DOI: 10.33498/louu-2022-01-131

Олексій Кресін

доктор юридичних наук, доцент,
член-кореспондент Міжнародної академії порівняльного права,
керівник Центру порівняльного правознавства Інституту держави і права імені В. М. Корецького НАН України (Київ, Україна)
ORCID ID: https://orcid.org/0000-0002-4016-6596
okresin@gmail.com

УДК 341.3

ВІДПОВІДІ НА ГІБРИДНІ ЗАГРОЗИ: МІЖНАРОДНИЙ ДОСВІД І ЗАКОНОДАВСТВО УКРАЇНИ[1]

Анотація. Протистояння держав і різноманітних недержавних акторів протягом історії людства ніколи не зводилося до суто військових засобів і не обмежувалося періодами офіційно проголошених воєн. Історія гібридних методів ведення воєн є не лише напрямом, а й цілою перспективною сферою наукових досліджень. Але в контексті безпосередніх практичних потреб доцільно аналізувати сучасні форми їх використання й осмислення. Важливою передумовою появи гібридних воєн стала заборона війни у міжнародному праві, що, безумовно, відобразило суттєві зміни у світогляді значної частини людства. Сучасна й всезагальна форма заборони війни у міжнародному праві представлена у Статуті Організації Об'єднаних Націй (ООН). Ці принципи послідовно розкривалися й удосконалювалися в наступних актах ООН.

Гібридну війну можна визначити як новий тип протистояння держав між собою та з недержавними акторами, діалектично пов'язаний із забороною в міжнародному праві звичайної війни як засобу національної політики. У вузькому розумінні, характерному для військових аналітиків, гібридна війна становить поєднання регулярних та іррегулярних методів ведення війни. У широкому і більш відповідному реаліям баченні гібридна війна є видом протистояння, заснованим на неофіційних, неавторизованих чи замаскованих невоєнних і воєнних ворожих діях, спрямованих на ураження всіх сфер життєдіяльності суспільства, включно з функціонуванням держави й економіки, соціальними комунікаціями, модусами поведінки людей. Можна визначити такі характеристики гібридної війни: транскордонність, тотальність і безперервність;

[1] Окремі аспекти цього дослідження висвітлювалися в інших публікаціях автора: О Кресін, 'Визнання, регулювання та забезпечення протидії гібридним загрозам у НАТО та ЄС' (2022) 33 Правова держава (у друці); О Кресін, 'Основні види гібридних загроз та правові основи забезпечення конструктивної взаємодії інститутів держави і суспільства' в *Державно-правові основи реалізації стратегії національної стійкості в умовах існування гібридних загроз для Української держави і суспільства: аналітична записка* (Пирожков С, Шемшученко Ю, Скрипнюк О та інші, Інститут держави і права імені В М Корецького НАН України 2021) (у друці); О Кресін, 'Проблеми протидії гібридним загрозам в українському законодавстві' (2022) 2 Зовнішня торгівля: економіка, фінанси, право (у друці).

неофіційний характер, за якого держави уникають формального проголошення війни; спрямованість на створення контрольованого реального чи суб'єктивно відчутного хаосу; домінування невоєнних засобів; різноманітність і ситуативність методів, що не піддаються точній класифікації, а відповідають вразливостям кожної сфери життєдіяльності та цінностей людини й суспільства; відсутність чіткої межі між зовнішньою і внутрішньою політикою в здійсненні й протидії гібридній війні; широке використання методів психологічного впливу на населення.

Ключові слова: заборона війни; гібридна війна; гібридні методи ведення воєн; протидія гібридній війні.

Сучасне осмислення гібридних загроз і методів ведення воєн

Протистояння держав і різноманітних недержавних акторів протягом історії людства ніколи не зводилося до суто військових засобів і не обмежувалося періодами офіційно проголошених воєн. Історія гібридних методів ведення воєн є не лише напрямом, а й цілою перспективною сферою наукових досліджень. Але в контексті безпосередніх практичних потреб доцільно аналізувати сучасні форми їх використання й осмислення.

Зазвичай дослідники ігнорують політичні й правові обставини, що сприяли появі сучасних гібридних воєн як феномену, а не лише як окремих "неконвенційних" (у розумінні міжнародного гуманітарного права й особливо IV Гаазької конвенції про закони і звичаї війни на суходолі[2]) методів протистояння держав, а натомість зосереджуються лише на нових технологіях останнього. На нашу думку, важливою передумовою появи гібридних воєн стала заборона війни у міжнародному праві, що, безумовно, відобразило суттєві зміни у світогляді значної частини людства.

Зокрема, у 1928 р. було укладено Загальний договір про заборону війни як інструменту національної політики (Пакт Бріана-Келлога, або Паризький пакт), учасницями якого стали понад 60 держав, включно з СРСР, і який вважається чинним і досі, зокрема для України. У документі було викладено переконання в тому, що

> прийшов момент розпочати відверту відмову від війни як знаряддя національної політики, аби мирні та дружні відносини, що існують нині між народами, могли стати постійними', а також що 'будь-які зміни у взаємних відносинах мають відшуковуватися лише у мирних засобах і здійснюватися законно і мирно[3].

[2] IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі від 18 жовтня 1907 р. <https://zakon.rada.gov.ua/laws/show/995_222#Text> (дата звернення: 10.01.2022).

[3] Договір про заборону війни як засобу національної політики (Пакт Бріана-Келлога) від 27 серпня 1928 р. <https://zakon.rada.gov.ua/laws/show/995_647#Text> (дата звернення: 10.01.2022).

Сучасна і всезагальна форма заборони війни у міжнародному праві представлена у Статуті Організації Об'єднаних Націй (далі – ООН), який починається з декларації рішучості об'єднаних націй 'позбавити прийдешні покоління жахіть війни', 'жити разом, у мирі один з одним, як добрі сусіди, і об'єднати наші сили для підтримки міжнародного миру та безпеки, і забезпечити прийняттям принципів і встановленням методів, щоби збройні сили використовувалися не інакше, як у спільних інтересах'. У цьому документі передбачається заборона агресивної війни та колективні заходи для 'запобігання та усунення загрози миру й придушення актів агресії, або інших порушень миру' (ст. 1)[4]. Ці принципи послідовно розкривалися й удосконалювалися в наступних актах ООН.

Безумовно, суперечки між державами, територіальні й інші претензії, економічна та інша конкуренція, а також екзистенційні суперечності на рівні ідентичності нікуди не зникли разом із забороною традиційного способу їх вирішення. Але цілковита делегітимація війни поставила перед потенційними агресорами загрози не лише репутаційних втрат, а й економічної та політичної ізоляції, можливого міжнародного санкціонування збройного вторгнення третіх держав та їх коаліцій. У цих умовах мали виникнути нові чи удосконалитися старі форми протистояння без формального проголошення чи визнання війни.

Як зазначають учені, сучасний поворот до більш відкритої конфронтації та посилення односторонності дій держав відбувся в умовах значних технологічних нововведень.

> Технологічний прогрес <…> відкрив нові шляхи для іноземного втручання та підривної роботи у формі фальшивих новин, впливу на вибори та кібершпіонажу. У результаті сучасні суспільства стали більш вразливими до актів тероризму і до ворожого впливу й втручання[5].

