УДК 327.56:355.45:004.9
DOI https://doi.org/10.32782/app.v75.2025.19

О. Г. Капсамун
orcid.org/0009-0003-8252-6566
аспірант кафедри політичних теорій
Національного університету «Одеська юридична академія»

ГІБРИДНА ВІЙНА ЯК ІНСТРУМЕНТ ДОСЯГНЕННЯ СТРАТЕГІЧНИХ ЦІЛЕЙ ДЕРЖАВ

У сучасному світі гібридна війна дедалі частіше виступає інструментом досягнення стратегічних цілей держав, поєднуючи засоби військового, інформаційного, економічного, дипломатичного та кібернетичного впливу. Вона дозволяє агресору уникати прямої відповідальності, діючи у сірій зоні між миром і війною, використовуючи проксі-структури, дезінформацію та асиметричні методи. Особливої актуальності дослідження набуло в умовах російсько-української війни, яка є одним із найбільш показових прикладів гібридного протистояння у XXI столітті. Водночас світовий порядок, заснований на чітких нормах міжнародного права, стикається з викликами, що потребують переосмислення традиційних концепцій безпеки та війни. Гібридні загрози підривають не лише державний суверенітет, а й демократичні інститути, викликаючи потребу в адекватних політичних, правових і безпекових відповідях. Відтак постає необхідність ґрунтовного наукового аналізу гібридної війни як нового типу стратегічного інструменту, її форм, механізмів досягнення геополітичних цілей держав.

У контексті постійної трансформації міжнародних відносин гібридні методи набули статусу невід'ємного елементу сучасних конфліктів, демонструючи свою ефективність у досягненні стратегічних цілей без прямого застосування військової сили. Ця оновлена форма ведення війни становить серйозний виклик традиційним підходам до забезпечення безпеки та оборони, змушуючи держави адаптуватися до нових типів загроз і формувати відповідні стратегії реагування та захисту (Буряченко, 2024, с. 25).

Відзначимо, що гібридна війна залишається нечітко окресленим поняттям, яке в політичному та академічному середовищі часто використовується як узагальнення для різноманітних форм агресії, що не досягають рівня відкритого збройного конфлікту. До її інструментарію зазвичай зараховують дезінформацію, саботаж, підривну діяльність і кібератаки. Події на кшталт захоплення та незаконної анексії Криму Росією у 2014 році, масштабних кібератак часто наводяться як ілюстрація ефективного застосування гібридних засобів (Maschmeyer, 2023). Ці приклади викликали широкий інтерес серед дослідників, багато з яких почали розглядати конфлікти низької інтенсивності як домінантну форму збройного протистояння в майбутньому. Відповідно, політичні керівники включили ці підходи до оновлених стратегій національної безпеки.

Сучасне розуміння гібридної війни значною мірою базується на уявленні про вирішальну роль інформаційних технологій у підвищенні її ефективності. Вважається, що ці технології значно розширюють можливості ведення конфліктів у сірій зоні – зокрема завдяки використанню кібероперацій та інформаційного впливу через соціальні мережі. Кібератаки дозволяють дистанційно виводити з ладу критичну інфраструктуру, завдавати економічних збитків і порушувати системи зв'язку. У свою чергу, кампанії у соціальних мережах можуть створювати атмосферу паніки, провокувати хаос і впливати на громадську думку (Maschmeyer, 2023). Таким чином, держава-агресор може досягати стратегічних цілей без прямого застосування військової сили, що раніше було неможливо без збройного втручання.

У відповідь на цю загрозу країни адаптували свої оборонні стратегії. У 2014 році НАТО визначило протидію «гібридним загрозам» як один із ключових пріоритетів. Ці загрози розуміються як комбінація військових і невійськових, відкритих і прихованих засобів, включно з дезінформацією, кібератаками, економічним тиском, підтримкою нерегулярних воєнізованих формувань та використанням регулярних військ (Wales Summit Declaration, 2014).

Стратегія гібридної війни являє собою довгостроковий план досягнення перемоги шляхом формування загальних цілей, визначення напрямів дій та системного впливу на вразливі місця супротивника із використанням комплексу гібридних загроз. Вона розрахована на тривалий період і охоплює територію всієї держави, передбачаючи можливість переходу до відкритого застосування сили, як правило, лише на завершальному етапі конфлікту. При цьому активно використовуються чинні правові та нормативні механізми, пов'язані з миротворчими та кризовими операціями, що вимагає переосмислення традиційних підходів до збройних конфліктів нового покоління. На відміну від антитерористичних операцій, які зазвичай реалізуються в стислі терміни та мають чіткі показники успіху – як-от знищення терористичної мережі чи ліквідація її керівників, – у гібридній війні оцінка ефективності значно складніша, оскільки результати не завжди є очевидними. Саме тому участь у такій формі протистояння потребує розробки відповідної довгострокової політичної стратегії, яка виступає основою для комплексної боротьби з противником у межах гібридного конфлікту (Natura nestatală a războiului hybrid, 2020).

