УДК 327.56:355.4 DOI 10.17721/2415-88IX.2025.99.263–275

Горбатенко Володимир Павлович
Доктор політичних наук, професор, провідний науковий співробітник відділу конституційного та муніципального права Інститут держави і права імені В. М. Корецького НАН України (м. Київ, Україна)
https://orcid.org/0000-0002-2400-954X
e-mail: stateandlaw@ukr.net

ЕСКАЛАЦІЯ ГІБРИДНОЇ ВІЙНИ: НОВІТНІ ВИКЛИКИ І ЗАСОБИ ПРОТИДІЇ

Резюме

Розглянуто перспективи гібридної війни на тлі цивілізаційного розвитку. Виявлено новітні виклики, пов'язані з удосконаленням технологій гібридної війни та загостренням протистояння політичних сил у сучасному світі. З'ясовано основні напрями, засоби і механізми протистояння гібридним загрозам, пов'язаним насамперед з агресією Росії проти України. Аргументовано, що гібридні війни в майбутньому слугуватимуть вагомою складовою міжнародних відносин, оскільки збережуться розбіжності між цивілізаціями і окремими країнами. Разом з удосконаленням інформаційно-комунікаційних технологій їх роль у досягненні політичних цілей зростатиме. З розвитком штучного інтелекту, вдосконаленням соціальних медіа гібридні війни зможуть посилити дезінформацію, втручання у вибори, вплив на громадську думку, атаки на системи державного управління та критичну інфраструктуру, торгівельні обмеження, енергетичний шантаж, погрози ядерною зброєю та ін. Оскільки гібридні війни вже сьогодні відзначаються непередбачуваністю, здатністю постійно змінювати форми і методи впливу, міжнародне співтовариство повинне навчитися діяти на випередження, реагувати на різного роду гібридні впливи, зважати на досвід України, здобутий в умовах російсько-української війни. Зроблено висновок, що в перспективі стратегія України і світового співтовариства має поєднувати оборонні й наступальні дії. Поступово ця стратегія повинна відтворити роль міжнародного права й міжнародної політики як чинників недопущення застосування сили у вирішенні територіальних та інших

політичних проблем, подолання ризиків, що включають тероризм, організовану злочинність, нелегальну міграцію, кібератаки, сепаратизм, поширення зброї масового ураження.

Ключові слова: російсько-українська війна; гібридна війна; інформаційна війна; національна безпека і оборона; асиметрична стратегія; інформаційно-комунікаційні технології; волонтерська діяльність; дезінформація; євроінтеграція; міжнародне право; штучний інтелект.

Вступ

Про гібридну війну як сучасний феномен на різних рівнях сказано вже досить багато. Це є свідченням того, що гібридні війни в майбутньому, ймовірно, слугуватимуть вагомою складовою міжнародних відносин. Допоки існуватимуть розбіжності між цивілізаціями і країнами подолати вплив таких воєн не вдасться. Навпаки, разом з удосконаленням інформаційно-комунікаційних технологій їх роль у досягненні політичних цілей зростатиме. З розвитком штучного інтелекту, вдосконаленням соціальних медіа гібридні війни зможуть посилити дезінформацію, втручання у вибори, вплив на громадську думку, атаки на системи державного управління та критичну інфраструктуру, торгівельні обмеження, енергетичний шантаж, погрози ядерною зброєю та ін. Гібридні війни вже сьогодні відзначаються непередбачуваністю, здатністю постійно змінювати форми і методи впливу. За цих умов міжнародне співтовариство повинне навчитися діяти на випередження, гнучко реагувати на різного роду гібридні впливи, зважати на досвід України, здобутий в умовах російсько-української війни.

І, не зважаючи на те, що перелік дослідників різних аспектів гібридної війни на сьогодні є досить значним, існує нагальна потреба її постійного наукового супроводження, оскільки вона динамічно розвивається й постійно вдосконалюється. Відповідно, метою даної статті є з'ясування перспектив гібридної війни на тлі цивілізаційного розвитку. До основних завдань дослідження віднесені: виявлення новітніх викликів, пов'язаних з удосконаленням технологій гібридної війни та загостренням протистояння політичних сил у сучасному світі; з'ясування основних напрямів, засобів і механізмів протистояння гібридним загрозам, пов'язаним насамперед з агресією Росії проти України.