Вважається, що концептуалізація гібридних методів протистояння розпочалася з узагальнення у США досвіду ведення складених (багатокомпонентних) воєн як поєднання дій регулярних та іррегулярних військ. На основі цього щонайпізніше у 1998 р. у США було запропоновано термін "гібридні методи ведення війни"[6].

Починаючи з 2006 р., поняття "гібридної загрози" з'являється у військових документах США. Американський військовий учений Ф. Гоффман у 2007 р. писав:

[4] Статут Організації Об'єднаних Націй і Статут Міжнародного Суду від 26 червня 1945 р. <http://www.un.org.ua/images/UN_Charter_Ukrainian.pdf> (дата звернення: 10.01.2022).

[5] A Sari (ed), *Hybrid threats and the law: Concepts, trends and implications* (The European Centre of Excellence for Countering Hybrid Threats 2020) 8.

[6] В Горбулін (ред), *Світова гібридна війна: український фронт* (НІСД 2017) 21–2.

> Гібридні війни можуть вести й держави, і недержавні актори. Гібридні війни включають низку різноманітних способів ведення війни, зокрема звичайні засоби, нерегулярні тактики і формації, терористичні акти, в тому числі невибіркове насильство й примус, а також кримінальний безлад. Ці мультимодальні дії можуть здійснювати окремі формування – або одне й те ж формування, але загалом їх операційно й тактично скеровують і координують у рамках основного бойового простору для досягнення синергетичних ефектів[7].

Одне з перших монографічних узагальнень гібридних загроз, здійснене у 2011 р. майором Б. Флемінгом, викладачем Школи поглибленого військового навчання Армії США, визначило гібридну війну як не обмежене загальноприйнятими правовими нормами і правилами ведення воєн операційне (між стратегією і тактикою) мистецтво, а її використання – як 'потенційну зміну парадигми, доктринальну та організаційну революцію у військовій справі'. Як наголошував автор, гібридні загрози – це невичерпна методологія і суміш дій, що 'обходить когнітивні межі традиційної характеристики загроз і застосування організованого колективного насилля' та не піддається класифікації. Асиметричний і непередбачуваний характер гібридних засобів дає змогу слабшому актору, не обмеженому цивілізованими звичаями, а також "когнітивними і географічними межами", одержувати перевагу над сильнішим опонентом. При цьому саме цивілізованість однієї із сторін протистояння виявляється її операційною вразливістю. Б. Флемінг прогнозував різке збільшення використання гібридних методів протистояння протягом найближчого десятиліття, що принципово змінять операційне середовище. Тому він закликав змінювати "лінійне мислення" американських військових, 'засноване на фундаменталізмі брудних чобіт та антиінтелектуальному редукціонізмі'[8].

Як зазначав Б. Флемінг, 'гібридні загрози осмислюють реалії середовища та притаманні йому складність і взаємозв'язки'. У той час як традиційні актори транслює стратегічний намір у тактичні дії, гібридні актори 'прагнуть сформувати умови для стратегічної можливості' та не допустити домінування традиційних акторів. Тому 'як вода існує у рідкій, газоподібній та твердій формах, так і гібридна загроза не має постійної форми, але трансформується та адаптується до умов, у яких перебуває, щоби діяти, виживати та досягати сприятливої переваги'; вона 'нехтує часом і простором для досягнення результату через виснаження', використовуючи відчуті слабкості й вразливості опонента. Б. Флемінг чітко

[7] В Тарасюк, *Застосування інформаційних технологій в умовах гібридної війни* (GlobeEdit 2020) 56.
[8] В Fleming, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. Fort Leavenworth* (United States Army Command and General Staff College 2011) II, 32–3, 39.

відокремлював гібридні засоби ведення війни від партизанських або іррегулярних, адже децентралізованість дій тут поєднується зі стратегічністю замислу, який визначає комплексне й синергійне поєднання різних засобів його реалізації[9].

Осмислення нового характеру воєн відбулося і в Росії. У Воєнній доктрині Російської Федерації (далі – РФ) 2010 р. особливістю сучасних воєнних конфліктів названо 'комплексне застосування військової сили, політичних, економічних, інформаційних та інших заходів невоєнного характеру, які реалізуються з широким використанням протестного потенціалу населення і сил спеціальних операцій'[10].

На початку 2013 р. ці положення було розвинуто начальником Генерального штабу РФ В. Герасимовим, що дало підстави аналітикам назвати нову формулу "нелінійної війни" доктриною Герасимова:

> Акцент методів протиборства, що використовуються, зміщується у бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невоєнних заходів, які реалізуються із залученням протестного потенціалу населення. Все це доповнюється воєнними заходами прихованого характеру, в тому числі через реалізацію інструментів інформаційного протиборства і через дію сил спеціальних операцій. До відкритого застосування сили, зазвичай під виглядом миротворчої діяльності і кризового врегулювання, перехід робиться тільки на певному етапі, в основному для досягнення остаточного успіху в конфлікті[11].

Відомий російський політтехнолог, експомічник Президента РФ В. Сурков запропонував такі елементи гібридної війни:

> 1) хибно-цільове програмування партнера-противника через "кооперацийну модель", під прикриттям якої реалізується програма його крипто-деструкції; 2) трансформація визначеностей і станів у сукупність невизначеностей, хаотизація причинно-наслідкових ланцюжків; 3) управління хаосом через швидкі рішення, ініціативні дії та превентивні заходи щодо інших акторів; 4) впорядкування хаосу, реінжиніринг простору, отримання нової реальності через синергетику[12].

В Україні природа й особливості гібридної війни стали предметом наукових досліджень переважно після анексії Криму й окупації частин До-

[9] Fleming 35–7.
[10] Военная доктрина Российской Федерации <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>. Цит. за: Горбулін (н 6) 37.
[11] В Герасимов, 'Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий' (*Военно-промышленный курьер*, 27.02.2013) <http://www.vpk-news.ru/articles/14632> (дата звернення: 10.01.2022).
[12] *Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ* (Мартинюк В ред, 2018) 8–9.

нецької й Луганської областей Росією. Зокрема, автори найбільш відомої й докладної монографії за редакцією академіка В. Горбуліна "Світова гібридна війна: український фронт" розглядають гібридну війну як світове протистояння, що прийшло на зміну холодній війні, й відбувається між сферами стабільності й сферами невизначеності, полягає у постійній напрузі, що може набувати форм збройного конфлікту чи протистояння в інших формах[13].

Цей вид війни автори визначають як

> воєнні дії, що здійснюють шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний із воєнних і невоєнних способів ведення гібридного конфлікту застосовується у воєнних цілях та використовується як зброя. Перетворення на зброю (weaponization) відбувається не тільки в медійній сфері. Так само в прямому сенсі у ролі зброї, яка завдає ураження різного рівня системам противника, застосовуються всі інші невоєнні засоби ведення гібридної війни[14].