Метою стратегії гібридної війни є ослаблення держави-мішені. Для досягнення цього здійснюється серія операцій із використанням як військових, так і невійськових засобів та ресурсів. У рамках єдиного задуму та плану проводяться дії, спрямовані на підрив економіки, порушення функціонування систем зв'язку, деструкцію інформаційного простору та вплив на світоглядні орієнтири населення. Агресор діє приховано, атакуючи державні установи країни-мішені, а також завдає ударів у сферах економіки, інформації, культури та ідеології – без офіційного оголошення війни. Об'єктами атак також стають правоохоронні органи та регулярні збройні сили. На вирішальному етапі агресор переходить до відкритих бойових дій, у яких бере участь разом із місцевими повстанцями, найманцями та приватними військовими компаніями, забезпечуючи їх підтримкою через спеціальні підрозділи, постачання озброєння та фінансування (Mitręga, 2020, p. 196).

До етапів розробки та реалізації стратегії гібридної війни можна віднести: визначення мети та сенсу війни (сформулюється загальна стратегічна концепція, що пояснює причини, цілі та формат майбутніх дій проти держави-мішені); виявлення вразливостей супротивника (здійснюється комплексний аналіз слабких місць у системах внутрішньої та зовнішньої безпеки цільової держави); формування набору гібридних загроз (розробляється комплекс засобів впливу з урахуванням місцевого контексту, специфіки регіону та соціально-політичної ситуації); планування операцій та прогнозування контрдій (створюється стратегічний план, який передбачає демонстрацію слабкостей у політичній, адміністративній, економічній, фінансовій, культурній та ідеологічній сферах супротивника, а також оцінюються потенційні варіанти контрстратегії); послідовне руйнування ключових державних систем (організовується систематичний вплив на критичні сфери життєдіяльності країни, з особливим акцентом на економіку, фінанси, бойовий дух збройних сил і населення); розгортання прихованої збройної агресії (без офіційного оголошення війни агресор застосовує підтримку місцевих повстанців і сепаратистів, використовуючи зовнішнє фінансування, постачання зброї та спеціальні підрозділи, наприклад, анексія Криму в 2014 році); висунення ультиматуму (агресор вимагає повного підпорядкування держави-жертви та прийняття нових політичних умов, зазвичай під загрозою подальшої ескалації) (Mitręga, 2020, p. 197–198).

З огляду на багатовимірний характер гібридної війни, для її систематичного аналізу та оцінки ефективності у досягненні стратегічних цілей держави важливо чітко розмежувати інструменти, які вона включає:

- дезінформація та ІПСО;
- кібероперації (шпигунство, саботаж, вплив на інформаційні системи);
- політичне втручання, підкуп, використання місцевих проксі-груп;
- економічні важелі (енергетичний шантаж, торгові обмеження, санкційна дипломатія);
- використання нерегулярних збройних формувань;
- атаки на демократичні процеси (вибори, медіа, інститути);
- правові інструменти: зловживання міжнародними нормами, маніпуляція правовими рамками (Hybrid Threats And Hybrid Warfare, 2024). Ці інструменти демонструють складність і неоднорідність гібридної агресії, яка набуває як прихованих, так і відверто деструктивних форм.

Після неоднозначного втручання росії в Україну у 2014 році концепція гібридної війни стала предметом підвищеного інтересу з боку західних науковців, військових аналітиків, представників оборонно-політичного середовища та засобів масової інформації (Solmaz, 2025). Проте, попри зростання популярності цього поняття, його використання супроводжується значними концептуальним та аналітичними труднощами, як відзначалось нами вже вище.

Інтерес до гібридної війни підтверджується також зростаючим числом прикладних досліджень, у яких ті чи інші кейси були класифіковані як прояви саме цього типу конфлікту. Зокрема, прикладами гібридних війн вважаються операції росії в Криму та на Сході України (Rácz, 2017), залякувальна політика Китаю щодо Тайваню (Ignatius, 2018), дестабілізуюча активність Ірану на Близькому Сході (Iranian Hybrid Warfare, 2018), а також провокаційні дії Північної Кореї щодо Південної Кореї (Kang, 2020).

