СУТНІСНІ РИСИ ТА ФУНКЦІОНАЛЬНІ КОМПОНЕНТИ СУЧАСНОЇ НЕКОНВЕНЦІЙНОЇ (ГІБРИДНОЇ) КОНФЛІКТНОСТІ

УДК 327:355.1(1-071)(477)

<https://doi.org/10.53679/2616-9460.1-2.2021.02>

Веденєєв Дмитро Валерійович –
професор Національної академії
керівних кадрів культури і мистецтв,
доктор історичних наук, професор
ORCID: 0000-0002-8929-9875

Семенюк Олександр Георгійович –
перший заступник керівника
Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю
при РНБО України, доктор юридичних наук
ORCID: 0000-0002-5096-1374

У статті¹ обґрунтовано, що стратегія й арсенал гібридної (асиметричної, неконвенційної) конфліктності у сучасному світі спираються на принципові якісні зміни, що відбулися на межі ХХ–ХХІ ст. унаслідок радикальних змін співвідношення сил на міжнародній арені, хаотизації міжнародних відносин, появи нових видів летального та нелетального озброєння, інноваційних технологій конструювання й демонтажу соціальних спільнот із наперед визначеними характеристиками. Ці зміни стосувалися концептуальних засад, структури, стратегії і тактики, форм і методів військово-політичного протистояння між сучасними державами та їх блоками, державами та неурядовими формуваннями тощо.

Здійснено спробу узагальнити найбільш усталені сутнісні риси та функціональні компоненти гібридних війн, визначено їхні сутнісні властивості: латентність певних фаз, дистанційний під-рив невійськовими й «неконтактними» методами спроможності держави до оборони й захисту національних інтересів; невідповідність міжнародному праву війни; комплексне застосування методів військового, спеціального та невійськового, а також дипломатичного, фінансово-економічного, гуманітарного тощо тиску на державу-жертву; широке використання антиурядових організацій і рухів, незаконних збройних формувань, сепаратистських, іредентистських, радикально-етноконфесійних течій, екстремістських угруповань, штучно створених деструктивних спільнот; пріоритетна роль спеціальних служб, сил спецоперацій, їх застосування для створення потужної антиурядової інфраструктури з метою дестабілізації легітимного державного

¹ Статтю підготовлено за програмою ЄС «Еразмус +» у рамках проекту «Академічна протидія гібридним загрозам – WARN» # 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP».

ладу; пріоритетна роль цілеспрямованого впливу на масову свідомість за допомогою масштабного застосування методів інформаційно-психологічного протиборства та кібервійни.

Ключові слова: національна безпека, військове мистецтво, неконвенційні війни, гібридна конфліктність, конфліктологія, безпекознавство.

Dmytro Viedienieiev, Oleksandr Semeniuk

ESSENTIAL FEATURES AND FUNCTIONAL COMPONENTS OF MODERN UNCONVENTIONAL (HYBRID) CONFLICT

*In the article*¹ the authors argue that the strategy and arsenal of hybrid (asymmetrical, unconventional) warfare in the contemporary world are fundamentally based on the qualitative changes that took place at the turn of the XXI century as a result of radical changes in the balance of power in the international arena, chaos in international relations, the development of new types of lethal and non-lethal weapons, new technologies of constructing and dismantling social communities with predetermined characteristics. These changes involved the conceptual framework, structure, strategy and tactics, forms and methods of the military and political confrontation between modern states and their blocks, as well as between states and non-governmental organisations.

The authors identify the essential features and functional components of hybrid warfare, such as its latency phases; the remote undermining of national defense capabilities by non-military and non-contact means; breaching the international law of war; the integrated use of military methods as well as specific means of non-military, diplomatic, financial and economic, humanitarian pressure on a victim state. They also include the extensive use of anti-government groups and movements; illegal armed groups, separatists, irredentists, radical ethnic and religious groups, extremist organizations, and artificially constructed destructive groups; the privileged role of intelligence services, special operations forces and their use for engineering a powerful anti-government infrastructure designed to destabilize the legitimate state system; the priority role of targeted influence on public opinion through the extensive use of methods of information and psychological warfare and cyberwarfare.

Keywords: national security, art of war, unconventional warfare, hybrid conflicts, conflictology, security studies.

Вивчення природи гібридних війн – актуальне завдання безпекознавства

Під час реформування сектору безпеки і оборони України важливо, щоб науково-дослідні та аналітико-прогностичні можливості цієї сфери відповідали актуальному рівню загроз. Тобто виникає потреба в поглиблених, вільних від примітивної ідеологізації досліджень конфліктності нового нетрадиційного (гібридного, асиметричного) типу.

Свого часу в Концепцію розвитку сектору безпеки і оборони України, затверджену Указом Президента України від 14 березня 2016 р. № 92 (нині документ втратив чинність), було внесено положення про гібридну війну (ГВ) як один із провідних чинників загроз безпеці держави та її визначення. Згідно з останнім гібридна війна трактувалась як комбінації різноманітних і динамічних дій регулярних сил, що взаємодіють зі злочинними озброєними угрупованнями та кримінальними елементами,

діяльність яких координується і здійснюється за єдиним замислом і планом із активним застосуванням засобів пропаганди, саботажу, навмисного завдання шкоди, диверсій і терору [1, р. II, п. 1].

У Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 р. № 392/2020, йдеться про те, що сучасна модель глобалізації уможливила поширення різних видів загроз: розроблення системи озброєнь на основі нових фізичних принципів і новітніх технологій, розповсюдження зброї масового ураження, міжнародного тероризму та міжнародної злочинності, зокрема в кіберпросторі, наркоторгівлі, торгівлі людьми, політичного та релігійного екстремізму, політичного насильства та сепаратизму, нелегальної міграції, кіберзагроз тощо [2, р. II, пп. 9, 10]. Наголошується на тому, що «держава врахує уроки гібридної агресії проти України, бойових дій на Близькому Сході у нових доктринальних підходах до забезпечення воєнної безпеки» [2, р. III, п. 44].

¹ The article was written under the EU Erasmus + project 'Academic Response to Hybrid Threats – WARN' 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP.

Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона», затверджена Указом Президента України від 25 березня 2021 р. № 121/2021, пропонує визначення гібридної війни як «комбінації різноманітних дій щодо прихованого застосування регулярних військ (сил), незаконних збройних формувань і терористичних організацій, використання пропаганди, саботажу, терору, вчинення диверсій, навмисного завдання шкоди громадянам, юридичним особам та об'єктам державної власності в Україні». Водночас ідеться про оборонну доцільність застосування всіх форм і способів протидії, «зокрема асиметричних та інших дій для оборони України, з дотриманням принципів і норм міжнародного права» [3].

Можна погодитися з думкою академіка НАН України В. Горбуліна про те, що «кожен конкретний елемент цієї “гібридної війни” не новий по суті і використовувався майже в усіх війнах минулого, однак унікальними є узгодженість і взаємозв'язок цих елементів, динамічність та гнучкість їхнього застосування, а також зростання ваги інформаційного чинника. Причому інформаційний чинник в окремих випадках стає самостійним складником і виявляється не менш важливим, ніж військовий». Учений наводить усталені в модерній світовій військово-політичній думці визначення цього новітнього типу конфліктних відносин: «неконвенційна війна», «нерегулярна війна», «змішана війна», або ж спонсоровані державою гібридні війни [4].

Нині замість т. зв. «конвенціональних» або «тотальних» війн між державами та коаліціями все частіше виникають війни нового концептуального типу. Їх ведуть між собою воєнно-політичні недержавні угруповання, які нерідко й створюються певними державами для реалізації своїх неблагонамірених геополітичних устремлінь. Зокрема, у 2010 р. Робоча група НАТО сформулювала таке визначення поняття гібридної загрози – це небезпека, створена реальним або потенціальним противником (державою, недержавною організацією або терористами), що полягає в реалізованій або потенційній можливості одночасного застосування традиційних і нетрадиційних військових методів для досягнення своїх цілей.

Сучасний світ стрімко поринає в хаос війн та конфліктів, деструктивних процесів, які неможливо передбачити. Розроблені в США і НАТО прогнози розвитку міжнародних процесів на майбутні кілька десятиліть містять передбачення щодо зростання глобальної нестабільності. Одним із її чинників

стане зростання ролі недержавних суб'єктів у разі розширення їх доступу до військових та інформаційних технологій, зброї масового ураження («дифузія глобальної потужності»), а також поширення у світі комбінацій за участю державних і недержавних учасників.

За слушним висловом італійського професора К. Санторо, розпочався «період цивілізаційних катастроф і глобального хаосу», ознаками якого є послаблення ролі ООН та системи міжнародного права внаслідок дестабілізації світової геополітичної ситуації; посилення військово-політичного розбалансування світу, бурхливий розвиток націоналізму, екстремізму й тероризму; поширення у світі воєнних конфліктів малої інтенсивності; розпад традиційних військово-політичних блоків та посилення НАТО з монополізацією права на застосування «гуманітарних інтервенцій» [5].