Як зазначає В. Горбулін, підсумком гібридної війни останніх років стало руйнування світового порядку, й зокрема міжнародного права, але й надалі ставкою у війні залишається демократична модель державності. Зовнішня загроза полягає у прагненні Росії 'розколоти українське суспільство, деморалізувати його, зруйнувати трансформацію і повернути Україну до зрозумілого агресору стану: корумпованого, авторитарного, глибоко вторинного щодо агресора'. Внутрішня загроза полягає, зокрема, у політичному популізмі, 'порожнечі обіцянок, агресії і жадобі влади' внутрішніх гравців. Один зі шляхів протидії цим загрозам вдосконалення організації суспільства – це 'процеси політичної консолідації, забезпечення успішності реформ і побудова держави, здатної захистити демократію від масштабної гібридної загрози з боку агресора'[15].

Як зазначається у недавньому колективному монографічному дослідженні "Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства", особливістю гібридної війни є те, що вона

> ведеться замасковано з використанням переважно нелінійних тактик і націлена не на захоплення усієї території країни, хоча не виключається взяття під контроль окремих територій, а на отримання патронату над

[13] Горбулін (н 6) 16.
[14] Там само 19.
[15] В Горбулін, 'Який Фенікс народиться зі згарища світової гібридної війни?' *(Дзеркало тижня)* <https://zn.ua/ukr/article/print/internal/yakiy-feniks-naroditsya-zi-zgarischa-svitovoyi-gibridnoyi-viyni-259112_.html> (дата звернення: 10.01.2022).

державою, який досягається через вплив на населення, політикум, бізнес, силові структури[16].

Саме тому ключовим елементом протидії гібридним загрозам, на думку науковців, є підвищення стійкості суспільства.

На нашу думку, гібридна війна як інтелектуальна технологія є надзвичайно привабливою через свою результативність за умов порівняно незначних витрат і репутаційних втрат, а тому можна припустити, що її використання вже нікуди не зникне, стане постійним чинником у міжнародних відносинах. Тому її слід сприймати не як тимчасовий стан, а як перманентний процес. Стратегія відповіді на неї, отже, повинна мати характер не завершеного плану, а постійного підходу, своєрідної незавершеної відкритої філософії політики, у якій константами можуть бути лише цінності та принципи.

У зв'язку з цим слід звернути увагу на плідність запропонованої низкою авторів концепції національної стійкості як стратегії збереження і розвитку суспільства та держави, забезпечення їх безпеки, національних інтересів, політичної й культурної суб'єктності[17]. У межах цього підходу, зокрема, можна розрізнити виклики та загрози. Виклики постають перед кожною сферою життєдіяльності суспільства. Зокрема, це невирішеність соціальних проблем, конфлікти інтересів груп населення, недоліки гуманітарного розвитку, недостатність ресурсів тощо. Виклики роблять розвиток суспільства вразливим у відповідній сфері. Безумовно, впоратися з усіма викликами і водночас неможливо. Але залежно від конструктивності, інклюзивності, оперативності, інтелектуального забезпечення, стратегічності державної політики та суспільних комунікацій кожен виклик може перетворитися або на шанс удосконалення суспільства, поліпшення життя людини, посилення стійкості держави або на ризик для людини, суспільства, держави, який в умовах гібридного протистояння перетворюється також на загрозу і поле для зовнішнього втручання. Безумовно, це стосується також економічного, технологічного, екологічного розвитку в їх взаємозв'язку із суспільним розвитком. У такому баченні і вразливість, і стійкість є відносними і мінливими, процесуальними показниками, постійними тут має бути лише забезпечення стратегії прогнозування, пошуку і вибору найбільш адекватних відповідей.

Протидія гібридним загрозам у НАТО та Європейському Союзі

Протягом багатьох десятиліть холодної війни ключовою для спільної політики держав – учасниць НАТО щодо протидії зовнішнім загрозам

[16] *Гібридні загрози Україні і суспільна безпека* (н 12) 8.

[17] С Пирожков, Є Божок, Н Хамітов, 'Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз' (2021) 8 Вісник НАН України.

була ст. 3 Північноатлантичного (Вашингтонського) договору 1949 р., згідно з якою 'сторони, окремо і разом, шляхом постійної й ефективної самодопомоги і взаємної допомоги, будуть підтримувати і розвивати свою індивідуальну та колективну спроможність протистояти збройному нападу'. Але передбачене у статтях 5 і 6 щодо взаємної і колективної допомоги бачення безпеки і нападу формально обмежувалося збройним нападом на територію, збройні сили, флот та літаки[18].

Звичайно, стратегічні документи НАТО і національне законодавство держав-учасниць у контексті протидії зовнішнім загрозам передбачали також заходи щодо "цивільної готовності", що нині визначається як "планування щодо цивільних надзвичайних ситуацій" і загалом відповідало радянському розумінню цивільної оборони. Цю сферу було добре організовано і забезпечено ресурсами, але у 1990-х роках відповідне фінансування було суттєво зменшено[19]. З часів закінчення холодної війни військові бюджети було значно скорочено, а більшість ресурсів, об'єктів оборони й критичної інфраструктури приватизовано, механізми і спроможності територіальної оборони зникли. Водночас суспільства стали більш вразливими через взаємозалежність у всіх сферах і технологічність, інформатизацію[20].

Поняття гібридної загрози як поєднання державами та недержавними акторами конвенційних і неконвенційних засобів ворожих дій було включене до Стратегічного концепту НАТО і "Доктрини Кепстоун"[21] НАТО у 2010 р.

Але можна стверджувати, що саме нові виклики, насамперед із боку РФ та дії ІДІЛ, звернули увагу НАТО на гібридні загрози. Зокрема, у 2014 р. Генеральний секретар НАТО А. Расмуссен звинуватив Росію у веденні гібридної війни й визначив останню як 'комбінацію військових дій, прихованих операцій і агресивної програми дезінформації'[22].

У 2015 р. на саміті міністрів закордонних справ держав – учасниць НАТО було ухвалено стратегію щодо ролі цієї організації у протидії гібридній війні, в якій підкреслюється основна відповідальність держав-учасниць за протидію гібридним загрозам. НАТО збиратиме і поширюватиме інформацію щодо гібридної активності, для чого у межах Об'єднаного департаменту розвідки і безпеки у структурі Штаб-квартири НАТО засновується відділ гібридного аналізу. НАТО допомагатиме державам-

[18] The North Atlantic Treaty. Washington D.C. 4 April 1949 <https://www.nato.int/cps/en/natohq/official_texts_17120.htm> (accessed: 10.01.2022).
[19] W-D Roepke, H Thankey, 'Resilience: the first line of defence' (*NATO Review,* 27.02.2019) <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html> (accessed: 10.01.2022).
[20] Resilience and Article 3 (11 Jun. 2021) <https://www.nato.int/cps/en/natohq/topics_132722.htm> (accessed: 10.01.2022).
[21] BI-SC Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats (25 August 2010) <https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf> (accessed: 10.01.2022).
[22] Тарасюк (н 7) 58.

учасницям виявляти їхню вразливості та посилювати їхню власну стійкість, надаватиме експертну і методичну допомогу в сферах цивільної оборони, запобігання і ліквідації наслідків хімічних, біологічних, радіологічних та ядерних катастроф, захисту критичної інфраструктури, стратегічних комунікацій, захисту цивільного населення, кібербезпеки, енергетичної безпеки, антитерористичної діяльності.