Методи дослідження

У пропонованому дослідженні використано: системний метод для з'ясування природи новітніх викликів, пов'язаних із застосуванням технологій гібридної війни та засобів протидії їхньому впливу; структурно-функціональний метод для виявлення ключових засобів убезпечення світового співтовариства від гібридних загроз.

Результати дослідження

Ще в 2016 році українські експерти закликали міжнародне співтовариство зробити належні *висновки* з гібридного російсько-українського конфлікту. Зокрема, М. Розумний зазначав, що світ загалом і кожна окремо взята країна опинилися перед загрозою дестабілізації, що доводить приклад війни на території колишньої Югославії. Відповідно мають сформуватися в Європі консолідовані зусилля щодо запобігання конфліктно-кризових ситуацій та проявів гібридної агресії [1, с. 18]. Відсутність належної реакції лідерів демократичних країн, недолугі спроби умиротворення агресора створили умови для широкомасштабного вторгнення Росії в Україну та подальшої ескалації застосування гібридних засобів ведення війни.

Зазначене вимагає від держав адаптивності, гнучкості, постійного удосконалення здатності реагувати на нові виклики. Разом із ризиками й реальним застосуванням гібридних засобів ведення війни вже відбуваються й відбуватимуться у подальшому контрзаходи проти них, включаючи системи удосконалення кібербезпеки, раннього виявлення загроз, утворення коаліцій держав з метою протистояння латентним агресивним діям, налагодження інформаційної гігієни населенняю Це є свідченням поступового зміцнення міжнародного співробітництва, спрямованого на формування єдиної системи протигібридної оборони як складової колективної безпеки. Таке співробітництво передбачає обмін досвідом, навчання персоналу системному застосуванню методик протистояння хакерським атакам на комп'ютерні й телекомунікаційні мережі, створення нових структур по боротьбі з дезінформацією за прикладом уже існуючих (StratCom Task Force; EUvsDisinfo та ін.). У розвиток наявних правових документів ЄС (Кодекс практики щодо дезінформації, Акт про цифрові послуги), продовжуватиметься процес формування європейського правового підходу до інформаційної безпеки.

Гібридна війна Росії проти України виявила серйозні прогалини в міжнародному праві, зокрема в тому його сегменті, що стосується регулювання збройних конфліктів. Відсутність нормативного регулювання цього новітнього явища пришвидшує використання нових засобів, щодо яких відсутні зобов'язуючі норми, відповідні санкції. Неможливість нормативного трактування цього поняття та пов'язаних з ним наслідків призводить до подвійного тлумачення двосторонніх та багатосторонніх договорів, використання правових прогалин, ігнорування державного суверенітету, страждання цивільного населення на окупованих територіях. У цьому контексті вчені зазначають: «Право збройних конфліктів було розроблене спільними діями міжнародної спільноти, яка змогла врегулювати найгостріші питання. На сьогодні ж з'явився новий виклик — гібридна війна. Для того, щоб попередити можливості підриву зусиль, що були спрямовані

на гуманізацію війни, міжнародне співтовариство повинно визнати, що питання про ефективність та практичність права збройних конфліктів повинне розширюватися по мірі розвитку нового «гібридного» виду війни» [2, с. 232]. Отже, у зв'язку з ризиками, які несе гібридна війна, міжнародне співтовариство муситиме подолати наявний консерватизм у міжнародно-правовій сфері, суттєво оновити право збройних конфліктів, виробити необхідні норми для уникнення зловживання цим правом і покарання тих, хто застосовують гібридні засоби ведення війни, що спричинюють страждання людей і порушують усталений міжнародний порядок та загальнолюдські цінності.

На думку автора, висловлену в 2019 році, контрзаходи проти сил зла передбачають «роз'яснювальну роботу серед населення окупованих територій; викриття діяльності незаконних збройних формувань; блокування лінгвістичної зброї, насамперед мовного чинника, особливо в потенційному поясі нестабільності (Закарпаття, Чернівецька та Південно-Східні області); формування морально-психологічної стійкості суспільства до диверсійних та терористичних актів» [3, с. 223]. Звичайно, за нинішніх умов ескалації гібридної агресії на тлі відкритого збройного нападу Росії на Україну, що має всі ознаки геноциду українського народу, протидія гібридній війні потребує значного вдосконалення й передбачає наступне.