Концепт гібридної війни став невід'ємним елементом як світової теоретико-конфліктологічної думки, так і доктринальних документів у сфері безпеки та оборони провідних країн світу. Наприклад, у травні 2020 р. на замовлення Міністерства оборони США стратегічний дослідницький центр RAND підготував науково-дослідні роботи щодо можливих воєнно-політичних ситуацій, з якими США можуть зіткнутися до 2030 р. Ці дослідження засвідчили: майбутні конфлікти переважно матимуть характер асиметричних війн та «гібридних збройних конфліктів у сірій зоні» [6].

Дослідження та прогнозування розвитку стратегії й тактики, технологій неконвенційного протистояння посіли провідне місце серед магістральних трендів світової науки та профільної аналітики. В Україні після 2014 р. відбулася стрімка інтенсифікація науково-аналітичних пошуків у царині осмислення генези та змісту феномену гібридної війни як новітньої концептуальної моделі неконвенційного (асиметричного) протистояння, розпочалися вивчення стратегії, тактики та арсеналу гібридного протистояння, історичних і поточних зразків нетрадиційного протистояння, пошук шляхів відвернення й протидії гібридним загрозам національній безпеці.

Значно активізувалося вивчення теоретичних і науково-практичних аспектів новітніх моделей асиметричного (неконвенційного) протистояння, які прийнято іменувати гібридною війною. У працях фахівців з військових наук, геополітики, конфліктології, інформаційної безпеки, міжнародного права та інших наукових галузей, зокрема

О. Артюшенка, В. Бочарнікова, Ю. Бута, В. Власюка, Д. Веденєєва, В. Горбуліна, О. Гойман, В. Грицюка, Р. Гули, О. Долженка, О. Дузь-Крятченка, Я. Жаркова, Я. Карман, О. Литвиненка, Є. Магди, Ю. Остаха, С. Павловської, Б. Парахонського, К. Попович, І. Руснака, О. Саєнка, С. Свешнікова, С. Сегеди, І. Сивака, А. Сиротенка, О. Сищука, А. Слюсаренка, І. Слюсаренка, В. Телелима, П. Ткачука, М. Требіна, В. Шевчука, О. Шклярської, І. Феськова, Г. Яворської та інших дослідників, узагальнено сучасні погляди на походження, сутність, зміст, функціональні компоненти, міжнародно-правову оцінку, стратегію та інструментарій гібридних війн, окремі їхні прояви та похідні від них загрози безпеці України, геополітичні та воєнно-політичні обставини розгортання неконвенційного протистояння між Росією та Україною.

Сутнісні риси гібридного протиборства

Проведені власні дослідження та аналіз спеціальних праць дають можливість запропонувати певні узагальнювальні судження щодо сутності й структурно-функціональної побудови модерної гібридної конфліктності.

Джерелами розробки форм і методів ГВ став аналіз особливостей застосування новітніх засобів і технологій збройної боротьби, прогресування невійськових форм протиборства (передовсім у сфері технологій соціальної інженерії, інформаційно-психологічного протиборства, кібервійни), інших методів впливу на соціально-політичну реальність, яку інколи об'єднують поняттям «м'яка» сила.

У сучасній світовій військово-політичній думці поширені різні назви конфліктних відносин новітнього типу: неконвенційна війна, нерегулярна війна, змішана війна, або гібридна війна, яку веде держава. У визначеннях констатується розмивання параметрів воєнного конфлікту та залучення до нього невійськових засобів, які не мають прямого відношення до класичного військового протистояння.

Поняття «гібридна війна» застосовується і як синонім асиметричного, неконвенційного, нетрадиційного, дисперсного тощо типу протистояння, і як окреме визначення новітнього типу конфліктності (протиборства).

Провідні сучасні теоретичні (концептуальні) конструкції багато в чому солідарні щодо розуміння

сутності й арсеналу гібридної конфліктності. Так, у концептуальних документах США і НАТО констатується, що ГВ є комбінацією звичайних, нерегулярних і асиметричних засобів у поєднанні з постійними маніпуляціями політичними та ідеологічними розбіжностями. У концепції NATO's Bi-Strategic Command Capstone Concept (2010 р.) гібридні загрози визначаються як такі, що створюються супротивником, здатним одночасно інтегровано використовувати традиційні та нетрадиційні засоби для досягнення власних цілей. У п. 13 Підсумкової декларації саміту НАТО (вересень 2014 р.) під гібридною війною пропонувалося розуміти проведення широкого спектра прямих бойових дій і таємних операцій, що здійснюються за єдиним планом збройними силами, партизанськими та іншими іррегулярними формуваннями за участю різноманітних цивільних компонентів.

Зауважимо, що стратегії ГВ та рекомендації з протистояння нетрадиційним загрозам, котрі США та їхні союзники в НАТО останнім часом інтенсивно розробляють, спрямовані переважно на внесення відповідних змін не лише в організацію та функціонування збройних сил, а й у діяльність державного і громадянського секторів. Наголошується на важливості налагодження тісної координації між силовими структурами для відвернення нетрадиційних загроз, пов'язаних із пропагандистськими кампаніями, кібератаками та сепаратистськими рухами (докладно див. [7]).

Живильним джерелом поширення нетрадиційного протистояння (окрім традиційних геополітичних загроз) стало додаткове зростання «підбурюючих факторів». Йдеться про реалізацію інтересів наднаціональних структур управління (ядром яких є верхівка транснаціональних корпорацій), поглиблення загрозливих диспропорцій світового розвитку, подальше дроблення національних держав, поширення неурядових військово-політичних рухів нового концептуального типу.

Гібридне протистояння у своїй концептуальній основі спрямоване на деморалізацію супротивника, дистанційний підрив (переважно невійськовими й неконтактними методами) його спроможності до оборони й захисту національних інтересів загалом, примушення його до капітуляції, відмови від реального державного суверенітету та готовності до нав'язування йому вигідної переможцям моделі зовнішньої та внутрішньої політики, відповідного корегування суспільно-економічного ладу та духовно-культурної сфери. Стратегія ГВ спрямована на знесення країни-жертви, зокрема через роз-

балансування адміністративно-політичного управління, сфери оборони та безпеки, економіки, інформаційно-культурного простору.

Найбільш усталеними доцільно вважати такі сутнісні риси гібридної війни:

- ГВ є різновидом асиметричних (неконвенційних) дій, інтегровано сполучає військові та невоенні інструменти протистояння, структурно охоплює театр прямого конфлікту, тилову («сіру») зону, простір міждержавних відносин, усю глибину суспільно-політичного й соціоментального виміру буття суспільства;
- театр ГВ – це багатовимірний реальний (фізичний) та віртуальний (інформаційно-ментальний) простір існування держави (групи держав, нації, етносу, людської спільноти тощо), який цілеспрямовано перетворюється на часопростір проведення заздалегідь спланованого комплексу прямих та непрямих (асиметричних) агресивних дій;
- для ГВ притаманні інноваційні технології та найсучасніші засоби мобілізації (наприклад, протиборство у кіберпросторі, інформаційно-комунікаційні мережеві технології), розроблення нових видів високоточної, «розумної» летальної та нелетальної зброї;
- важливими суб'єктами (формами) протиборства стають мережеві та поліцентричні структури;
- ГВ комплексно поєднує дії (заходи) політичного, дипломатичного, власне воєнного, інформаційно-психологічного, когнітивно-ментального, економічного, екологічного та іншого характеру, котрі скоординовано проводять (можуть проводити) за єдиним задумом та одночасно у кількох територіальних або функціонально-структурних вимірах;
- значно розширився комплекс гібридних загроз, який поповнився сучасними високотехнологічними небезпеками (наприклад, дії в енергетичній сфері, кібератаки, використання соціальних мереж, «кліматична зброя» тощо);
- у ГВ суттєво зростає роль спеціальних служб, спеціальних операцій, неурядових організацій різної спрямованості, партизансько-повстанських, транснаціональних терористичних та організованих злочинних (мафіозних) й інших деструктивних недержавних формувань, а також штучно (технологічно) створених спільнот

із наперед визначеними соціоментальними та ідеологічними властивостями.

При цьому властивостями, що відрізняють асиметричне протистояння від класичних типів війн, є, зокрема, такі:

- неоголошений, не оформлений у міжнародно-правовому відношенні характер протистояння (агресивних дій);
- приховування політичних цілей і реально розпочатої агресії;
- нанесення кількох, зосереджених за часом і місцем, військових та невійськових ударів з неочікуваним для супротивника результатом і неприйнятним для жертви збитком;
- нав'язування супротивнику протиборства в принципово новій системі координат;
- відсутність звичної лінії фронту, широке застосування можливостей спеціальних служб та військ (сил) спеціального призначення;
- використання високоточної зброї (у разі прямого застосування збройних сил – масоване), засобів радіоелектронної боротьби, кібернетичної зброї та інших новітніх високотехнологічних засобів протиборства;
- застосування принципово нових форм і технологій невійськового насильства з акцентом на ураження управлінської, інформаційно-психологічної сфер та суспільної свідомості супротивника;
- штучне створення й пріоритетне використання неурядових організацій і рухів, ЗМІ, парамілітарних формувань (повстансько-партизанських, терористичних, організованих злочинних угруповань).