У цьому контексті зростає потреба у концептуальному уточненні підходів до класифікації гібридних конфліктів. Пропонується застосувати концепції Д. Кілкуллена, підхід, орієнтований на ворога (цю концепцію можна охарактеризувати формулою: «спочатку переможи ворога – все інше прийде згодом») та підхід, орієнтований на населення («спочатку потрібно взяти під контроль населення, а все інше буде наслідком цього») (Kilcullen, 2007). Однак перед цим давайте коротко пояснимо, що Д. Кілкаллен має на увазі під підходами, орієнтованими на населення та ворога, у контексті боротьби з повстанцями. Як зазначалося, застосування концепцій, орієнтованих на населення та ворога, до аналізу гібридної війни дозволяє краще зрозуміти її різні форми. У цьому контексті Т. Солмазом (2025) пропонується нове визначення гібридної війни, яка поділяє її на два основні підтипи – гібридну війну, орієнтовану на населення, та гібридну війну, орієнтовану на ворога. Такий поділ ґрунтується на характері проведених операцій (підривних чи руйнівних) та їхніх головних стратегічних цілей.

У гібридній війні, орієнтованій на населення, ключовим завданням є вплив на громадянське суспільство держави-противника та на осіб, які приймають політичні рішення, шляхом залякування, тиску та примусу з мінімальним використанням прямої конфронтації. Метою тут не є нанесення шкоди військовому потенціалу противника, а створення соціального та політичного тиску, що змушує його змінювати поведінку (Solmaz, 2025).

Натомість гібридна війна, орієнтована на ворога, передбачає активне використання насильства, застосування військової сили – як прихованої, так і непрямої – з метою фізичного послаблення чи знищення збройних сил противника. Поряд із цим, активно використовуються психологічні операції та підривна діяльність, спрямовані на вплив на населення та політичне керівництво ворожої держави (Solmaz, 2025).

Попри те, що обидва підтипи мають низку спільних характеристик – зокрема, прагнення контролювати населення та впливати на стратегічні рішення – між ними існує принципова відмінність. У гібридній війні, орієнтованій на ворога, перемога над збройними силами супротивника є основною метою, після досягнення якої реалізуються інші політичні чи соціальні завдання. У гібридній війні, орієнтованій на населення, навпаки, акцент робиться на маніпуляції громадською думкою та створенні внутрішнього тиску без масштабного військового втручання. Для ілюстрації цієї відмінності доцільно звернутися до двох показових прикладів: спроб Китаю дестабілізувати Тайвань і збройних операцій рф 2014–2021 рр.

Політична мета кампанії гібридної війни Китаю проти Тайваню полягає в тому, щоб утримати уряд Тайваню від проголошення «незалежності де-юре» та утримати правлячу партію від переобрання на Тайвані (Solmaz, 2024). У кампанії гібридної війни проти Тайваню Пекін у переважній більшості випадків використовував некінетичні інструменти, тоді як засоби прямої сили відігравали лише другорядну, допоміжну роль. Основний акцент був зроблений на інформаційно-психологічному впливі – зокрема, на пропагандистських кампаніях і поширенні дезінформації, спрямованих на формування недовіри до уряду Тайваню, підрив його легітимності та вплив на суспільні настрої. Паралельно застосовувався широкий спектр інших гібридних інструментів – дипломатичний тиск, економічні важелі впливу та кібероперації, які були націлені як на загальну громадськість острова, так і на політичне керівництво. Загальна мета цих дій полягала у розхитуванні внутрішньої єдності, створенні соціальних розколів і просуванні наративу про доцільність об'єднання з материковим Китаєм (Solmaz, 2024).

Кінетичні елементи гібридної кампанії Китаю проти Тайваню здебільшого мають демонстративний і залякувальний характер, спрямований не на ведення прямих бойових дій, а на тиск на керівництво острова та його населення. У цьому контексті Пекін активно застосовує інструменти військово-психологічного впливу, зокрема проведення масштабних навчань поблизу тайванських берегів, регулярні порушення зони ідентифікації протиповітряної оборони Тайваню, використання нерегулярних морських формувань, відомих як «малі блакитні чоловічки», а також погрози застосування сили. Ці дії спрямовані на посилення відчуття вразливості серед громадськості та тиску на політичне керівництво Тайваню. Такий акцент на впливі на осіб, які приймають ключові рішення, та на контроль над суспільними й політичними процесами відповідає логіці гібридної війни, орієнтованої на населення (Solmaz, 2024). У межах цього підходу Пекін надає перевагу не військовому знищенню супротивника, а завоюванню лояльності або підпорядкуванню населення як основному інструменту досягнення своїх стратегічних цілей.