1. Створення нової моделі системи національної безпеки і оборони України, спроможної відповідати на виклики сьогодення і майбутнього. Широкомасштабна війна з перших днів виявила недоліки системи національної безпеки і оборони України. Спільною ознакою усіх попередніх стратегічних документів з цього питання був їхній відверто декларативний характер. Російська агресія звела нанівець більшість основоположних принципів. Нові виклики зумовили необхідність динамічної переорієнтації ЗСУ на стандарти НАТО; нагальні потреби забезпечення інформаційної, енергетичної безпеки, кібербезпеки. Поряд із цим на поверхню вийшли корупція, неефективна система державного управління, соціокультурні протиріччя всередині українського суспільства — «хвороби», боротьба з якими потребує значних консолідованих зусиль держави й суспільства.

У виробленні та реалізації нової стратегії національної безпеки і оборони України варто особливу увагу приділити подоланню етнополітичної дезінтеграції держави. На цьому, зокрема, ще раніше наголошували фахівці Інституту держави і права імені В. М. Корецького НАН України: «Зміцнення національної ідентичності, розвиток патріотизму, створення умов для міжетнічного діалогу є основними завданнями у сфері національної безпеки не лише для країн, що стали об'єктом агресії з боку сусідніх держав, а й для етнічно однорідних держав. Недостатня увага до цих питань у вітчизняній стратегії національної безпеки та державній політиці

призведе до того, що невирішені етнічні проблеми будуть використовуватися як внутрішніми, так і зовнішніми силами для дестабілізації ситуації в країні у майбутньому» [4, с. 65]. У цьому контексті політика ідентичності стає одним із головних пріоритетів розвитку держави тепер і в доступній для огляду перспективі.

У контексті формування нової національної стратегії безпеки і оборони основними завданнями України мають стати: 1) виснаження противника, стимулювання міжнародної допомоги, активізація політики партнерства, залучення іноземних інвестицій; 2) домінування власної політичної волі у проблемних регіонах, здійснення ефективних внутрішніх реформ, побудова сучасної системи державного управління з дотриманням демократичних принципів, прав і свобод, підтримка малого й середнього бізнесу, боротьба з корупцією; 3) налагодження цифрової безпеки, що передбачає навчання користувачів захисту своїх акаунтів, уникнення фішингових атак; розвиток медіаграмотності населення зі створенням відповідних освітніх програм для вироблення в користувачів критичного мислення, здатності розпізнавати маніпуляції.

2. Формування на основі здобутого воєнного досвіду асиметричної стратегії як відповіді на новітні виклики російської збройної й гібридної агресії. Зважаючи на відхід Росії від вимог міжнародного права, правил і стандартів демократичної поведінки держави на міжнародній арені, відповідь демократичного світу і України не може бути симетричною й вимагає застосування оперативної і нестандартної асиметричної стратегії. На основі аналізу ролі асиметричних чинників у гібридній війні І. Дерев'янко слушно зазначає: «Через стрімкий науково-технічний прогрес і зростання асиметричної війни тотальні війни можуть бути неефективними навіть проти держав, які володіють відносно меншими ресурсами та впливом на міжнародній арені» [5, с. 11]. Україна своїми асиметричними діями довела, що в сучасних умовах така стратегія означає постійний системний тиск на «вразливі місця» супротивника, здатність організовувати свою діяльність і мислити відмінним від опонента чином задля максимізації власних переваг, захоплення ініціативи чи забезпечення простору для маневрування.

Формування стратегії гнучкого реагування на асиметричній основі передбачає мобілізацію суспільства на захист країни (залучення висококваліфікованих кадрів з геополітики, етнополітики, національної безпеки, інформаційно-комунікаційних технологій; стимулювання волонтерського руху; проведення ефективних точкових операцій; створення оборонних рубежів з метою врівноваження співвідношення сил та ін.). Ефективними механізмами позбавлення Росії «козирів» у асиметричній війні мають слугувати: викриття й нейтралізація залишків російської «п'ятої колони», насамперед у таких промислових центрах як Харків, Дніпро, Миколаїв, Одеса,

Запоріжжя; спрощена процедура надання громадянства представникам Російської Федерації, які беруть участь у збройній боротьбі проти агресії, виступають проти імперської політики та ідеології «русского мира». У цьому контексті, важливо відзначити, що у гібридному протистоянні програє той, хто втрачає волю до перемоги, не здатен мобілізувати суспільство, переконати його у доцільності матеріальних витрат та людських жертв.