Стратегія неконвенційної конфліктності

Під стратегією гібридної війни доцільно розуміти концептуально обґрунтований, спланований, цілеспрямований, довгостроковий алгоритм прихованих дій держави щодо інших держав і спільнот, спрямований на досягнення цілей держави – ініціатора ГВ засобами, які суперечать нормам міжнародного права та добросусідства. На стратегічному рівні ГВ є часткою загального військово-політич-

ного курсу держави, що потребує завчасного розроблення доктринальних основ її ведення, розбудови відповідної інфраструктури. Готовність певної держави до застосування методів ГВ слугує промовистим індикатором сутності й спрямованості її державного ладу, офіційної ідеології, аксіологічної шкали та змісту зовнішньої політики.

Стратегія гібридної війни радикально відрізняється від традиційної ієрархії пріоритетів. Їх послідовність за важливістю цілей унаочнив у середині 1990-х років полковник ВПС США Дж. Уорден¹. Згідно з його «теорією п'яти стратегічних кілець» супротивник постає у вигляді мішені з п'ятьма концентричними колами, що розташовані в порядку зменшення важливості ураження. Її центром є політичне керівництво супротивника, його лідери; далі розташовані система життєзабезпечення, інфраструктура та економіка, власне населення, і лише останнє коло – це збройні сили. При цьому основні підривні зусилля мали би застосовуватися для ідейно-політичного роззброєння, деморалізації та дискредитації політичних лідерів та управлінських кіл (докладно див. [8; 9]).

Провідний принцип стратегії гібридної війни – забезпечення максимальної концентрації ресурсів на вразливих ділянках з метою гарантованої дестабілізації політичного та військового керівництва держави-жертви, її соціально-економічних структур, культурно-світоглядної сфери з подальшим скасуванням реального суверенітету та передачею під зовнішнє управління (докладно див. [10]).

Зробимо спробу виокремити кілька стратегічних етапів алгоритму розгортання гібридної війни:

- 1) здійснення державою-агресором стратегічної розвідки із виявлення слабких і вразливих ланок у забезпеченні оборони, внутрішньої та зовнішньої безпеки потенційного об'єкта агресії;
- 2) формування комплексу гібридних загроз з урахуванням місцевої специфіки, створення позицій впливу в управлінській та інших соціально значущих сферах життєдіяльності держави;

¹ Джон Уешлі Уорден III (нар. 1943 р.) – полковник у відставці, якого називають провідним теоретиком ВПС США другої половини XX ст. Брав участь у розробленні низки ударних повітряних операцій США (зокрема, проти Лівії в 1986 р., операції «Миттева блискавка» – повітряної частки операції «Буря в пустелі» у 1991 р.), інноваційних підходів до сучасних війн, проектування довгострокових кампаній. Розробив системний підхід до бойових дій – операції на основі ефектів, суть якої настановою про першочергову концентрацію зусиль не на власне розгромі сил супротивника, а на деморалізуючому впливі на свідомість останнього.

3) реалізація послідовного руйнівного впливу на ключові сфери військового, адміністративно-політичного управління, економічний лад та інформаційно-ментальну сферу за допомогою інформаційної зброї, спеціальних операцій, активізації «п'ятої колони» тощо;

4) організація скоординованих дій внутрішньої деструктивної опозиції, радикально-екстремістських формувань для дестабілізації ситуації, створення гострої політичної кризи й технологічного стимулювання «мирних» масових протестних акцій для повалення існуючого ладу (правлячої адміністрації) або кардинальної зміни політичного курсу держави;

5) (як варіант) розгортання неоголошених військових дій та підривних операцій з допомогою місцевих заколотників, сепаратистів, етнорелігійних фанатиків, носіїв екстремістської ідеології при наданні їм фінансування, зброї, інформаційно-політичної підтримки, а також залученні найманців, інструкторів, організації дипломатичного тиску тощо;

6) висування у випадку поразки або поступливості жертви ультимативних вимог щодо повної капітуляції або часткового задоволення вимог, або (у разі фіаско гібридного наступу) – зміна тактики, переведення конфлікту у відкладений («заморожений») стан.

Що стосується форм і методів гібридної війни, то їм властиве нове концептуальне поєднання та застосування сукупності новітніх і традиційних, військових і невійськових методів протиборства, які становлять основу ГВ як принципово нового типу конфліктних відносин у сучасному світі (див. також [11; 12]).

Для інструментарію гібридної війни властиві стирання граней між війною і миром, реальними і віртуальними типами протиборства, сполучення «твердої» і «м'якої» сили.

До основних форм ведення гібридної війни можуть належати, зокрема:

- тривалі за часом, непрямі дії політичного, інформаційного, економічного, розвідувально-підривного характеру, які можуть принести ініціаторам ГВ бажаний кінцевий результат;
- проведення після підготовчого періоду послаблення країни-жертви масштабної кампанії з пріоритетним застосуванням силового тиску

в супроводі інших методів ГВ (пряма або прихована збройна агресія, заколоти, державний переворот тощо);

- інспірування внутрішньої дестабілізації й досягнення контролю (керованості) над політичним життям країни-жертви без прямого збройного втручання заздалегідь підготовленими внутрішніми деструктивними силами та завдяки дезорієнтації населення.

Провідними методами гібридної війни можна вважати:

- приховані військові дії збройних сил, сил спецоперацій того чи того масштабу;
- бойові, диверсійно-терористичні дії підконтрольних агресору іррегулярних збройних формувань (ІЗФ), наприклад, повстанських рухів, озброєного підпілля, терористичних, кримінальних угруповань тощо;
- політико-дипломатичний тиск;
- методи економічної війни та підризу економічного потенціалу країни-жертви;
- формування внутрішньої деструктивної опозиції, створення сильних позицій впливу в органах влади, управління, силових структурах, ЗМІ, партійно-політичній сфері країни-жертви;
- масштабну інформаційно-психологічну війну;
- розвідувально-підризу діяльність спецслужб.

Окремого дослідження потребує модельний варіант гібридної війни, який спирається на дестабілізацію внутрішньої ситуації країни-жертви та проведення державного перевороту в тій або тій формі (також і практично безкровною формою). У цьому разі повалення легітимної влади базується на комплексному застосуванні витончених технологій щодо маніпулятивного управління масовою свідомістю, конструювання поведінки великих людських спільнот («мас») та управління нею, створення деструктивної опозиції й незаконних парамілітарних формувань.

Світовий та вітчизняний досвід останнього десятиліття дають змогу виокремити такі елементи алгоритму дестабілізаційних дій:

- 1) виявлення уразливих ланок державного організму та визначення стратегії підризних дій;

- 2) визначення джерел фінансування дестабілізаційної кампанії;

- 3) виявлення або інспірування, консолідація протестних суспільних груп та їхніх ватажків (функціонерів, активу), створення в столиці та регіонах держави опорних структур для переходу до силового етапу;

- 4) створення мережових структур з усебічної підтримки (міжнародно-політичної, організаційної, інформаційно-психологічної, інструкторської, матеріально-фінансової, розвідувально-безпекової) антиурядової опозиції, неурядових організацій;

- 5) формування механізмів для організації заворушень, антиурядових виступів, включно мобілізацію, озброєння, розгортання заздалегідь підготовлених формувань бойовиків тощо.

Фахівці-безпекознавці пропонують комплекс заходів із відвернення стратегічної неочікуваності сучасних підризних технологій, що передбачає:

- виявлення індикаторів, які сигналізують про наближення та ступінь загроз штучної дестабілізації суспільно-політичної системи, системи управління державою, духовно-світоглядної сфери народу;
- своєчасну «інвентаризацію» уразливих ланок життя держави і суспільства, аналіз характеру та спрямованості гібридних загроз;
- розроблення загальнодержавної та відомчої нормативно-правової, концептуальної та розпорядчо-директивної бази протидії відповідним загрозам, у т. ч. корегування конституційно-правової бази держави;
- навчання кадрів (управлінських і спеціальних), які здатні протистояти загрозам нового типу;
- підготовку відповідних відомств, інших елементів сектору безпеки та оборони держави до відсічі профільним загрозам, створення інтегрованої системи їх спільних дій тощо.

Мілітарний компонент конфліктів майбутнього

Можна впевнено стверджувати, що в структурі гібридної війни суттєве значення зберігатимуть власне бойові дії, передовсім сухопутного характеру. Так, за деякими оцінками, у локальних кон-

фліктах та війнах 1991–2015 рр. загинуло понад 1 млн людей. Основною формою ведення бойових дій у гібридних війнах залишається, на думку дослідників, загальновійськовий бій із розмаїттям тактичних прийомів, які застосовують винахідливо й нестандартно¹.