Також стратегія спрямована на стримування гібридних загроз: підвищення підготовленості й готовності своїх військ, удосконалення процесів ухвалення рішень, посилення структури командування. У випадку неуспіху стримування НАТО підтвердила готовність оперативно й ефективно захистити держав-учасниць від будь-якої загрози[23]. Зокрема, очевидно вперше у цьому документі гібридні напади було кваліфіковано як вид агресії, що є підставою для колективної оборони (застосування ст. 5 Вашингтонського договору)[24].

Ще важливішими є документи, ухвалені за підсумками Варшавського саміту Північноатлантичної ради 2016 р., тобто зустрічі всіх глав держав і голів урядів держав-учасниць. Зокрема, у комюніке саміту гібридну війну було визначено як широку, складну та гнучку комбінацію конвенційних і неконвенційних засобів, відкритих і прихованих військових, парамілітарних і цивільних заходів протистояння, що використовуються державами та недержавними акторами у високоінтегрований спосіб для досягнення їхніх цілей. Було підтверджено поширення на можливі випадки гібридної війни зобов'язання щодо колективної оборони[25].

Як зазначалося у резолюції "Базові вимоги НАТО щодо національної стійкості", схваленій під час Варшавського саміту, 'стійкість є необхідною основою для надійного стримування і оборони та ефективного виконання ключових завдань Альянсу'. Бути стійкими щодо змін викликів безпеки 'вимагає від союзників підтримувати і захищати критичні цивільні спроможності, поряд і на підтримку військовим спроможностям, та наскрізно працювати всім органам влади й з приватним сектором'[26].

Ця резолюція містить сім основних взаємно пов'язаних *вимог щодо національної стійкості,* зокрема у контексті гібридних загроз, які надають нове тлумачення і розкривають зміст ст. 3 Вашингтонського договору: 1) забезпечення безперервності в управлінні та критичних управлінських послугах (зокрема, здатність приймати рішення, доводити їх до адре-

[23] NATO's response to hybrid threats (16 Mar. 2021) <https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en> (accessed: 10.01.2022).
[24] Горбулін (н 6) 36.
[25] Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016 <https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid> (accessed: 10.01.2022).
[26] Commitment to enhance resilience, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016 <https://www.nato.int/cps/en/natohq/official_texts_133180.htm> (accessed: 10.01.2022).

сатів, реалізувати їх в умовах кризи); 2) стійкість постачання енергії (резервні плани, внутрішні та міжнародні енергетичні мережі); 3) здатність ефективно вирішувати проблеми з неконтрольованим рухом людей і не допускати конфліктів цих рухів із силами НАТО у випадку розгортання останніх; 4) стійкість харчових і водних ресурсів (гарантування безпеки їх постачання від зривів та саботажу); 5) здатність упоратися з масовими жертвами (забезпечення спроможності систем охорони здоров'я, достатньої наявності й захищеності медичного постачання); 6) стійкість систем цивільних комунікацій (забезпечення функціонування телекомунікацій та цифрових мереж навіть в умовах кризи, з достатньою резервною здатністю); 7) стійкість транспортних систем (забезпечення швидкого пересування сил НАТО територіями держав-членів, надійності забезпечення транспортними мережами здійснення цивільних послуг навіть в умовах криз)[27]. Важливо, що Варшавська резолюція 2016 р. не стала декларативним чи рекомендаційним документом, на її виконання регулярно здійснюються узагальнюючі дослідження, що виявляють проблемні сфери, де потрібна увага національної влади чи допомога Альянсу[28].

У Декларації Брюссельського саміту Північноатлантичної ради 2018 р. було зазначено, що метою гібридної діяльності держав і недержавних акторів є створення непевності та затирання межі між миром, кризою та конфліктом. У документі було підкреслено готовність НАТО за рішенням Північноатлантичної ради допомагати державам-учасницям у протидії "гібридним операціям", наголошено на розгляді можливої гібридної війни як збройного нападу, що є підставою для реалізації зобов'язання щодо колективного захисту. Резолюція дала старт створенню команд підтримки протидії гібридній війні для посилення стійкості держав-членів[29].

Вимоги Варшавської резолюції 2016 р. уточнювалися у рішеннях НАТО. Зокрема, у 2019 р. на саміті міністрів оборони НАТО щодо стійкості систем цивільних комунікацій додано такі вимоги: надійні комунікаційні системи, включно з інтернетом *5G*, надійні варіанти відновлення цих систем, пріоритетний доступ національних органів влади до них у періоди кризи, докладний аналіз ризиків щодо комунікаційних систем. Також у 2020 р. ці вимоги було уточнено з огляду на нові технології інтернет-зв'язку, вплив та наслідки пандемії *COVID-19*[30].

У комюніке Брюссельського саміту Північноатлантичної ради у червні 2021 р. було проголошено створення Всеохопної політики кібернетично-

[27] Resilience and Article 3 (n 20).
[28] Roepke, Thankey (n 19).
[29] Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018 <https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21> (accessed: 10.01.2022).
[30] Resilience and Article 3 (n 20).

го захисту з трьома пріоритетами: стримування, оборона та посилення стійкості. Було наголошено, що кібернетичні атаки як засіб гібридних операцій за рішенням Північноатлантичної ради можуть визнаватися випадком нападу на держав-учасниць, рівнозначним збройному нападу, що передбачає колективну оборону. Значну увагу приділено енергетичній безпеці, зокрема диверсифікації та інтеграції шляхів постачання енергоносіїв, захисту критичної інфраструктури[31].

У резолюції "Посилені зобов'язання щодо стійкості", ухваленій під час цього саміту як доповнення до Варшавської резолюції 2016 р., передбачається розробка державами – учасницями НАТО національних цілей і планів щодо підвищення стійкості. Серед загроз стійкості держав, що виходять від інших держав і недержавних акторів, названі:

> конвенційні, неконвенційні та гібридні загрози й дії; терористичні атаки; шкідлива кібердіяльність, що зростає й стає дедалі більш складною; дедалі більш поширена ворожа інформаційна діяльність, включно з дезінформацією, спрямована на дестабілізацію наших суспільств та підрив цінностей, які ми поділяємо; спроби втручання у наші демократичні процеси та належне врядування[32].

Серед *посилених зобов'язань щодо підвищення стійкості* названі: безпека і диверсифікація ланцюжків поставок, а також стійкість критичної інфраструктури (на землі, в морі, космосі та кіберпросторі) та ключової промисловості, включно з їх захистом від шкідливої економічної діяльності; використання розвитку технологій для захисту комунікацій нового покоління, захисту технологій та інтелектуальної власності; долання викликів енергетичній безпеці, що породжуються природними катастрофами, посиленими змінами клімату; збільшення вкладень у потужні, гнучкі та сумісні військові спроможності; посилення взаємодії держав-учасниць (консультації, рішення, дії); готовність до оперативної зміни політики НАТО; посилення взаємодії органів влади з приватним, громадським секторами, суспільством, посилення публічної комунікації; посилення взаємодії з міжнародними організаціями (насамперед з ЄС) та державами – партнерами поза НАТО. Основою стійкості називається відданість спільним цінностям[33].

У статті співробітників Департаменту оборонної політики і планування НАТО В.-Д. Рьопке і Г. Сенке стійкість цивільних структур, ресурсів та послуг називається першою лінією оборони сучасних суспільств. Стійкі

[31] Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021 <https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en> (accessed: 10.01.2022).
[32] Strengthened Resilience Commitment <https://www.nato.int/cps/en/natohq/official_texts_185340.htm> (accessed: 10.01.2022).
[33] Ibid.