Оборонна стратегія, яку змушена застосовувати Україна, покликана мінімізувати негативні наслідки від дій небезпечного суперника, що має значну перевагу в силі й використовує своє домінуюче становище. Самостійних зусиль України у використанні цієї стратегії недостатньо. Потрібна безупинна допомога світового співтовариства. У цьому контексті стратегія асиметричного характеру означає насамперед застосування проти агресора санкцій, що включають економічні, фінансові, інформаційні та персональні обмеження. На думку українських фахівців Національного інституту стратегічних досліджень, санкції можуть стати дієвим інструментом, якщо вони будуть застосовуватись системно, консолідованими зусиллями Заходу. Відповідно санкційна політика має включати: 1) тиск на нафтогазовий сектор з огляду на його особливу вразливість, насамперед зниження цінової стелі на російську нафту; 2) розширення переліку товарів і секторів економіки, які підпадатимуть під санкції; 3) правове врегулювання питань щодо використання заморожених активів російських олігархів; 4) просування українського наративу в публічній та інформаційній площинах щодо подій російсько-української війни, зокрема, апелювання до колонізаторської сутності російської політики» [6, с. 72 — 73]. Попри скептичне ставлення деяких фахівців щодо реального впливу застосовуваних санкцій, вони мають надзвичайно важливе стратегічне значення.

Допомагаючи Україні, демократичний світ (насамперед Європейський Союз) підняв власний авторитет, виявивши на офіційному рівні безкомпромісність щодо застосування санкцій, не дивлячись на очевидні економічні втрати. У застосуванні асиметричної стратегії Європейського Союзу значне місце відводиться наданню всебічної підтримки Україні, яка несе неймовірні втрати внаслідок війни. Ця допомога, поряд із наданням зброї, здійснюється у формах підтримки курсу України на євроінтеграцію, медичної допомоги, матеріального забезпечення вимушених мігрантів. Породжені санкціями проблеми поступово формують внутрішню опозицію путінському режимові всередині самої Росії.

Важливу роль у асиметричній стратегії відіграє вивчення ризиків для Європи гібридної політики Росії. До таких ризиків відносяться: провокаційна проросійська політика в окремих європейських країнах; діяльність фондів, культурних товариств («Росспівробітництво», «Російські доми»), аналітичних центрів проросійської спрямованості в Європі, що включає

дії, спрямовані на недопущення розширення Європейського Союзу або навіть і на його розвал; системна підтримка з боку Росії ультраправих та ультралівих політичних партій і рухів (це стосується в першу чергу Франції, Італії, Угорщини).

3. Належне використання інформаційно-комунікаційних можливостей (потенціалу публічної дипломатії; взаємодії держави, військових, волонтерів, громадськості; гнучкої динаміки засобів масової інформації та соціальних мереж). Технології гібридної війни, які динамічно розвиваються, перетворили інформаційно-комунікаційну сферу на визначальну арену протиборства сторін, в даному випадку — Росії і України. Дезінформації, яку активно просуває агресор, в українському інформаційно-комунікаційному просторі предостатньо. Натомість нагальною потребою постала необхідність поширення української інформації на територію країни-агресора.

І хоча таке поширення стикається з численними перешкодами через політику російського уряду щодо контролю над інформаційним простором, існують певні шляхи та методи, які використовуються для забезпечення доступу до української інформації для російських громадян. Українська інформація поширюється через VPN, TOR-мережу та інші інструменти, що дозволяють обходити блокування російського уряду. Існують, хоча й нечисленні, російські громадяни, які виступають проти війни та підтримують Україну, займаються поширенням об'єктивної інформації про неї. Важливим способом донесення правди до росіян є залучення міжнародних ЗМІ до висвітлення та поширення необхідної інформації серед російськомовної аудиторії. Поряд із цим створюються альтернативні інформаційні ресурси, такі як російськомовний телеканал «Freedom», що є важливим засобом у боротьбі з дезінформацією.