У бойових діях неконвенційних війн зростатимуть значення вогневого ураження, зокрема розвідувально-ударними комплексами високоточної зброї, реактивними системами залпового вогню, ствольною артилерією з керованими боєприпасами тощо, показників забезпечення піхоти ПТРК та ПЗРК, БЛА тактичної ланки, тактичними ПЕОМ, що в сукупності перетворює сухопутні підрозділи на єдиний інтегрований організм.

В армії США нині розробляють концепцію автономних роботизованих систем на основі «партнерства між людьми й роботами, які працюють на підставі синергетичних команд» у складі 150 військовослужбовців та 2000 роботів. «Війни шостого покоління» розраховані на виведення з ладу систем управління та життєзабезпечення розвинутих країн із достатньо сильними «традиційними» арміями. У перспективі розглядається можливість творення розвідувально-ударних комплексів із літаків-роботів та «роботоподібних» піхотинців (з комп'ютеризованими бойовими скафандрами та екзоскелетами). Відомий футуролог Е. Тоффлер ще 1993 р. пропонував поєднати такі високотехнологічні підрозділи з новим типом організації та управління (таким, що фактично виводив би їх навіть з-під формального державного контролю), створивши наймані сили багатонаціональних добровольців під командуванням «транснаціональних рад директорів», із правом вести локальні бойові дії, спецпропаганду, спецоперації щодо місцевих еліт. Подібні формування, писав Тоффлер, могли би «покрити земну кулю миротворчими організаціями з високою мотивацією» та «самоокупністю».

Бойові дії в гібридній війні набувають певних характерних властивостей, серед них:

- непостійна й незначна чисельність збройних формувань ворогуючих сторін (до 30–60 тис. вояків), а простір бойових дій обмежується десятками чи двома-трьома сотнями кілометрів;
- «клаптиковий» характер бойових дій, ведення протиборства за одночасного збереження господарської діяльності населення;
- відсутність суцільної лінії зіткнення військ, нечіткі обриси фронту й тилу, орієнтація дій військ на захоплення й утримання важливих населених пунктів, транспортних вузлів, доріг, опора на мережу потужних блокпостів (взводних, ротних опорних пунктів з підтримкою танків та артилерії) тощо;
- зростання організаційно-управлінської самостійності підрозділів і частин, інтеграція на тактичному рівні різнорідних підрозділів за типом ротних, батальйонних, бригадних тактичних груп, створення міжвидових угруповань військ на оперативному-тактичному рівні;
- різке зростання вогневої потужності підрозділів (частин) та зменшення щільності бойових порядків, вогневий зв'язок (взаємопідтримка) військ на значній відстані (30–70 км), поява нових тактичних прийомів – «вогневого обрамлення», «вогневого прочісування» тощо;
- висока маневреність (аеромобільність) військ, зростання ролі ініціативних, рейдових, автономних дій;
- суттєве зростання ефективності та значення розвідувально-диверсійних дій, спецпропаганди, співробітництво (забезпечення лояльності) з місцевим цивільним населенням;
- значна питома вага партизанських дій (улаштування засідок, диверсій, нальотів, боротьба на комунікаціях, мінні й терористичні війни тощо), які здійснюються власне іррегулярними формуваннями, у т. ч. створеними та підготовленими спецвійськами регулярних сил, та, відповідно, антипартизанських дій;
- участь у бойових діях іррегулярних проксіформувань на службі у певних держав, найманців, співробітників приватних військових компаній;
- інтенсивне ведення радіоелектронної боротьби, забезпечення оперативного надходження у війська даних космічної, повітряної, спеціальної (від військ спецпризначення та партизанських формувань, «п'ятої колони» у підпіллі), морської, стратегічної агентурної розвідки; характерним для ГВ є те, що іррегулярні учасники можуть отримувати матеріально-технічне, кадрове й розвідувальне забезпечення можливостями потужних армій великих держав, які зацікавлені в певному розвитку неконвенційного конфлікту;

¹ Огляд воєнних компонентів ГВ подано за [13–17].

- готовність до ведення бойових дій в урбанізованому просторі;
- зростання небезпеки страждань і кількості жертв серед мирного населення, порушень права війни, військових злочинів, застосування протиправних методів ведення війни та «умиротворення» населення;
- одночасне бойове застосування високотехнологічних і застарілих систем (зразків) озброєння.

З'явилася можливість визначати й ставити завдання щодо стратегічного рівня управління на тактичному, навіть безпосередньо засобами вогневого ураження в режимі наближеного до реального часу. Це стосується тактичної ланки «окрема бойова машина – підрозділ» (взвод, рота). Так, Армія оборони Ізраїлю з 2021 р. переозброюється новими танками «Меркава-4 Барак», здатними обробляти інформацію від десятків датчиків та надавати її, вже проаналізовану, командирів машини в порядку важливості. Бойова машина, повністю керована 46 комп'ютерами, оснащена засобами віртуальної реальності, що вмонтовані в систему управління, а також системою попередження про небезпеку. Особливий електронний «мозок робота» виконує функції штучного інтелекту. До слова, модернізовані російські танки Т-90М «Прорив» інтегровані в мережевоцентричну систему тактичного управління, т. зв. «армійський Інтернет», що об'єднує на полі бою всі об'єкти, оснащені такими комплексами, видає цілевказівки екіпажу тощо.

Для воєнних конфліктів сучасності стало характерним залучення тактичних сил і засобів до виконання оперативно-стратегічних і стратегічних завдань. Взаємозв'язок у формах і способах застосування виникає не тільки між стратегічним і оперативним чи оперативним і тактичним рівнями, але й між стратегічним і тактичним. Тому в сучасних умовах тактичні дії військових частин (підрозділів) впливають не лише на розвиток тактики, а й на стратегію, воєнно-стратегічну обстановку та політичну ситуацію в країні у цілому.

Загалом поглиблене вивчення застосування Збройних Сил України (ЗСУ) у конфлікті на сході України уможливило дійти нових теоретичних висновків (узагальнень) щодо характеру воєнної компоненти гібридних конфліктів. Зокрема з'ясовано, що з появою нових видів зброї, насамперед керованої та високоточної, та пов'язаними із цим змінами в характері збройної боротьби, в 1970–1980-ті рр. минулого сторіччя стратегічні завдан-

ня воєнних конфліктів могли вирішуватись оперативними й тактичними угрупованнями військ. Завдяки стрімкому розвитку засобів розвідки, зв'язку, об'єднанню їх в автоматизовані системи управління військами та зброєю ущільнились інформаційні потоки та значно скоротився цикл управління. Завдання щодо стратегічного рівня управління вже можливо ставити навіть безпосередньо засобами вогневого ураження в режимі часу, що наближений до реального.

Синергія бойового застосування збройних сил підсилюється розробкою новітніх тактичних алгоритмів, що спираються на організаційно-технологічні інновації у військовій справі. Зокрема, для стратегії та арсеналу гібридних війн у сучасних умовах все більше значення набуває мережевоцентричне протистояння: 1) перетворення глобального простору на інтегрований театр протистояння; 2) руйнівний вплив на комп'ютерні мережі, автоматизовані системи управління супротивника; 3) застосування новітніх способів організації й управління деструктивними силами, що використовуються в ГВ.

Нова концепція ведення війн на засадах мережевоцентричності була розроблена Офісом реформування збройних сил міністра оборони США під орудою віце-адмірала Артура К. Сібровскі. Її активно впроваджували в практику ведення бойових дій США в Іраку та Афганістані. На думку розробників, ця концепція у майбутньому, «якщо не замінить традиційну теорію війни, то суттєво й невідворотно змінить її». Ключовим є поняття «мережа» – новий інформаційний простір, у якому розгортаються стратегічні операції військового, дипломатичного, медійного та економічного характеру. При цьому бойові одиниці, системи зв'язку, розвідка й контррозвідка, дипломатичні кроки, обробка суспільної свідомості, психологічні операції та етнопсихологічні конструкції, наука й релігійна сфера оголошуються взаємопов'язаними елементами єдиної мережі. Війна перетворюється на мережеве явище, де інформація циркулює постійно.

Концепція «мережевоцентричної війни» дозволяє вести не обмежену національними та географічними кордонами війну, що вражає як військові, так і цивільні мережі в мирний та воєнний час. Комп'ютери та їх мережі стають безпосереднім об'єктом бойових дій. Зламування військових та цивільних мереж супротивника, вчинене спеціально підготовленими хакерами, здатне дезорганізувати систему військового управління, енергетич-

ної, транспортної систем, повітряного сполучення, призвести до людських жертв і масштабного економічного збитку, посіяти паніку й антиурядові настрої в мешканців урбанізованого простору сучасних держав.

Спецслужби та сили спецоперацій у сценаріях неконвенційного протидіювання

У гібридній війні цілеспрямовано застосовуються дії спеціальних служб у вигляді сукупності скоординованих заходів (акцій) розвідувального, контррозвідувального, диверсійного, інформаційно-психологічного та іншого характеру різної тривалості й інтенсивності, які здійснюють кадрові працівники спеціальних служб і створений ними апарат негласних помічників відповідно до загального задуму ГВ¹.