суспільства, де всі органи влади, публічний і приватний сектори залучені до планування цивільної готовності, мають менше вразливостей і становлять чинник стримування потенційного ворога, який не може досягти бажаних цілей. Також такі суспільства мають кращі шанси на швидке відновлення до передкризового функціонального рівня. Підходом НАТО автори називають посилення стійкості на випадок будь-якої загрози – природного надзвичайного лиха, викликів гібридної війни, тероризму, збройного конфлікту чи їх поєднання[34].

Основним органом НАТО щодо цивільної підготовленості й стійкості нині є Комітет планування щодо цивільних надзвичайних ситуацій *(Civil Emergency Planning Committee)*. Він на постійній основі займається моніторингом і аналізом впливу криз, поширює інформацію і кращі практики серед держав-учасниць[35].

ЄС почав розглядати проблеми гібридних загроз комплексно лише у 2015 р. У доповіді Високого представника ЄС із зовнішніх справ та політики безпеки 2016 р. "Спільна позиція щодо протидії гібридним загрозам" було наголошено на тому, що визначення цих загроз має залишатися гнучким і не може бути точним і вичерпним. Але доповідь усе ж визначає їх як

> суміш силової та підривної діяльності, конвенційних та неконвенційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть бути скоординовано використані державою чи недержавними акторами для досягнення певних цілей, залишаючись при цьому нижче порога офіційно оголошеної війни <…> Гібридні загрози спрямовані на використання вразливостей країни і часто на підрив основоположних демократичних цінностей і свобод[36].

Стверджуючи національну специфіку гібридних загроз і відповідальність за протидію ним держав – членів ЄС, доповідь наголошує на потребі координації їхніх зусиль. Основними засобами протидії гібридним загрозам документ називає їх усвідомлення, посилення стійкості держав, попередження, відповідь на кризи та відновлення. Зокрема, стійкість у документі визначається як "спроможність витримувати стрес і відновлюватися, посилюючись викликами". Йдеться про ключову інфраструктуру, ланцюжки постачання та суспільство. Щодо суспільства йдеться насамперед про протидію радикалізації та насильницькому екстремізму. Це передбачає елементи контролю щодо поширення інформації і протидії пропаганді, роботу з радикалізованими та вразливими особами,

[34] Roepke, Thankey (n 19).
[35] Resilience and Article 3 (n 20).
[36] Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response. European Commission <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN> (accessed: 10.01.2022).

підготовку фахівців, обмін практиками та інформацією між державами, цілеспрямовану роботу правоохоронних органів, як і розуміння та усунення економічних, політичних та соцієтальних чинників, що сприяють розвитку екстремізму і радикалізму[37].

У доповіді Європейського Парламенту "Протидія гібридним загрозам: Співпраця ЄС-НАТО" (березень 2017 р.) залежно від інтенсивності гібридної небезпеки та намірів залучених акторів виокремлюються: гібридна загроза ('явище, що є наслідком зближення і взаємної пов'язаності різних елементів, які разом формують більш складну і багатовимірну загрозу'), гібридний конфлікт ('ситуація, в якій сторони конфлікту уникають явного використання збройних сил одна проти одної, покладаючись натомість на поєднання військового залякування (незавершені атаки), використання економічних і політичних вразливостей, дипломатичні чи технологічні засоби досягнення своїх цілей'), гібридна війна ('ситуація, в якій країна вдається до явного використання збройних сил проти іншої країни чи недержавного актора разом із сумішшю інших засобів, зокрема, економічних, політичних та дипломатичних'). Документ називає викликом необхідність переходу від статичного розуміння переліку гібридних загроз до розуміння "динамічної природи гібридності", тобто процесів, а також передумов і мотивів цих процесів, що можуть перетворювати певні ситуації на гібридні загрози[38].

У документі вказується на *сучасні тенденції у протидії гібридним загрозам.* 1. Концептуальні тенденції: поява, окрім управлінських, загальносуспільних стратегій менеджменту ризиків та побудови стійких суспільств. Як зазначається, 'фокусування на стійкості допомагає пом'якшити ризики, які можуть вести до гібридних конфліктів у майбутньому (зокрема, щодо енергії чи доступу до води), та вдосконалює практики асоційованого менеджменту ресурсів'. 2. Матеріальні тенденції: публічно-приватне співробітництво щодо безпеки і розвитку, яке враховує, що ресурси протидії гібридним загрозам перебувають у руках не лише уряду, а й громадянського суспільства, приватного сектора, окремих громадян. 3. Правові тенденції: посилення взаємодії між державами для вироблення спільних підходів до кваліфікації гібридних загроз, а також альтернативних конвенціям підходів (зокрема, заходів щодо розвитку довіри, співробітництва у сфері правозастосування тощо). 4. Інституційні тенденції: розширення сфери діяльності наявних чи створення нових інституцій[39].

[37] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats – a European Union response (n 36).
[38] Countering hybrid threats: EU-NATO cooperation. European Parliamentary Research Service Briefing. March 2017. EPRS_BRI(2017)599315_EN.
[39] Ibid.

Доповідь Європейської Комісії "Підвищення стійкості та підтримка спроможностей для відповіді на гібридні загрози" 2018 р. важливим елементом відповіді на гібридні загрози називає посилення стійкості, яке залишається здебільшого у сфері відповідальності держав-членів. Але ЄС у співпраці з НАТО сприяє їм у цьому. З цією метою у 2016 р. було підписано спільну декларацію двох організацій[40]. Чотирма сферами пріоритетного співробітництва ЄС і НАТО щодо протидії гібридним загрозам є: ситуаційне оповіщення, стратегічні комунікації, кібербезпека, попередження і залагодження криз[41].

Стратегія безпеки ЄС "Безпечний союз" 2020 р. пропонує 'загальносуспільний підхід до безпеки, який може у координованій манері ефективно відповідати швидкозмінному ландшафту загроз'. Основні підходи ЄС, згідно із стратегією, полягають у "внутрішньо-зовнішньому зв'язку" (координації дій держав-членів та взаємодії зі стратегічними партнерами, зокрема з НАТО і G7), усвідомленні та впровадженні безпекового виміру в будь-якій політиці з метою формування 'екосистеми безпеки, що охопить весь обшир європейського суспільства'. Поняття останньої засноване на розумінні безпеки як спільної відповідальності європейських та національних інституцій, бізнесу, громадського сектора та громадян, пов'язаності безпеки з основоположними цінностями, зростанні взаємного зв'язку між внутрішньою і зовнішньою безпекою[42].

Як зазначається у документі, криза, пов'язана з вірусом *COVID-19*, продемонструвала, 'як соціальні поділи та невизначеності створюють безпекову вразливість', що посилює потенціал складних та гібридних атак держав і недержавних акторів. Ці напади використовують вразливості за допомогою суміші кібератак, руйнування критичної інфраструктури, кампаній дезінформації, радикалізації політичного наративу. Зокрема, пандемія інструменталізується через 'маніпуляцію інформаційним середовищем та виклики ключовій інфраструктурі', ослаблення соціальної згуртованості, підрив довіри до інституцій ЄС та урядів держав-членів.