У процесі використання ЗМІ та соціальних мереж важливою функцією для сторони, що захищається, є координація інформаційних потоків, які стосуються військових дій, протистояння гібридній агресії. Особливо важливим є встановлення повного контролю не лише над інформаційним простором своєї країни, а й, по мірі можливості, — країн, які з подачі агресора можуть впливати на перебіг війни. До організацій, які активно чинять опір ворогу в інформаційному полі, належать: StopFake (займається перевіркою фактів та викриттям російської пропаганди, досліджує методи її впливу на Україну та інші європейські країни); PR Army (організація, що висвітлює інформацію про Україну в міжнародних медіа, надає компетентних експертів для закордонних ЗМІ, розслідує наслідки депортації українців до Росії); Molfar (компанія, що здійснює воєнні розслідування, зокрема ідентифікує воєнних злочинців, спростовує пропагандистські наративи, займається геопросторовою розвідкою); «Детектор медіа» (аналітичний

центр, що сприяє грамотності серед українців, протидії російській дезінформації, підвищенню якості контенту вітчизняних медіа).

Вагомим чинником у протистоянні інформаційній війні, як основній складовій гібридних дій, має слугувати боротьба з інформаційно-психологічними впливами. Протистояння деструктивному впливу більш могутнього противника передбачає інтенсивне використання засобів інформаційно-психологічного впливу. Чим сильніший суперник, тим більш асиметричною має стати інформаційна дія, здатна ефективно протидіяти масованій пропаганді. У цьому контексті важливою проблемою є розвиток стратегічних комунікацій як засобу боротьби з дезінформацією. Сутність стратегічного підходу «полягає в реалізації масовості та адресності інформаційних матеріалів; цілеспрямованості, превентивності та креативності повідомлень, ефективності розподілу ресурсів, гнучкості та простоті контенту» [7, с. 313]. В нашому випадку така комунікація повинна включати: зв'язок з населенням окупованих територій; захист державної мови й національної культури, жорстку протидію антиукраїнським наративам; формування морально-психологічної стійкості суспільства до повітряних атак, диверсійних актів; подолання комплексу меншовартості, психології раба, сформованої ідеологією «старшого брата»; створення каналів інформаційної взаємодії з опозиційно налаштованою російською аудиторією; захист національного інформаційного та соціокультурного простору України; подолання світоглядного хаосу, некритичності мислення, диктату міфів, забобонів, цілеспрямоване розвінчування інформаційної агресії.

Для ефективної взаємодії всіх суб'єктів інформаційної діяльності доцільно активно використовувати поряд з військовими структурами можливості громадських — аналітичних центрів, благодійних фондів, культурних товариств. Вагомим чинником є створення системи удосконалення підготовки фахівців у закладах вищої освіти України для кадрового забезпечення структур, орієнтованих на протидію національній безпеці держави в інформаційній сфері. З 2014 року інформаційній експансії активно протидіє волонтерський рух. Волонтери поширюють правдиву інформацію про Україну й таким чином підтримують її позитивний імідж у світі, в умовах інформаційної експансії допомагають державі протидіяти російській пропаганді, згуртовують та підтримують моральний дух населення, надають допомогу колишнім військовополоненим та людям з деокупованих територій.

Гібридна війна як новий вид міждержавного протистояння потребує застосування новітніх технологій на базі штучного інтелекту. Деякі з них уже активно впроваджуються в Україні й дозволяють долати сильнішого ворога. До таких ефективних розробок належать: система ситуаційної поінформованості (Kropyva); додаток GIS Arta, що допомагає синхронізувати

наведення артилерії; засоби автономної навігації без використання GPS; технології ідентифікації дезінформації та бот-мереж; системи виявлення і нейтралізації мін та боєприпасів. На часі створення засобів підготовки та прийняття рішень, що стосуються захисту інформаційного простору. Можливості штучного інтелекту в цій сфері дозволять забезпечити перевагу у військовій, економічній, інформаційній, технологічній сферах. Корисним і доцільним у цьому відношенні є цільове застосування мереж, що передбачає «створення з взаємодіючих агентів багатоагентних систем, де кожен агент володіє частковим уявленням про глобальну проблему і вирішує частину спільного завдання». Відповідно комплекс завдань «розподіляється між агентами з присвоєнням кожному ролі згідно його можливостей» [8, с. 144]. Рішення на основі штучного інтелекту в умовах війни мають важливе значення для захисту українських життів та національної безпеки.