У межах гібридної війни рф проти України активно використовувала широкий арсенал невійськових інструментів, таких як дезінформаційні кампанії, кібератаки та економічний тиск, прагнучи мінімізувати потребу в прямому застосуванні збройної сили. Проте попри важливість цих засобів, ключовим елементом стратегії росії під час операції на Сході була саме військова поразка супротивника. Значні бойові втрати з обох сторін свідчать про домінування силового компонента та пріоритетне спрямування зусиль на фізичне знищення ворожих збройних формувань (Solmaz, 2025). Таким чином, це є типовим прикладом гібридної війни, орієнтованої на ворога, де досягнення перемоги над військовим противником виступає головною ціллю, а всі інші політичні, соціальні та інформаційні завдання підпорядковуються цій стратегічній меті.

Вважаємо, що попри стратегічне місце, яке гібридна війна посідає в сучасному безпековому дискурсі, її практична ефективність у досягненні довгострокових цілей залишається суперечливою. Застосування інформаційних кампаній, кібератак, економічного тиску, хоча й створює тимчасові переваги, далеко не завжди гарантує бажаний політичний або військовий результат. Показовим є приклад анексії Криму у 2014 році, що нерідко трактується як успішна гібридна війна. Однак навіть у цьому випадку визначальними чинниками стали внутрішні соціальні та політичні передумови, а не виняткова ефективність гібридних інструментів як таких. Подальші події, зокрема повномасштабне вторгнення росії в Україну в 2022 році, продемонстрували межі впливу таких засобів: попри масштабну дезінформацію та кібератаки, агресору не вдалося дестабілізувати українське суспільство чи паралізувати його спротив. Навпаки, суспільство виявило високий рівень консолідації, адаптивності та рішучості, що зруйнувало розрахунок на швидку перемогу через гібридні методи. Такий досвід підриває уявлення про гібридну війну як універсальний інструмент досягнення стратегічного домінування.

Отже, гібридна війна формується як системний інструмент досягнення стратегічних цілей держави в умовах багатовимірного безпекового середовища. Вона поєднує різнорідні засоби впливу – від військових до інформаційно-психологічних – у межах єдиної стратегії, спрямованої на підрив цілісності та стабільності держав-мішеней. Досвід останніх років засвідчує не лише ефективність окремих гібридних тактик, але й виявляє межі їхнього впливу в умовах мобілізації суспільного спротиву та міжнародної консолідації. Подальші дослідження доцільно спрямувати на концептуалізацію механізмів гібридної агресії, уточнення ознак гібридного конфлікту як типу міждержавної взаємодії, а також на формування адаптивних моделей безпекової відповіді демократичних держав. Особливу увагу варто приділити порівняльному аналізу стратегій ревізіоністських держав і розвитку нормативно-правової бази протидії гібридним загрозам на міжнародному рівні.

Література

Буряченко, О. (2024). Гібридна війна як нова форма глобального протистояння. Наукові праці Міжрегіональної академії управління персоналом. *Політичні науки та публічне управління, 2(74),* 24-31. URL: https://doi.org/10.32689/2523-4625-2024-2(74)-3

Hybrid Threats And Hybrid Warfare Reference Curriculum (2024). *NATO*. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

Ignatius, D. (2018). China's hybrid warfare against Taiwan. *The Washington Post.* URL: https://www.washingtonpost.com/opinions/2018/12/14/chinas-hybrid-warfare-against-taiwan/

Iranian Hybrid Warfare (2018). *Wavell Room*. URL: https://wavellroom.com/2019/07/13/iranian-hybrid-warfare-military-response-deterence-options/?utm_source=RC+Defense+Morning+Recon&utm_campaign=b07b3b5e43-EMAIL_CAMPAIGN_2019_07_15_08_00&utm_medium=email&utm_term=0_694f73a8dc-b07b3b5e43-81835773

Kang, D. (2020). The Multi-Domain Operation's Viability as a Future War Concept of the Republic of Korea Military: Can It Counter North Korean Hybrid Warfare? URL: https://apps.dtic.mil/sti/pdfs/AD1124669.pdf

Kilcullen, D. (2007). Two Schools of Classical Counterinsurgency. *Small Wars Journal.* URL: https://smallwarsjournal.com/2007/01/28/two-schools-of-classical-counterinsurgency/

Maschmeyer, L. (2023). Assessing Hybrid War: Separating Fact from Fiction. *CSS Analyses in Security Policy, 332*. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf

Mitręga, A. (2020). The strategy of waging hybrid warfare in the 21 century. *Rocznik Bezpieczeństwa Morskiego Rok Xiv – 2020*, 187-203. URL: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-89ef5623-750e-4326-aecd-56195a5ce590 .