Серед основних засобів протидії гібридним загрозам називаються: раннє виявлення, аналіз, готовність, 'розвиток стійкості й попередження через відповіді на кризи та управління їх наслідками'. Важливо, що наголошено, хоча й не розкрито, на необхідності ініціатив у сферах освіти, технологій та наукових досліджень. Як зазначається у документі, цен-

[40] Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 13.6.2018. JOIN(2018) 16 final <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016> (accessed: 10.01.2022).

[41] Joint Staff Working Document EU operational protocol for countering hybrid threats "EU Playbook". Brussels, 5.7.2016. SWD(2016) 227 final.

[42] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. COM/2020/605 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605> (accessed: 10.01.2022).

тральним для попередження і захисту від гібридних загроз є розвиток стійкості. Тому структури ЄС збиратимуть, поширюватимуть, аналізуватимуть інформацію в цій сфері й мають створити єдині стандарти для держав-членів, зокрема "базові показники секторальної гібридної стійкості", протоколи відповідей на гібридні кризи[43].

Спеціалізованою аналітичною й контррозвідувальною структурою ЄС є *EU Hybrid Fusion Cell,* що перебуває у структурі Розвідувального і ситуаційного центру *(EU Intelligence and Situation Centre, EU INTCEN)* – частини Служби зовнішньої діяльності ЄС. Зокрема, вона фокусується на ідентифікації зовнішніх гібридних загроз щодо ЄС та держав Східного партнерства. Створено також Міжгалузеву групу "Протидія гібридним загрозам" *(ISG "Countering Hybrid Threats")*, яка аналізує виконання програмних цілей актів ЄС щодо протидії гібридним загрозам. Існує "Гібридна мережа ЄС" *(Points of Contact for EU Hybrid Network)* – мережа відповідальних за співробітництво представників європейських і національних відомств, сфера діяльності яких пов'язана з гібридними загрозами. Ця мережа забезпечує оперативну взаємодію з *Hybrid Fusion Cell*[44]. У 2015 р. засновано експертну структуру *East Stratcom Task Force* для боротьби з дезінформацією з боку РФ та розвитку комунікацій з державами Східного партнерства. Пізніше за її зразком було створено відповідні структури для Західних Балкан й арабомовного світу. Здійснюються заходи щодо перевірки стійкості різних сфер життєдіяльності європейських держав[45].

Забезпечення протидії гібридним загрозам в українському законодавстві

Протягом тридцятилітнього незалежного розвитку в Україні було створено розвинену систему законодавства у сфері захисту національної безпеки. Починаючи з 1990-х років (Концепція (основи державної політики) національної безпеки України[46], схвалена Постановою Верховної Ради України у 1997 р., стратегії національної безпеки, закони "Про основи національної безпеки України"[47], "Про Цивільну оборону України"[48] та ін.) вона відрізняється концептуальною комплексністю, не лише регулюючи основні сфери реальних і потенційних загроз, а й розглядаю-

[43] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. COM/2020/605 final (n 42).

[44] Joint Staff Working Document EU operational protocol for countering hybrid threats "EU Playbook" (n 41).

[45] Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 13.6.2018. JOIN(2018) 16 final (n 40).

[46] Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 р. № 3/97-ВР <https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80#Text> (дата звернення: 10.01.2022).

[47] Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964-IV <https://zakon.rada.gov.ua/laws/show/964-15#Text> (дата звернення: 10.01.2022).

[48] Про Цивільну оборону України: Закон України від 3 лютого 1993 р. № 2974-XII <https://zakon.rada.gov.ua/laws/show/2974-12#Text> (дата звернення: 10.01.2022).

чи їх у нерозривному зв'язку зовнішніх і внутрішніх чинників, суб'єктності держави, суспільства і громадянина. Іншою важливою характеристикою законодавства України в цій сфері є спрямованість не лише на збереження функціонування держави і життєдіяльності суспільства, а й на захист демократичного розвитку, прав і свобод людини, притаманних українському суспільству цінностей.

Водночас визначені засади й орієнтири тривалий час залишалися значною мірою декларативними. Наприклад, законодавство щодо цивільного захисту від початку було спрямоване на вирішення питань надзвичайних ситуацій. Тому воно охоплює питання вразливостей у життєдіяльності суспільства й економіки лише частково. Водночас воно весь час було значною мірою декларативним, ніколи повністю не виконувалося, не забезпечувалося достатньо ані кадрово, ані фінансово, ані матеріально. В умовах приватизації та браку уваги держави до цивільної оборони її інфраструктура не розвивалася, була частково перепрофільована або зруйнована.

У чинному Законі України "Про національну безпеку України"[49] поряд із державною безпекою було запроваджено категорії громадської безпеки і порядку – як захищеності життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості. У Законі передбачено інституційну структуру забезпечення національної безпеки, що визначає сфери відповідальності та взаємодію центральних органів виконавчої влади.

Закон, що значною мірою має рамковий характер, передбачив необхідність своєї деталізації й реалізації у низці стратегічних документів (документів довгострокового планування), що повинні схвалюватися Радою національної безпеки і оборони України і затверджуватися указами Президента України. Вони, в свою чергу, мають бути основою для розроблення галузевих стратегій і концепцій, державних цільових програм, оперативних планів та планів застосування сил і засобів у кризових ситуаціях міністерствами та іншими центральними органами виконавчої влади. Також передбачено проведення комплексних оглядів сектора безпеки і оборони, включно з оглядом громадської безпеки та цивільного захисту, які має організовувати Кабінет Міністрів України й затверджувати Рада національної безпеки і оборони України (далі – РНБО) та які мають сприяти послідовному нарощуванню спроможностей складових національної безпеки.

[49] Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 10.01.2022).

Не маючи змоги тут проаналізувати положення всього законодавства України у сфері захисту національної безпеки, звернемо увагу ще на два, на нашу думку, найбільш новаційні за предметом регулювання акти законодавства. Закон України "Про основні засади забезпечення кібербезпеки України"[50] 2017 р. вводить в українське право систему нових понять – кібернетичний інцидент, кібератака, кібербезпека та ін. Ключові категорії закону пов'язуються з виявленням, запобіганням і нейтралізацією реальних і потенційних загроз національній безпеці, забезпеченням сталого розвитку інформаційного суспільства та цифрового комунікативного середовища. Закон передбачає формування державного реєстру об'єктів критичної інформаційної інфраструктури, щодо яких Кабінет Міністрів України має розробити загальні вимоги кіберзахисту, індикатори кіберзагроз, вимоги до проведення незалежного аудиту інформаційної безпеки. Закон України "Про основи національного спротиву"[51] розкриває сучасну концепцію всезагального спротиву із залученням громадян до дій, спрямованих на забезпечення воєнної безпеки, суверенітету й територіальної цілісності держави, стримування, стійкість і відсіч агресії, завдання противнику неприйнятних втрат, зокрема, шляхом організації руху опору.