При цьому в рамках сценаріїв гібридної війни можна виокремити такі основні функції (задачі) спецслужб:

- довгострокове й цілеспрямоване збирання за допомогою оперативно-технічних, агентурно-оперативних і легальних методів інформації про стан об'єкта агресивних дій, становище на потенційному або реальному театрі проведення ГВ;
- інформаційно-аналітичне та прогностичне забезпечення відповідних спеціалізованих державних структур і ситуативних управлінських (координаційних) органів з організації та ведення асиметричних підливних дій проти інших держав;
- створення сталих позицій прямого чи опосередкованого впливу в суспільно-політичних, управлінських, фінансово-економічних, військових, медійних та інших сферах у спосіб вербувального або прихованого залучення до співробітництва громадян іноземних держав, які за своїм статусом (можливостями) можуть бути використані (сприяти) реалізації сценаріїв ГВ;
- залучення до інспірування державних переворотів, заколотів, масових акцій та інших дій, що здатні призвести до насильницького повалення легітимної влади, тривалої дестабілізації ситуації в державі;
- участь у створенні й управлінні роботою неурядових (легальних і незаконних) організацій, рухів, засобів масової інформації, навчально-тренувальних структур та інших суб'єктів суспільно-політичного життя, чия діяльність підпорядкована загальній стратегії непрямих підливних дій;
- участь у створенні необхідних структур, підготовці кадрів та безпосередньому веденні інформаційної (інформаційно-психологічної) війни;
- налагодження та підтримка каналів незаконного фінансування антидержавних сил (структур), включно бойових і терористичних формувань, перекидання зброї, диверсійних засобів, інформаційної продукції тощо для забезпечення їх незаконної діяльності;
- організація професійної підготовки та виховання спеціалістів (організаторів) розвідувально-диверсійних, терористичних акцій, спецпропаганди та інших деструктивних дій, їх нелегальне перекидання на театр дій ГВ;
- безпосереднє здійснення диверсійних, терористичних акцій, організації масових заворушень, повстань та інших особливо небезпечних злочинів проти державного ладу;
- контррозвідувальний захист власних спецслужб і створених ними антиурядових формувань від оперативної діяльності розвідувальних органів супротивника тощо.

Виняткового значення в гібридній війні набуває застосування сил спеціальних операцій (ССО). Його провідною формою є спеціальні операції, що проводяться спеціально організованими, навченими та озброєними військовими або іррегулярними силами для досягнення воєнних, політичних, економічних чи інформаційних цілей нетрадиційними військовими засобами у зайнятих супротивником або політично нестабільних районах. Ці операції ведуться самостійно чи скоординовано з операціями решти збройних сил.

Нерідко ССО використовують у тісній взаємодії зі спеціальними службами та антиурядовими парамілітарними формуваннями (повстансько-партизанськими, терористичними, організованими злочинними тощо), зокрема з метою здійснення спеціальної розвідки в інтересах власних військ та інших суб'єктів ГВ; виведення з ладу систем державного та військового управління; знищення

¹ Про трансформацію сучасних спецслужб див. [18].

(захоплення) штабів, важливих військових об'єктів, об'єктів тилу збройних сил тощо; паралізувати роботу транспорту та життєво важливої інфраструктури; проведення диверсійних дій у тилу збройних сил, терористичних актів проти представників командного складу та державного апарату, захоплення в полон воєначальників і командирів; проведення спеціальних інформаційно-психологічних операцій для підриву морально-психологічного стану військовослужбовців та населення країни, що є жертвою ГВ; організації бойової та спеціальної підготовки незаконних (ірегулярних) збройних формувань із числа громадян країни, що стала жертвою гібридної агресії, найманців, іноземців та осіб без громадянства – учасників збройних конфліктів у «гарячих точках» світу тощо.

Залежно від конкретного прояву гібридної війни, особливостей структури військової організації певної держави в неконвенційних діях можуть брати участь окремі частини (підрозділи) військ спеціального призначення або високомобільних сил («командос», повітряно-десантні, десантно-штурмові, аеромобільні підрозділи), а за наявності ССО як самостійного компонента збройних сил можливе комплексне застосування функціональних спецпідрозділів – спеціальної (глибинної) розвідки, розвідувально-диверсійних, інформаційно-психологічних операцій тощо.

Аналіз сучасних військово-теоретичних поглядів на застосування ССО у війнах (конфліктах) нового концептуального типу дає можливість виокремити основні задачі, які елітні війська можуть здійснювати за умов ГВ [19; 20]. Зокрема, спецпризначенці:

- *на етапі підготовки й розгортання неконвенційної війни:* організовують антиурядові виступи, повстанські й партизанські рухи з метою дестабілізації обстановки в окремій країні та повалення її уряду; захоплюють або ліквідують політичних, державних та військових діячів, які здатні відігравати провідну роль в організації відсічі агресії; проводять диверсії та акти саботажу; збирають розвідувальні відомості політичного, економічного та військово-стратегічного характеру; формують партизанські (повстанські) загони, здійснюють підготовку партизан (повстанців); накопичують, розподіляють і приховують зброю та засоби матеріально-технічного забезпечення в районах, де в майбутньому планується розгортання партизанських баз; захоплюють полонених і заручників; проводять психологічні операції; діють на території іноземної держави у складі антиурядових органів самоврядування;

- *на етапі ведення повномасштабної асиметричної війни:* збирають розвідувальні відомості в інтересах угруповань своїх військ на театрі воєнних дій; виводять із ладу або захоплюють важливі військові та промислові об'єкти в тилу супротивника з використанням як звичайної, так і зброї масового ураження; проводять рейди й улаштовують засідки в тилу супротивника; виводять із ладу комунікації, системи державного, військового управління й тилового забезпечення; наводять з використанням радіо- й лазерних навідників високоточну зброю на особливо важливі об'єкти супротивника; проводять диверсії, акти терору, саботажу та психологічні операції для послаблення тилу, деморалізації особового складу і населення супротивника; виявляють, викрадають або знищують певні види зброї чи важливі елементи, зразки техніки та озброєння, таємні документи; організовують втечу з полону своїх військовослужбовців та цивільного персоналу; проводять пошуково-рятувальні операції.

«Дикі гуси» на полях гібридної війни

Ще однією важливою часткою стратегії, форм і методів гібридної війни стало цілеспрямоване використання приватних військових компаній (ПВК). Це – недержавні структури, що виконують широкий спектр послуг: від підготовки й навчання військовослужбовців до проведення військових операцій. Окрім назви ПВК, використовують також інші: приватизовані військові фірми, військові контрактори.

За ступенем навченості та оснащеності ПВК фактично стали різновидом ССО, мало поступаючись їм та експедиційним формуванням збройних сил провідних держав. Співробітники ПВК відіграли помітну роль у низці державних переворотів, створенні обстановки «керованого хаосу» в ресурсних регіонах Африки південніше Сахари, на Близькому Сході, у Центральній Азії, Південній Америці. ПВК діють у понад 100 країнах світу, вони фактично є учасниками всесвітнього ринку військових послуг, утворюючи його специфічний сегмент. За даними Брукінгського інституту (США), прибутки ПВК щорічно становлять 180 млрд дол.

До ПВК переважно залучають висококваліфікованих, досвідчених армійських офіцерів, колишніх співробітників спецслужб та військ спеціального призначення, інших профільних спеціалістів, зокрема психологів, фахівців у галузі комп'ютерних технологій, дестабілізації банківських систем. За оцінками, загальний кадровий потенціал ПВК в сучасному світі становить 2 млн співробітників.

Високий рівень бойової та спеціальної підготовки, відсутність стримуючих правових і моральних норм, тіньовий характер діяльності та складність доведення причетності до реалізації державної політики перетворює ПВК на вельми ефективне, хоча й витратне, знаряддя прихованої гібридної війни. У рамках стратегії неконвенційної війни ПВК можуть використовуватися для здійснення державних переворотів, ведення безпосередніх бойових дій, проведення розвідки, організації диверсійно-терористичних акцій, брутальних провокацій, бойової та спеціальної підготовки незаконних збройних формувань, охорони ватажків закатників, тероризування (залякування) населення, забезпечення незаконного постачання зброї та боєприпасів тощо [21; 22].

«Універсальні солдати» бойовищ постмодерну

Одним із центральних елементів неконвенційної конфліктності, та, одночасно, її технологічною новацією є використання неурядових організацій (НУО) та рухів. Це неодмінний складник арсеналу гібридної війни, який зосереджений на створенні й підготовці легальними та незаконними методами керованих з-за кордону різноманітних неурядових (громадських) самодіяльних організацій (товариств, фондів, культурно-просвітницьких, аналітичних, етнорелігійних, молодіжних, спортивних та інших організацій і рухів, засобів масової інформації тощо). Їм відведена відповідна функція в загальному плані дестабілізації (поваленні) легітимного державного ладу, порушенні територіальної цілісності країни-жертви, реалізації інших частин загального задуму ГВ. До відомих дестабілізаційних доктрин, у яких важливе місце відводиться «незалежній опозиції», належить доктрина «керованого хаосу».