Natura nestatală a războiului hybrid (2020). URL: https://srcaltufevo.ru/ro/gibridnye-voiny-v-klassifikaciivoz-gibridnaya-voina-kak-novyi-tip-voiny.html

Rácz A. (2017). Russia's Hybrid War n Ukraine. Breaking the Enemy's Ability to Resist. *The Finnish Institute of International Affairs.* URL: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

Solmaz, T. (2024). China's Hybrid Warfare Against Taiwan: Motives, Methods, and Future Trajectory. *The Institute for Regional Security*. URL: https://regionalsecurity.org.au/article/chinas-hybrid-warfare-against-taiwan-motives-methods-and-future-trajectory/

Solmaz, T. (2025). The Need for a Taxonomy of Hybrid Warfare: Population-Centric vs. Enemy-Centric Approaches. *Irregular Warfare Center.* URL: https://irregularwarfarecenter.org/publications/perspectives/the-need-for-a-taxonomy-of-hybrid-warfare-population-centric-vs-enemy-centric-approaches/

Wales Summit Declaration (2014). *NATO.* URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

References

Buriachenko,O. (2024). Hibrydna viina yak nova forma hlobalnoho protystoiannia [Hybrid warfare as a new form of global confrontation]. *Naukovi pratsi Mizhrehionalnoi akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia* [Research papers of the Interregional Academy of Personnel Management. Political Science and Public Administration], *2(74),* 24-31. URL: https://doi.org/10.32689/2523-4625-2024-2(74)-3 [in Ukrainian].

Hybrid Threats And Hybrid Warfare Reference Curriculum (2024). *NATO.* URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf [in English].

Ignatius, D. (2018). China's hybrid warfare against Taiwan. *The Washington Post.* URL: https://www.washingtonpost.com/opinions/2018/12/14/chinas-hybrid-warfare-against-taiwan/ [in English].

Iranian Hybrid Warfare (2018). *Wavell Room*. URL: https://wavellroom.com/2019/07/13/iranian-hybrid-warfare-military-response-deterence-options/?utm_source=RC+Defense+Morning+Recon&utm_campaign=b07b3b5e43-EMAIL_CAMPAIGN_2019_07_15_08_00&utm_medium=email&utm_term=0_694f73a8dc-b07b3b5e43-81835773 [in English].

Kang, D. (2020). The Multi-Domain Operation's Viability as a Future War Concept of the Republic of Korea Military: Can It Counter North Korean Hybrid Warfare? URL: https://apps.dtic.mil/sti/pdfs/AD1124669.pdf [in English].

Kilcullen, D. (2007). Two Schools of Classical Counterinsurgency. *Small Wars Journal*. URL: https://smallwarsjournal.com/2007/01/28/two-schools-of-classical-counterinsurgency/ [in English].

Maschmeyer, L. (2023). Assessing Hybrid War: Separating Fact from Fiction. *CSS Analyses in Security Policy, 332*. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf [in English].

Mitręga, A. (2020). The strategy of waging hybrid warfare in the 21 century. *Rocznik Bezpieczeństwa Morskiego Rok Xiv – 2020*, 187-203. URL: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-89ef5623-750e-4326-aecd-56195a5ce590 [in English].

Natura nestatală a războiului hybrid [The non-state nature of hybrid warfare] (2020). URL: https://srcaltufevo.ru/ro/gibridnye-voiny-v-klassifikaciivoz-gibridnaya-voina-kak-novyi-tip-voiny.html [in Romanian].

Rácz A. (2017). Russia's Hybrid War n Ukraine. Breaking the Enemy's Ability to Resist. *The Finnish Institute of International Affairs*. URL: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf [in English].

Solmaz, T. (2024). China's Hybrid Warfare Against Taiwan: Motives, Methods, and Future Trajectory. *The Institute for Regional Security*. URL: https://regionalsecurity.org.au/article/chinas-hybrid-warfare-against-taiwan-motives-methods-and-future-trajectory/ [in English].