Положення цих та інших законів, ратифікованих Україною міжнародних договорів розкриваються у документах довгострокового планування. Основним серед них є Стратегія національної безпеки України, що затверджується указом Президента України. Однією з основних засад чинної Стратегії національної безпеки України 2020 р. є концепт стійкості, який розуміється як здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх вразливостей. Питання стійкості у Стратегії розглядається щодо кожної визначеної в ній сфери, вразливої до загроз національній безпеці. Стратегія оперує поняттям гібридної війни, пов'язуючи з нею політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби здійснення агресії. Наголошується на підривній діяльності РФ проти України, спрямованій на дестабілізацію українського суспільства, його роз'єднання, зокрема за допомогою його вразливостей і перетворення деструктивних внутрішніх акторів на інфраструктуру зовнішнього впливу.

Стратегія національної безпеки 2020 р. передбачає розробку стратегічних документів для її реалізації в різних сферах. Але сьогодні ухвалено менше половини із запланованих документів, зокрема: Стратегію людського розвитку; Стратегію воєнної безпеки України; Стратегію розвитку

[50] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 10.01.2022).

[51] Про основи національного спротиву: Закон України від 16 липня 2021 р. № 1702-IX <https://zakon.rada.gov.ua/laws/show/1702-20#Text> (дата звернення: 10.01.2022).

оборонно-промислового комплексу України; Стратегію економічної безпеки; Стратегію енергетичної безпеки; Стратегію кібербезпеки України.

Серед стратегічних документів галузевого характеру слід відзначити насамперед Стратегію воєнної безпеки 2021 р. Вона заснована на ідеї стійкого й всеохоплюючого стримування та опору, які передбачають використання для відсічі агресії всього потенціалу держави та суспільства, застосування у боротьбі всіх законних форм збройної боротьби, включно з асиметричними діями, налагодження надійних каналів комунікації з населенням та підтримання його життєдіяльності. Серед іншого передбачається підтримання не лише оперативного і мобілізаційного, а й громадського військового резерву. Стримування в контексті всеохоплюючої оборони України передбачає готовність не лише сил оборони, а й національної економіки, населення та всієї держави до відсічі збройній агресії. Значною мірою Стратегія складається з доволі загальних положень без розкриття форм, засобів та інституційного забезпечення їх реалізації.

Натомість Стратегія економічної безпеки України на період до 2025 р., затверджена у 2021 р., має не лише теоретичний, а й цілком визначений практичний, хоча й вузький, потенціал. У Стратегії помітна орієнтація на усвідомлення і концептуалізацію безпекової складової у різних сферах життєдіяльності з метою забезпечення їх стійкості від зовнішніх і внутрішніх викликів та загроз. Стратегія обґрунтовує постійний моніторинг і щорічну оцінку економічної стійкості на основі визначених індикаторів рівня економічної безпеки та їх критичних меж, наводяться відповідні індикатори та методики, розроблені на основі уточнення розробок, запроваджених Міністерством економічного розвитку й торгівлі України в 2013 р.

Стратегія енергетичної безпеки 2021 р., схвалена розпорядженням Кабінету Міністрів України, розвиває поняття стійкості функціонування енергетичного сектора на основі диференціації викликів, ризиків та загроз у цій сфері та принципів і завдань їх менеджменту. У документі заявлено про необхідність запровадження механізму співпраці та взаємодії між державою та операторами критичної інфраструктури енергетичного сектора на випадок кризових ситуацій, зокрема щодо залучення представників держави до участі та контролю за виконанням планів реагування на кризи, механізмів державно-приватного партнерства для забезпечення енергетичної безпеки. Але загалом Стратегія має значною мірою декларативний характер.

Стратегія кібербезпеки України 2021 р. у дусі підходів останнього десятиліття до проблем безпеки визнає кіберпростір разом з іншими фізичними просторами одним з можливих театрів воєнних дій, а також пропонує загальне бачення кібервикликів і кіберзагроз, і зокрема в умовах пандемії *COVID-19*, передумов та чинників, які формують такі загро-

зи. Принципами протидії таким загрозам, слідом за документами НАТО, називаються стримування, стійкість і взаємодія. Констатуючи суттєві успіхи України в інституційному і технічному забезпеченні протидії кіберзагрозам, Стратегія визначає подальші потреби цієї сфери, адаптуючи загальні безпекові орієнтири НАТО й українського законодавства. Зокрема, це стосується й залучення до вирішення завдань у цій сфері більш широкого кола учасників, зокрема й суб'єктів господарювання, громадські об'єднання та окремих громадян України. Значну увагу в документі приділено вже створеному Національному координаційному центру кібербезпеки, який є робочим органом РНБО України. Власне, Стратегія докладно викладає та уточнює повноваження цього органу. Також пропонується низка ініціатив у сфері розвитку кібербезпеки, які може бути реалізовано державними органами, приватним і громадським сектором. Їх має бути деталізовано у плані реалізації Стратегії, що буде розроблено Національним координаційним центром кібербезпеки, без уточнення суб'єкта схвалення (вірогідно, РНБО). Передбачається регулярне здійснення огляду стану національної системи кібербезпеки, а також кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Декларується перспективна розробка постійної оцінки ефективності реалізації Стратегії на основі системи індикаторів стану кібербезпеки. Достатньо знаковим також вважаємо вказівку в Стратегії на наступальні дії в кіберпросторі як один з орієнтирів політики безпеки України.

До документів стратегічного планування у сфері протидії загрозам національної безпеки можна віднести й інші нормативно-правові акти, наприклад, затверджену указом Президента України Концепцію боротьби з тероризмом в Україні 2019 р. Вона, зокрема, передбачає визначення переліку і характеристик, заходів щодо захисту, ведення реєстру найбільш уразливих об'єктів можливих терористичних посягань, оцінку терористичних ризиків тощо.

Розроблено систему інших підзаконних актів на виконання положень законодавства у сфері протидії гібридним та іншим загрозам національній безпеці. Наприклад, це акти Кабінету Міністрів України: Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури 2019 р., Порядок формування переліку об'єктів критичної інформаційної інфраструктури 2020 р., Розпорядження про затвердження плану заходів з реалізації Концепції боротьби з тероризмом в Україні 2021 р. тощо.

Одним з останніх у цій сфері є Указ Президента України від 17 вересня 2021 р. "Про Стратегічний оборонний бюлетень України"[52], який

[52] Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України": Указ Президента України 17 вересня 2021 р. № 473/2021 <https://zakon.rada.gov.ua/laws/show/473/2021#Text> (дата звернення: 10.01.2022).

визначає основні напрями реалізації воєнної політики України в контексті всеохоплюючої оборони України, перспективну модель Збройних Сил України та інших складових сил оборони і вимоги до її побудови, основні спроможності сил оборони, яких необхідно досягти, стратегічні цілі розвитку сил оборони, основні завдання та очікувані результати їх досягнення.

Документ розкриває закладену в Законі України "Про основи національного спротиву" концепцію всеохоплюючої оборони й стійкого опору як використання всього потенціалу держави та суспільства в умовах неможливості досягнення воєнного паритету з противником, а також запропоновану в Стратегії національної безпеки України ідею асиметричних дій. Асиметричні та непрямі дії згідно із Стратегічним оборонним бюлетенем – це вміння вчиняти дії, які відрізняються від дій противника, з організацією своєї діяльності та мислення таким чином, щоб відрізнятися від нього з метою використання його вразливих місць та максимізації своїх переваг, шляхом перехоплення ініціативи та/або забезпечення простору для маневрування, ефективного використання факторів моральної переваги країни, яка захищає свої національні цінності та національні інтереси. Варто підкреслити також відображені в документі ідеї превентивних дій, здійснення впливу на кіберпростір противника, знищення або захоплення кіберінфраструктури противника, мережецентричного підходу до ведення бойових дій. Стратегічний оборонний бюлетень наголошує на координації дій і розподілі відповідальності всіх державних органів і суспільства, розвитку ефективної системи стратегічних комунікацій із суспільством тощо.