Активну роль у формуванні, підготовці й управлінні такими структурами відіграють спецслужби та підконтрольні їм зарубіжні організації, аналітичні центри. Країни – ініціатори гібридної війни для підтримки (захисту) протиправних дій неурядових організацій можуть здійснювати на уряд країни-жертви дипломатичний, інформаційний, економічно-санкційний тиск, проводити спеціальні акції впливу з метою деморалізації політичного керівництва та командного складу силових структур, їх підкуп, демонстрації військової сили тощо.

Сценарії ГВ з використанням мережі НУО особливо ефективні в країнах з високим рівнем корупції та соціальної несправедливості, нестабільною по-

літичною, етноконфесійною ситуацією, відцентровими тенденціями в територіальному устрої, відсутністю доступу до якісної освіти та занепадом загальнокультурного рівня населення, поширеними деструктивними ідеологіями тощо.

Зазвичай фінансування неурядових організацій здійснюється з-за кордону через фонди, що легально існують, а також із залученням ресурсів опозиційно налаштованих фінансово-промислових груп, мафіозних угруповань, злочинних співтовариств. Упродовж тривалого періоду до цих організацій добирають функціонерів та активістів, на семінарах, курсах, тренінгах навчають їх (із визначенням спеціалізації та організаційно-тактичного рівня майбутньої діяльності) методів конспірації, роботи з людьми, способів виготовлення інформаційно-пропагандистських матеріалів, інспірування вуличних акцій протесту та «громадянської непокори», дискредитації влади та її силових структур, організації масових заворушень, інших деструктивних акцій.

Створюється мережа (без видимого керівного центру) спеціалізованих НУО. Залежно від національної специфіки країни, конкретної соціально-політичної ситуації та ступеня опору влади визначають співвідношення «мирних» та насильницьких дій НУО.

У сучасних умовах великого значення набувають: управління НУО через соціальні мережі; формування т. зв. «кліпової свідомості» людей, особливо молоді, що позбавляє особистість раціональних механізмів мислення й здатності до аналізу причинно-наслідкових зв'язків дійсності, значно полегшує управління ситуативно створеними спільнотами; поширення інформації (зокрема неправдивої), яка підриває довіру до влади, деморалізує управлінський та силовий апарат; розроблення символіки й закодованих інформаційних імпульсів («мемів»), що спонукають до дії; використання технологій впливу на підсвідомість людей, включно поширення чуток і паніки, застосування музики, ритмів, світлових ефектів; формування образів «сакральних жертв режиму» тощо.

Тактика й технології послуговування НУО в рамках стратегії антиконституційних дій (у варіанті т. зв. «стратегії зламу») може розподілятися на кілька етапів:

- 1) підготовчий (збирання необхідної інформації; визначення джерел фінансування; формування гасел і настанов; установа контролю

над ЗМІ, організаціями систем зв'язку та управління; підготовка активістів, блогерів, бойовиків, спеціалістів з агітації, розвідки, безпеки, взаємодії зі ЗМІ, роботи з різними категоріями населення, логістики; визначення об'єктів ударів тощо);

- 2) формування «організованого протестного руху» на базі існуючих НУО, підготовлених до відповідних місій кадрів, використання підконтрольних ЗМІ та соціальних мереж;
- 3) провокування події-інциденту, здатного спричинити масове суспільне обурення та вивести людей на вулицю, створити суспільну турбулентність, яку неможливо розрядити ординарними способами легітимної комунікації між дискредитованою державою та населенням;
- 4) конфліктної мобілізації та формування «політичного натовпу» як окремого табору громадянського конфлікту (він де-факто має риси «окремої політичної нації»), який радикально протиставляє себе державі, її прихильникам та пасивній більшості населення;
- 5) висування ультимативних вимог до влади та вирішальний тиск (штурм), форми й результати якого залежать від позиції влади, її здатності й готовності до опору, підтримки її законослухняним населенням тощо.

Синергетичні можливості застосування НУО та штучно (технологічно) створених людських спільнот із наперед визначеними соціоментальними та поведінково-психологічними характеристиками продемонструвала хвиля заколотів, заворушень, повалень легітимних урядів, тривалої дестабілізації, кровопролиття та відкидання назад у цивілізаційному поступі.

Радикально-екстремістські організації також відіграють помітну роль у стратегії неконвенційної конфліктності. Їх місія полягає в цілеспрямованому використанні, створенні, підготовці й усебічній підтримці антиурядових, переважно озброєних рухів, організацій, осередків, які сповідують радикальні ідеологічні погляди та надають перевагу насильницьким методам досягнення своїх цілей.

Подібні угруповання можуть виникати на етноконфесійному, ідейному, територіально-сепаратистському, кримінальному, корпоративному ґрунті. Спеціальні служби та інші зацікавлені структури держав – ініціаторів ГВ можуть надавати радикаль-

ним угрупованням усебічну підтримку для якісного посилення їхніх деструктивних можливостей, створювати подібні угруповання для виконання відповідних завдань, зокрема таких, які мали б покладатися на профільні підрозділи регулярних армій або спецслужб.

За умов розвитку етноконструктивістських технологій, або т. зв. «етнічної зброї» (формування нових спільнот із наперед визначеними ідейними та соціально-психологічними властивостями, відповідними фобіями), у стратегії асиметричного протистояння зростає значення штучного творення радикальних антиурядових організацій на етноконфесійному ґрунті, а також іредентистських і сепаратистських рухів. Як свідчить світовий досвід останніх десятиліть, міжнаціональні й релігійні конфлікти, спровоковані із застосуванням цих рухів, надзвичайно складні для врегулювання, здатні спричинити численні жертви, призвести до втрати реального суверенітету й територіальної цілісності, розпаду громадянських спільнот.

Сприятливим середовищем рекрутування «живої сили» деструктивних акцій в умовах урбанізації, а також зубожіння значної частки населення, зниження його культурного рівня та відсутності привабливої ідеології громадянської консолідації слугують молодіжні неформальні організації та рухи, наприклад, фан-клуби, «ультрас», ультранаціоналістичні, неонацистські формування, деструктивні секти, «бійцівські клуби», підконтрольні мафіозним структурам «вуличні банди» та ін.

Економічна зброя сучасності

Не можна обминути увагою економічний компонент гібридної війни, що передбачає комплекс прихованих або відкритих заходів, які здійснюються відповідно до загального задуму ГВ з метою дестабілізації продуктивних сил, фінансово-економічної сфери, економічного базису обороноздатності держави, підризу соціальної стабільності суспільства, ураження позицій держави, що стала жертвою гібридної війни в міжнародних економічних відносинах тощо.

Економічна зброя сучасності може охоплювати такі форми: санкційний тиск; валютно-фінансові махінації; стимулювання боргової залежності; закриття власних ринків для експорту інших держав; розривання традиційних економічних зв'язків, трудову міграцію; заборону на постачан-

ня технологій експорту важливих для партнерів сировини й продукції; торговельно-економічне ембарго; збільшення митних платежів; цілеспрямовану дискредитацію економічного реноме держави у світі; приховане нав'язування завідомо руйнівних для національної економіки моделей економічного розвитку тощо. Засобами економічного знесення можуть слугувати нав'язування гонки озброєнь, провокування локальних сутичок і стану напруги, спонукання до збільшення витрат на посилення охорони кордонів, посилення мобілізаційного тягаря на економіку.

Знаряддя ураження свідомості еліти

До арсеналу гібридної війни увійшла т. зв. «організаційна зброя». Це узагальнена назва комплексу невійськових методів протидії, часто-густо довгострокового характеру. Вони повною мірою властиві стратегічному рівню ГВ, можуть здійснюватись у відкритий або протизаконний спосіб. Метою застосування організаційної зброї є самодезорієнтація та самодезорганізація супротивника, хаотизація державного та суспільного життя, втрата жертвою ГВ здатності до опору через глибинну ерозію управлінської та ідейно-духовної сфери.

Особливе значення надається досягненню прихованого управління культурно-світоглядною сферою (з використанням технологій інформаційно-мережевого впливу локального та глобального масштабу), яке здійснюється з метою перекодування ментального поля населення країни-жертви у спосіб переорієнтації, послаблення та знищення традиційних духовних і культурних цінностей народу, ерозії його етнорелігійної матриці.

Цей специфічний вид організаційної зброї паразитує на свободі слова, інформаційній відкритості сучасних демократичних суспільств, глобальних інформаційних зв'язках, наявності мережі Інтернет, соціальних мереж, міжнародному культурно-освітньому обміні, зацікавленості багатьох держав у залученні зарубіжної допомоги (фінансування) для підготовки науково-педагогічних кадрів, фахівців сучасних гуманітарних спеціальностей тощо.

