M., & Roberts, C. (2021). Enlarging NATO's toolbox to counter hybrid threats. *NATO Review*. <https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>
5. Handler, S. (2022). The 5x5—Non-state armed groups in cyber conflict. *Atlantic Council*. <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/>
6. Zamir, M., & Kaunert, C. (2025). Radicalisation and Counter-Terrorism—Reviewing the Problems in Strategic Communications Role in Counter-Terrorism. In *Strategic Communications' Role in Counter-Terrorism: The Power of Counter-Narratives* (pp. 11-63). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89110-6_2
7. Hofmann, C., & Schneckener, U. (2011). Engaging non-state armed actors in state- and peace-building: options and strategies. *International Review of the Red Cross*, 93(883), 603–621. <https://doi.org/10.1017/S1816383112000148>
8. Felbab-Brown, V. (2023). Nonstate armed actors in 2023: Persistence amid geopolitical shuffles. *Brookings Institution*. <https://www.brookings.edu/articles/nonstate-armed-actors-in-2023-persistence-amid-geopolitical-shuffles>
9. Mumford, A. (2013). Proxy Warfare and the Future of Conflict. *The RUSI Journal*, 158(2), 40–46. <https://doi.org/10.1080/03071847.2013.787733>
10. Forest, J. J. (2021). *Digital influence warfare in the age of social media*. Bloomsbury Publishing USA. <https://jamesforest.com/wp-content/uploads/2021/05/Ch1-Digital-Influence-Warfare.pdf>

11. United Nations Security Council. (2016). *Resolution 2261 (2016)* [on establishment of a political mission in Colombia to monitor the ceasefire]. U.N. Doc S/RES/2261(2016). [https://undocs.org/S/RES/2261\(2016\)](https://undocs.org/S/RES/2261(2016))
12. Brechenmacher, S. (2019). Stabilizing Northeast Nigeria after Boko Haram. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/2019/05/03/stabilizing-northeast-nigeria-after-boko-haram-pub-79042>
13. Verkhovna Rada of Ukraine. (2003, March 20). *Law of Ukraine on combating terrorism No. 638-IV*. <https://zakon.rada.gov.ua/go/638-15>
14. United Nations Security Council. (2001). *Resolution 1373 (2001)* [Counter-terrorism]. U.N. Doc S/RES/1373(2001). [https://undocs.org/S/RES/1373\(2001\)](https://undocs.org/S/RES/1373(2001))
15. United Nations Security Council. (1999). *Resolution 1267 (1999)* [on sanctions against the Taliban and Al-Qaida]. U.N. Doc S/RES/1267(1999). [https://undocs.org/S/RES/1267\(1999\)](https://undocs.org/S/RES/1267(1999))
16. International Committee of the Red Cross. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*. Adopted 8 June 1977, entered into force 7 Dec 1978. https://zakon.rada.gov.ua/go/995_200
17. Fritz, J. (2013). Counterinsurgency is not the problem. *War on the Rocks*. <https://warontherocks.com/2013/08/counterinsurgency-is-not-the-problem/>
18. Isacson, A. (2021). A long way to go: Implementing Colombia's peace accord after five years. *Washington Office on Latin America*. <https://www.wola.org/analysis/a-long-way-to-go-implementing-colombias-peace-accord-after-five-years/>
19. Cordesman, A. (2020). Afghanistan: The peace negotiations have become an extension of war by other means. *Center for Strategic and International Studies*. <https://www.csis.org/analysis/afghanistan-peace-negotiations-have-become-extension-war-other-means>
20. Steinbach, M. (2016). ISIL online: Countering terrorist radicalization and recruitment on the internet and social media. *FBI National Security Branch*. <https://www.fbi.gov/news/speeches-and-testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media->
21. BBC News. (2023). What is Russia's Wagner group, and why is the UK banning it? *BBC*. <https://www.bbc.com/news/world-60503037>
22. Brown, D. (2019). How the U.S. hacked ISIS. *NPR*. <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>
23. NATO. (2024). Countering terrorism. *NATO*. https://www.nato.int/cps/uk/natohq/topics_77646.htm
24. United Nations. (2006). *United Nations Global Counter-Terrorism Strategy* [Resolution A/RES/60/288]. <https://docs.un.org/en/A/RES/60/288>