Solmaz, T. (2025). The Need for a Taxonomy of Hybrid Warfare: Population-Centric vs. Enemy-Centric Approaches. *Irregular Warfare Center.* URL: https://irregularwarfarecenter.org/publications/perspectives/the-need-for-a-taxonomy-of-hybrid-warfare-population-centric-vs-enemy-centric-approaches/ [in English].

Wales Summit Declaration (2014). *NATO.* URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm [in English].

Анотація

Капсамун О. Г. **Гібридна війна як інструмент досягнення стратегічних цілей держав. –** Стаття.

У статті досліджується гібридна війна як інструмент реалізації стратегічних цілей держав у сучасному глобальному безпековому середовищі. Обґрунтовується, що гібридна війна є системною формою міждержавного протистояння, яка поєднує військові, інформаційні, економічні, політичні, дипломатичні та кібернетичні засоби впливу в межах єдиної стратегічної логіки. Автор аналізує концептуальні підходи до класифікації гібридних конфліктів, зокрема запропоновану Т. Солмазом типологію, яка розрізняє війни, орієнтовані на ворога, і війни, орієнтовані на населення. Наведено приклади застосування гібридних інструментів у зовнішній політиці Китаю щодо Тайваню та військової агресії рф проти України. Увага зосереджена на ключових характеристиках гібридної війни, до яких належать дезінформація, ІПСО, кібератаки, економічний тиск, маніпуляції нормами міжнародного права і т.п. Розкрито основні етапи реалізації гібридної стратегії. Стаття також порушує питання ефективності гібридної війни як інструменту досягнення політичного домінування, демонструючи, що успіх таких стратегій залежить не лише від застосованих інструментів, а й від внутрішньої стійкості та згуртованості суспільства-об'єкта впливу. Відзначено, що гібридна війна поєднує різноманітні засоби впливу – від військових до інформаційно-психологічних – у межах єдиної стратегії, спрямованої на підрив цілісності та стабільності держав-мішеней. Досвід останніх років засвідчує не лише ефективність окремих гібридних тактик, але й виявляє межі їхнього впливу в умовах мобілізації суспільного спротиву та міжнародної консолідації. Відзначено, що подальші дослідження доцільно спрямувати на концептуалізацію механізмів гібридної війни, уточнення її ознак, а також на формування адаптивних моделей безпекової відповіді демократичних держав. Особливу увагу варто приділити порівняльному аналізу стратегій ревізіоністських держав і розвитку нормативно-правової бази протидії гібридним загрозам на міжнародному рівні.

Ключові слова: гібридна війна, гібридні загрози, безпека, стратегічні цілі, гібридна стратегія.

Summary

Kapsamun O. H. **Hybrid warfare as a tool for achieving the strategic goals of states. –** Article.

The article examines hybrid warfare as a tool for implementing the strategic goals of states in the modern global security environment. It is argued that hybrid warfare is a systemic form of interstate confrontation that combines military, information, economic, political, diplomatic and cyber means of influence within a single strategic logic. The author analyzes conceptual approaches to the classification of hybrid conflicts, in particular the typology proposed by T. Solmaz, which distinguishes wars focused on the enemy and wars focused on the population. Examples of the use of hybrid instruments in China's foreign policy towards Taiwan and the Russian Federation's military aggression against Ukraine are given. Attention is focused on the key characteristics of hybrid warfare, which include disinformation, IPSO, cyberattacks, economic pressure, manipulation of international law, etc. The main stages of implementing the hybrid strategy are revealed. The article also raises the issue of the effectiveness of hybrid warfare as a tool for achieving political dominance, demonstrating that the success of such strategies depends not only on the tools used, but also on the internal stability and cohesion of the society being influenced. It is noted that hybrid warfare combines various means of influence – from military to informational and psychological – within a single strategy aimed at undermining the integrity and stability of target states. The experience of recent years demonstrates not only the effectiveness of individual hybrid tactics, but also reveals the limits of their influence in the context of the mobilization of public resistance and international consolidation. It is noted that further research should be directed at conceptualizing the mechanisms of hybrid warfare, clarifying its features, and forming adaptive models of the security response of democratic states. Particular attention should be paid to a comparative analysis of the strategies of revisionist states and the development of a regulatory framework for countering hybrid threats at the international level.

Key words: hybrid warfare, hybrid threats, security, strategic goals, hybrid strategy.