Інструментарій організаційної зброї тісно пов'язаний з інформаційним впливом та діяльністю неурядових організацій, базується на організаційно-управлінських, інформаційних, культурологічних, психологічних технологіях.

Як свідчить досвід глобального протистояння доби холодної війни, сучасних нетрадиційних конфліктів, організаційна зброя може передбачати:

- формування керованої ззовні, неадекватної в професійному та моральному відношенні «п'ятої колони» в органах державного, військового, безпекового управління, місцевого самоврядування, в інших значущих сферах управління країною і суспільством;
- нав'язування «самозгубних» моделей, концепцій розвитку економіки, демонтажу вітчизняного військово-промислового комплексу та системи науково-дослідних і дослідно-конструкторських робіт;
- стимулювання руйнації традиційної системи освіти, виховання, фундаментальної науки та центрів технологічного зростання;
- вживлення у масову свідомість, ментальну сферу, зміст освіти та масової культури чужорідних, таких, що суперечать цивілізаційній матриці народу, ідей, уявлень, цінностей та змістів;
- руйнацію традиційної моралі, сталих суспільних зв'язків, мобілізуючої морально-психологічної готовності народу до захисту власної безпеки та національних інтересів.

Важливим маніпулятивним елементом організаційної зброї є «когнітивна зброя», сутність якої полягає в досягненні інтелектуальної переваги над супротивником та маніпулюванні його свідомістю за допомогою наукових і псевдонаукових конструкцій. Когнітивна зброя як знаряддя сучасного конфлікту охоплює сферу вироблення й прийняття рішень та передбачення дій супротивника з урахуванням національної психології й ментальності, цивілізаційних факторів. Прогнозовані когнітивні впливи можуть застосовуватися для дискредитації інноваційних наукових розробок, упровадження яких може посилити обороноздатність і конкурентоспроможність країни-жертви, нав'язування через «п'яту колону» заздалегідь помилкових, тупикових концептуальних рішень у сфері управління та оборони, економічного розвитку тощо (*докладно див. [23; 24]*).

Комплекс технічних та організаційно-технологічних заходів у рамках стратегії гібридної війни, що спрямований на здобуття переваги в комп'ютерних мережах або виведення їх з ладу для підриву дієздатності супротивника, називають кібернетичною

війною. Вона щільно пов'язана з інформаційним протиборством, мережевоцентричним протиборством як одним із провідних форм ГВ (сюди ж спеціалісти відносять інформаційні дії, психологічні акції та кібернетичні атаки, скеровані як на структурні технічні компоненти держави, так і на свідомість її громадян). Поряд із поняттям традиційної радіоелектронної боротьби з'явилися нові: «операції в кіберпросторі», «кібервійна», «програмно-математична зброя», «інформаційні операції» та «інформаційна війна». Низка провідних країн та організацій світу (США, Велика Британія, Китай, Ізраїль, Росія, кіберцентр НАТО) створили в складі збройних сил і спецслужб штатні структури та підрозділи з кібернетичної війни та протидії їй.

Висновки

На межі XX–XXI ст. (зокрема, й на основі потужної спадщини планетарного протистояння суспільних систем та міжблокової конфронтації 1945–1991 рр.) склалися численні стратегічні, тактико-технологічні та інформаційно-когнітивні передумови для формування нового якісного типу конфліктності – гібридної як синтезування різноманітних новітніх форм і методів деструктивної діяльності та їх комплексного скоординованого застосування.

Проведений конфліктологічний аналіз інноваційних явищ межі XX–XXI ст. свідчить про те, що в цілому концептуальні схеми, стратегія й тактика гібридної війни як явища багато в чому є традиційними (стандартними) елементами збройного конфлікту або латентного протистояння держав (або держав і недержавних військово-політичних суб'єктів). Серед них – економічний тиск і санкції, інформаційна підготовка, політичне оформлення протиборчих сторін, методи таємної війни та робота спецслужб тощо. Тобто в основі сутності ГВ – широкий спектр конфронтаційних дій, до яких вдаються у рамках гнучкої стратегії з довгостроковими цілями, заснованих на комплексному застосуванні дипломатичних, інформаційних, воєнних та економічних засобів для дестабілізації супротивника. За подібною парадигмою може відбуватися протистояння між державами, між державою та іррегулярними збройними формуваннями, а також між державою та ІЗФ, що отримують допомогу (або інспіровані) ззовні.

Водночас стратегія й арсенал гібридної (асиметричної, неконвенційної) конфліктності в сучасному світі спираються на принципи якісні

зміни, що відбулись у концептуальних засадах, структурі, стратегії й тактиці, формах і методах військово-політичного протистояння між сучасними державами та їх блоками, державами та неурядовими формуваннями та ін., які сталися на межі XX–XXI ст. унаслідок радикальних змін у співвідношенні сил на міжнародній арені, хаотизації міжнародних відносин, появи нових видів летального та нелетального озброєння, інноваційних технологій конструювання й демонтажу соціальних спільнот, набуття сучасною війною (конфліктними відносинами) всеосяжного характеру з глобальним охопленням суходолу, Світового океану, повітряно-космічного простору, світової економіки та віртуально-інформаційного простору.

Подібне протистояння у своїй концептуальній основі спрямоване на деморалізацію супротивника, дистанційний підрив (переважно невійськовими й неконтактними методами) його спроможності до оборони й захисту національних інтересів загалом, примушування його до капітуляції, відмови від реального державного суверенітету, готовності до нав'язування йому вигідної переможцям моделі зовнішньої та внутрішньої політики, відповідного корегування суспільно-економічного ладу та духовно-культурної сфери.

Водночас узагальнення найбільш усталених наукових і науково-практичних поглядів дозволяє констатувати консенсусність у визнанні неодмінних елементів гібридної війни, як-от:

- неоголошеність, прихованість, відсутність оформлення відповідно до міжнародного права війни;
- створення із наперед визначеними характеристиками антиурядових організацій і рухів, незаконних збройних формувань і широке їх використання;
- експлуатація течій сепаратистського, ірредентистського, радикально-етноконфесійного характеру, екстремістських угруповань, деструктивних спільнот тощо;
- пріоритетна роль спеціальних служб, сил спецоперацій, залучення їх до створення потужної антиурядової інфраструктури дестабілізації (повалення) легітимного державного ладу;
- пріоритетна роль цілеспрямованого впливу на масову свідомість через масштабне застосування методів інформаційно-психологічного

протиборства, технологій створення кон'юнктурних соціальних суб'єктів із необхідними властивостями, обробки свідомості та управління великими соціальними спільнотами тощо;

- комплексне застосування інших методів невійськового тиску на державу-жертву, включно й дипломатичних, фінансово-економічних, гуманітарних та ін.

Новітні типи (моделі) неконвенційних небезпек спонукають держави до формування стратегії попередження та відсічі загрозам гібридної війни, тобто творення цілеспрямованої, унормованої стратегії спільної інтелектуальної й практичної діяльності держави та суспільства, спрямованої на попередження, мінімізацію загрози, безпосередню протидію та усунення наслідків ГВ, що може, зокрема, передбачати:

- формування довгострокової воєнно-політичної стратегії як основи протидії потенційним джерелам ГВ;
- створення спеціального державного органу для координації зусиль на загальнонаціональному рівні з протидії гібридним загрозам;
- підготовку (адаптацію) збройних сил, сил спеціальних операцій та спеціальних служб, правоохоронних та інших державних органів і громадських об'єднань до синергетичної протидії загрозам неконвенційного характеру;

- перекриття каналів фінансування та матеріально-технічного постачання деструктивних сил;

- використання на міжнародній арені зовнішньополітичних важелів, включно з міжнародними санкціями, для протидії державам, що вдалися до гібридної війни;

- організацію своєчасної розвідувальної та інформаційно-аналітичної роботи з метою виявлення підготовки асиметричних агресивних дій, безпосереднє розвідувально-інформаційне забезпечення протидії ГВ;

- захист електронних мереж і ресурсів від кібератак, масової свідомості – від деструктивних інформаційно-психологічних впливів, розвиток засобів інформаційного впливу на супротивника;

- забезпечення надійної охорони кордонів, зокрема відвернення незаконної міграції, створення непідконтрольних владі етнорасових анклавів у великих містах, етнічних організованих злочинних угруповань тощо;

- підтримання в належному функціональному стані мобілізаційної системи й територіальної оборони держави;

- запровадження інформаційно-просвітницької роботи з населенням щодо роз'яснення сутності, форм і методів гібридної війни, безпосередніх загроз подібних антидержавних дій.