Разом із активізацією застосування гібридних маніпуляцій свідомістю людей загострилась проблема перевірки інформації на достовірність. З огляду на це, перспективною технологією виступає фактчекінг — інструмент журналістських розслідувань, спрямований на викриття маніпуляцій, недостовірних фактів у риториці суб'єктів політики, громадських діячів різного рівня, спотворення реальності в публікаціях, розміщених у засобах масової інформації чи соціальних мережах.

Фактчекінг активно застосовується в журналістиці з 2016 року. За висновком українських фахівців, у добу постправди він є «ефективним засобом отримання правдивої інформації», що дозволяє «формувати політичну грамотність населення» [9, с. 138]. Ключовими напрямками застосування фактчекінгу в умовах гібридної війни можуть слугувати: створення фактчекінгових компаній при редакціях впливових ЗМІ задля здійснення верифікаційної діяльності в періоди найбільшого попиту, соціальних, політичних, військових потреб; боротьба з фейками спільними зусиллями на основі медіапартнерства (як окремих компаній всередині країни, так і групи країн на основі коаліційних угод); залучення потенціалу краудфандингу (добровільного громадського фінансування), використання якого, зокрема, є характерним для вищезгаданого українського проєкту «StopFake».

Висновки

Таким чином, гібридна війна, як новітній феномен, відзначається стійкою тенденцією до вдосконалення та розширення сфери застосування політико-психологічних і технологічних засобів. Відповідно, в перспективі стратегія України і світового співтовариства має поєднувати оборонні й наступальні дії з метою убезпечити себе від дій суперника, який має значну перевагу за військовим і фінансово-економічним потенціалом, нав'язує свою волю й інтереси. Поступово ця стратегія повинна повернути

міжнародні відносини в річище демократичного правопорядку та європейської безпеки, що передбачає: непорушність кордонів, побудову ефективної енергетичної безпеки, недопущення застосування сили у вирішенні політичних проблем; подолання латентних загроз, до яких відносяться тероризм, транснаціональна організована злочинність, нелегальна міграція, кібератаки, сепаратизм, глобальні зміни клімату, розповсюдження зброї масового ураження і засобів її доставки.

Список посилань

1. Російська «гібридна» агресія: цілі і наслідки, засоби протистояння (інтерв'ю). Національна безпека і оборона. 2016. № 9 — 10 (167 — 168). С. 17 — 37.
2. Власюк В. В., Карман Я. В. Деякі основи поняття «гібридна війна» в міжнародному праві. Право і громадянське суспільство. Науковий журнал. Електронне видання. 2015. № 1. С. 226 — 234.
3. Горбатенко В. Футурологія і політика: монографія. Київ: Академвидав, 2019. 288 с.
4. Етнополітична безпека України: політико-правові механізми протидії етнополітичній дезінтеграції держави: Наукова записка / Горбатенко В. П. (керівник авт. кол.), Шемшученко Ю. С., Кресіна І. О., Стойко О. М. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2015. 80 с.
5. Дерев'янко І. П. Гібридна війна як різновид асиметричних дій. Міжнародні відносини: теоретико-практичні аспекти. 2023. Вип. 11. С. 6 — 16.
6. Міжнародні санкції як інструмент стримування російської агресії проти України: аналіт. доп. / [А. Бобровицький, Н. Гавриленко, А. Гончарук, І. Ус, Г. Широкий, Р. Юлдашев]; за заг. ред. М. Паламарчука. Київ: НІСД, 2023. 76 с.
7. Новакова О., Черненко О. Розвиток стратегічних комунікацій як засіб боротьби з дезінформацією в українському суспільстві. Вісник Львівського університету. Серія філос.-політолог. студії. 2023. Вип. 49. С. 308 — 314.
8. Ситник Г. П., Заворітня Г. П., Марутян Р. Р. Інформаційно-комунікаційні технології у сфері національної безпеки: навчальний посібник / за заг. ред. Г. П. Ситника. Київ: ТОВ «Академпрес», 2024. 176 с.
9. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька; ред.-упор.: О. І. Харитоненко, Ю. С. Полтавець. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.