Список використаних джерел

1. Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 № 92. URL: <https://zakon.rada.gov.ua/laws/show/92/2016#Text> (дата звернення: 11.08.2021).
2. Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 № 392/2020. URL: <https://www.rnbo.gov.ua/ua/Ukazy/4693.html> (дата звернення: 11.09.2021).
3. Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона», затверджена Указом Президента України від 25.03.2021 № 121/2021. URL: <https://www.president.gov.ua/documents/1212021-37661> (дата звернення: 11.08.2021).
4. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Дзеркало тижня. Україна*. 2015. 23 січ.
5. Мухаев Р. Т. Геополитика. М. : ЮНИТИ-ДАНА, 2010. С. 129.
6. Бартош А. Америка готовится к войнам будущего. Трансформации вооруженных конфликтов приведут к изменениям в стратегической культуре. *Независимое военное обозрение*. 2020. 17 июл. URL: https://nvo.ng.ru/gpolit/2020-07-16/10_1100_usa.html (дата звернення: 11.09.2021).
7. Веденеев Д., Слюсаренко А. «Гібридна» війна. Оформлення концептуальних поглядів на сутність конфліктності асиметричного типу. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2018. № 21. С. 28–46.

8. Арзуманян Р. Концепция операций, базирующихся на достижении эффектов. «21-й ВЕК». 2010. № 1. С. 71–116.
9. Савин Л. Новые способы ведения войны: как Америка строит империю. СПб. : Питер, 2016. 384 с.
10. Веденеев Д. В. Гібридна війна: щодо визначення поняття стратегії. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку* : зб. наук. пр. за матер. IV міжнар. наук.-практ. конф. (18 вересня 2020 р.). Острог, 2020. С. 10–19.
11. Веденеев Д. Від Макіавеллі до війн роботів: граматика «гібридної» війни. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2019. № 3. С. 27–38.
12. Веденеев Д. Партитура «гібридної» війни: вибір зброї. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2019. № 5. С. 16–29.
13. Беспилотный «Иноходец», танк «Прорыв» и стратегический «Кедр». *Независимое военное обозрение*. 2021. 4 окт. URL: https://nvo.ng.ru/nvo/2021-03-04/2_1131_week.html (дата звернення: 11.09.2021).
14. Гельман З. Четыре танкиста и робот. URL: https://mnenia.zahav.ru/Articles/10713/chetire_tankista_i_robot (дата звернення: 07.07.2021).
15. Кудрявцев А. Военные конфликты третьего тысячелетия. *Независимое военное обозрение*. 2016. 4 янв. URL: https://nvo.ng.ru/reality/2016-04-01/6_conflicts.html (дата звернення: 11.09.2021).
16. Основи планування операцій за стандартами НАТО / [М. В. Гребенюк, С. М. Салкуцан, Ю. П. Остах, А. І. Шигида]. Київ : НУОУ ім. І. Черняхівського, 2015. 120 с.
17. Тоффлер Э. Война и антивоина. М. : АСТ, 2005. С. 334–335.
18. Паливода В. О. Діяльність спеціальних служб іноземних держав у мінливому світі : зб. статей та аналіт. матер. Київ : НІСД, 2020. 336 с.
19. Слюсаренко А. В. Імовірний алгоритм застосування сил (військ) спеціальних операцій у конфлікті «гібридного» типу. *Військово-історичний меридіан*. 2017. № 4. С. 114–120.
20. Веденеев Д., Слюсаренко А. Сили спеціальних операцій: провідна сила війн майбутнього. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2020. № 3. С. 20–33.
21. Веденеев Д. Армія тіньової світобудови. Чи потрібні Україні приватні військові кампанії? *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2020. № 4. С. 11–25.
22. Веденеев Д. Армія тіньової світобудови. Чи потрібні Україні приватні військові кампанії? *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2020. № 5. С. 18–33.
23. Веденеев Д. «Вишукана» гібридна зброя: ураження свідомості керманичів та інтелігенції. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2020. № 9. С. 20–32.
24. Веденеев Д. «Вишукана» гібридна зброя: ураження свідомості керманичів та інтелігенції. *Виклики і ризики. Безпековий огляд Центру дослідження армії, конверсії та роззброєння*. 2020. № 10. С. 14–26.

References

1. Verkhovna Rada of Ukraine. *The Concept of Development of the Security and Defense Sector of Ukraine*, approved by the Decree of the President of Ukraine of March 14, 2016 No. 92. (2016). zakon.rada.gov.ua. Retrieved September 10, 2021 from <https://zakon.rada.gov.ua/laws/show/92/2016#Text> [in Ukrainian].
2. National Security and Defense Council of Ukraine. *National Security Strategy of Ukraine*, approved by the Decree of the President of Ukraine of September 14, 2020 No. 392/2020. (2020). rnbo.gov.ua. Retrieved September 11, 2021 from <https://www.rnbo.gov.ua/ua/Ukazy/4693.html> [in Ukrainian].
3. National Security and Defense Council of Ukraine. *Strategy of Military Security of Ukraine "Military Security – Comprehensive Defense"*, approved by the Decree of the President of Ukraine dated 25.03.2021 No. 121/2021. (2021). President of Ukraine Volodymyr Zelensky: Official website. Retrieved September 11, 2021 from <https://www.president.gov.ua/documents/1212021-37661> (дата звернення: 11.08. 2021).
4. Horbulin, V. (2015, January 23). «Hybrid War» as the key tool of the Russian geostrategy of a revenge. *Dzerkalo Tyzhnia. Ukraina* [in Ukrainian].
5. Mukhayev, R. T. (2010). *Geopolitics*. Moscow: UNITI-DANA, p. 129 [in Russian].
6. Bartosh, A. (2020, July 17). *America is preparing for the wars of the future. Transformations of armed conflicts will lead to changes in strategic culture*. *Nezavisimoe voennoe obozrenie*. https://nvo.ng.ru/gpolit/2020-07-16/10_1100_usa.html [in Russian].
7. Viedienieiev, D., & Sliusarenko, A. (2018). «Hybrid» war. Design of conceptual views on the essence of asymmetric type of conflict. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 21, 28–46 [in Ukrainian].
8. Arzumanyan, R. (2010). Concept of the Effects-based Operations. «21st CENTURY», 1, 71–116 [in Russian].
9. Savin, L. (2016). *New Ways to Wage War. How America Builds Empire*. St. Petersburg: Piter, 384 p. [in Russian].

10. Viedienieiev, D. V. (2020). Hybrid war: regarding the definition of a strategy. Proceedings of the IV International Scientific and Practical Conference *Education and science in the field of national security: problems and priorities of development (Ukraine, September 18, 2020)*. Ostroh, pp. 10–19 [in Ukrainian].
11. Viedienieiev, D. (2019). From Machiavelli to robot wars: the grammar of «hybrid» war. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 3, 27–38 [in Ukrainian].
12. Viedienieiev, D. (2019). The score of the «hybrid» war: the choice of weapons. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 5, 16–29 [in Ukrainian].
13. *Unmanned «Inokhodets», tank «Proryv» and strategic «Kedr»*. (2021, March 4). Nezavisimoe voennoe obozrenie. https://nvo.ng.ru/nvo/2021-03-04/2_1131_week.html [in Russian].
14. Gelman, Z. (n. d.). *Four tankers and a robot*. mnenia.zahav.ru. Retrieved July 07, 2021 from https://mnenia.zahav.ru/Articles/10713/chetire_tankista_i_robot [in Russian].
15. Kudryavtsev, A. (2016, January 4). *Third millennium military conflicts* Nezavisimoe voennoe obozrenie. https://nvo.ng.ru/realty/2016-04-01/6_conflicts.html [in Russian].
16. Grebeniuk, M. V., Salkutsan, S. M., Ostakh, Yu. P., & Shihida, A. I. (2015). *Fundamentals of Operations Planning According to NATO Standards*. Kyiv: The National Defence University of Ukraine named after Ivan Cherniakhovskiy, 120 p. [in Ukrainian].
17. Toffler, E. (2005). *War and Anti-War*. Moscow: AST, pp. 334–335 [in Russian].
18. Palyvoda, V. O. (2020). *Foreign special services' activities in a changing world*. Kyiv: NISD, 336 p. [in Ukrainian].
19. Sliusarenko, A. V. (2017). Possible Algorithm of Special Operations Forces (Troops) Usage in a «Hybrid» Type of Conflict. *Viiskovo-istorychnyi merydian*, 4, 114–120 [in Ukrainian].
20. Viedienieiev, D., & Sliusarenko, A. (2020). Special operations forces: the leading force of the wars of the future. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 3, 20–33 [in Ukrainian].
21. Viedienieiev, D. (2020). Army of the shadow universe. Does Ukraine need private military companies? *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 4, 11–25 [in Ukrainian].
22. Viedienieiev, D. (2020). Army of the shadow universe. Does Ukraine need private military companies? *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 5, 18–33 [in Ukrainian].
23. Viedienieiev, D. (2020). «Exquisite» hybrid weapon: damage to leaders' and intellectuals' mind. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 9, 20–32 [in Ukrainian].
24. Viedienieiev, D. (2020). «Exquisite» hybrid weapon: damage to leaders' and intellectuals' mind. *Vyklyky i ryzyky. Bezpekovi ohliad Tsentru doslidzhennia armii, konversii ta rozzbroiennia*, 10, 14–26 [in Ukrainian].