References

1. Russian “hybrid” aggression: goals and consequences, means of confrontation (interview). (2016). National Security and Defense, No. 9 — 10 (167-168), 17-37 (in Ukrainian).
2. Vlasyuk V. V. & Karman Ya. V. (2015). Some foundations of the concept of “hybrid war” in international law. Law and civil society. Scientific journal. Electronic edition, No. 1, 226-234. (in Ukrainian).
3. Gorbatenko V. (2019). Futurology and politics: monograph. Kyiv: Akademvydav. 288 p. (in Ukrainian).
4. Ethnopolitical security of Ukraine: political and legal mechanisms for countering the ethnopolitical disintegration of the state: Scientific note. (2015). / Gorbatenko V.P. (head of the author’s collection), Shemshuchenko Yu.S., Kresina I.O., Stoyko O.M. Kyiv: V.M. Koretsky Institute of State and Law, NAS of Ukraine. 80 p. (in Ukrainian).
5. Derevyanko I. P. (2023). Hybrid war as a type of asymmetric action. International relations: theoretical and practical aspects, Issue 11, 6 — 16. (in Ukrainian).
6. International sanctions as a tool for deterring Russian aggression against Ukraine: analytical supplement. (2023). / [A. Bobrovytskyi, N. Gavrylenko, A. Goncharuk, I. Us, G. Shyrokyi, R. Yuldashev]; ed. by M. Palamarchuk. Kyiv: NISD. 76 p. (in Ukrainian).
7. Novakova O. & Chernenko O. (2023). Development of strategic communications as a means of combating disinformation in Ukrainian society. Visnyk of Lviv University. Series of philosophical and political science studies, Issue 49, 308-314. (in Ukrainian).
8. Sytnyk G. P., Zavoritnya G. P. & Marutyan R. R. (2024). Information and communication technologies in the sphere of national security: a textbook / edited by G. P. Sytnyk. Kyiv: Akadempress LLC. 176 p. (in Ukrainian).
9. Hybrid war and journalism. Problems of information security: a textbook (2018). / edited by V. O. Zhadka; editors-supervisors: O. I. Kharytonenko, Yu. S. Poltavets. Kyiv: Publishing House of the National University named after M. P. Dragomanov. 356 p. (in Ukrainian).

ISSN 2415–881X Politology Bulletin, Issue 99 (2025)
UDC 327.56:355.4 DOI 10.17721/2415-88IX.2025.99.263–275

Volodymyr Horbatenko
Doctor of Political Sciences, Professor, Leading Research Fellow
of the Department of Constitutional and Municipal Law
Institute of State and Law named after V. M. Koretsky
National Academy of Sciences of Ukraine (Kyiv, Ukraine)
https://orcid.org/0000-0002-2400-954X
e-mail: stateandlaw@ukr.net

HYBRID WARFARE ESCALATION: NEW CHALLENGES AND COUNTERMEASURES

Abstract

The prospects of hybrid warfare against the background of civilizational development are considered. The latest challenges associated with the improvement of hybrid warfare technologies and the aggravation of the confrontation between political forces in the modern world are identified. The main directions, means and mechanisms of countering hybrid threats, primarily associated with Russia's aggression against Ukraine, are clarified. It is argued that hybrid wars will serve as an important component of international relations in the future, since differences between civilizations and individual countries will persist. Along with the improvement of information and communication technologies, their role in achieving political goals will grow. With the development of artificial intelligence and the improvement of social media, hybrid wars will be able to intensify disinformation, interference in elections, influence public opinion, attacks on government systems and critical infrastructure, trade restrictions, energy blackmail, threats with nuclear weapons, etc. Since hybrid wars are already today characterized by unpredictability, the ability to constantly change forms and methods of influence, the international community must learn to act in advance, respond to various types of hybrid influences, and take into account Ukraine's experience gained in the conditions of the Russian-Ukrainian war. It is concluded that in the future, the strategy of Ukraine and the world community should combine defensive and offensive actions in order to protect itself from the actions of an opponent who has a significant advantage in military and financial and economic potential and imposes its will and interests. Gradually, this

strategy should return international relations to the course of democratic rule of law and European security, which provides for: the inviolability of borders, the construction of effective energy security, the prevention of the use of force in solving political problems; overcoming latent threats, which include terrorism, transnational organized crime, illegal migration, cyberattacks, separatism, global climate change, proliferation of weapons of mass destruction and their means of delivery.

Keywords: Russian-Ukrainian war; hybrid war; information war; national security and defense; asymmetric strategy; information and communication technologies; volunteering; disinformation; European integration; international law; artificial intelligence.

Надійшла до редакції 20.10.2025

Прийнято до друку 18.11.2025

Оприлюднено 29.12.2025