Висновки. На нашу думку, гібридну війну можна визначити як новий тип протистояння держав між собою та з недержавними акторами, діалектично пов'язаний із забороною в міжнародному праві звичайної війни як засобу національної політики. У вузькому розумінні, характерному для військових аналітиків, гібридна війна становить поєднання регулярних та іррегулярних методів ведення війни. У широкому і більш відповідному реаліям баченні гібридна війна є видом протистояння, заснованим на неофіційних, неавторизованих чи замаскованих невоєнних і воєнних ворожих діях, спрямованих на ураження всіх сфер життєдіяльності суспільства, включно із функціонуванням держави та економіки, соціальними комунікаціями, модусами поведінки людей. Можна визначити такі характеристики гібридної війни: транскордонність, тотальність і безперервність; неофіційний характер, за якого держави уникають формального проголошення війни; спрямованість на створення контрольованого реального чи суб'єктивно відчутого хаосу; домінування невоєнних засобів; різноманітність і ситуативність методів, що не піддаються точній класифікації, а відповідають вразливостям кожної сфери життєдіяль-

ності та цінностей людини й суспільства; відсутність чіткої межі між зовнішньою і внутрішньою політикою в здійсненні й протидії гібридній війні; широке використання методів психологічного впливу на населення. На нашу думку, транскордонний, атериторіальний характер частини методів гібридної війни припускає дзеркальний або діалектичний вплив на суспільство не лише об'єкта, а й суб'єкта гібридної агресії – тому ефективний насамперед у ситуації значних відмінностей між суспільствами, коли припущені недоліки першого відповідають припущеним перевагам іншого. Крім того, в умовах світової гібридної війни немає сфер, регіонів чи держав абсолютної невразливості, але перевагу мають громадянські суспільства з найбільш стійкими демократичними традиціями, безсумнівністю демократичної легітимності основних процедур і процесів, або найбільш контрольовані й закриті тоталітарні держави з архаїчним рівнем суспільного розвитку, а найбільш вразливими є суспільства і держави у процесі суттєвого реформування.

Для концептів та орієнтирів НАТО у сфері протидії гібридним загрозам було характерне формальне обмеження розуміння безпеки та нападу переважно військовими питаннями. Але починаючи з 2014 р., це бачення поступово розширюється, спочатку через поняття прихованих операцій та інформаційних засобів протистояння. Найновішою тенденцією є наголос стратегічних документів НАТО на таких гібридних загрозах, як кібернапади, шкідлива економічна діяльність, свідоме порушення режиму постачання енергоносіїв.

У документах НАТО останніх років акценти суттєво зміщуються, дедалі більше увага приділяється безпеці цивільних спроможностей як "першої лінії оборони", а в межах концептів стійкості та цивільної готовності затираються межі між гібридними, природними і техногенними загрозами. При цьому цивільна готовність передбачає, зокрема, інтеграцію безпекової діяльності національних органів влади, приватного і громадського секторів, а основою стійкості проголошується відданість спільним цінностям держав-учасниць.

НАТО проголошує протидію гібридним загрозам насамперед сферою відповідальності держав-учасниць, які мають підвищувати свою стійкість. Альянс встановлює базові вимоги щодо стійкості, серед яких насамперед захист державного управління, порядку, комунікацій, включно з інформаційними мережами, та забезпечення базових потреб населення. Водночас принциповими змінами у розумінні відповідальності НАТО стало визнання починаючи з 2015 р. гібридного нападу (фізичних дій, а згодом і віртуальних) видами збройної агресії, що передбачають можливість колективної оборони. Крім того, НАТО визначила сферою своєї діяльності збирання і поширення інформації, консультування, методичну та експертну допомогу в сфері протидії гібридним загрозам.

ПРАВО УКРАЇНИ • 2022 • № 1 • 131-155

ЄС розвиває свою стратегію протидії гібридним загрозам починаючи з 2015 р. Як і НАТО, ЄС проголошує протидію гібридним загрозам насамперед сферою відповідальності держав-членів, але на себе покладає координацію їх політики, встановлення і забезпечення дотримання єдиних стандартів, збирання інформації та здійснення перспективних аналітичних досліджень. Водночас значна частина повноважень щодо колективної протидії гібридним загрозам фактично передається НАТО.

Стратегічні документи ЄС вказують на динамічну природу феномена гібридності, яка має мінливий процесуальний характер, який складно точно ідентифікувати та класифікувати, а також на синергетичний характер гібридних викликів, що саме у своєму поєднанні створюють комплексні загрози суспільству. Для підходів ЄС характерна концепція загальносуспільного менеджменту ризиків як елемента протидії гібридним загрозам. Вона, зокрема, передбачає розгляд частини загроз як викликів, що за умови їх передбачення та адекватної відповіді можуть стати шансом для посилення стійкості суспільств і держав. Зокрема, йдеться про необхідність гармонізації суспільних відносин, усунення передумов для розвитку екстремізму й радикалізму, пом'якшення ризиків, інклюзивний менеджмент ресурсів тощо.

Завдяки такому підходу, як припускається, ризики (принаймні, внутрішні) не повинні перетворитися на загрози, що здатні стати передумовою гібридного конфлікту і навіть гібридної війни. При цьому ключовим є розвиток публічно-приватного співробітництва з метою збереження довіри до європейських і національних інституцій, відданості спільним цінностям, усвідомлення і реалізація безпекового виміру будь-якої сфери політики держав та ЄС, нерозривності внутрішнього і зовнішнього вимірів безпеки суспільства.

В Україні було створено розвинене, але значною мірою декларативне законодавство у сфері захисту національної безпеки. І лише починаючи з 2018 р. було вперше централізовано управління, запропоновано систему координації органів влади у сфері національної безпеки, створено нормативно-правові основи для комплексної інституційної структури забезпечення національної безпеки як сфери відносин і взаємодії органів виконавчої влади та інших інститутів. І так само вперше протягом сучасного етапу було створено засади ієрархічної структури нормативно-правових актів, згідно з якою загальні положення законів розкриваються у визначеному переліку стратегічних документів (документів довгострокового планування), деталізуються у галузевих стратегіях і концепціях, державних цільових програмах, комплексних оглядах сектора безпеки і оборони, операційних документах (операційних планах, планах застосування сил і засобів, протоколах реагування на кризові ситуації та відновлення після них, реєстрах об'єктів). Нарешті, все це забезпечується

нормативно-правовими актами і положеннями технічного характеру, що містять механізми й засоби оцінки і моніторингу стійкості й вразливості, ризиків і загроз (індикатори, вимоги, методики, порядки, плани реалізації, матеріали оглядів тощо).

Також сучасний етап розвитку законодавства України у сфері національної безпеки характеризується: новими філософськими засадами, визначеними як "нова культура безпеки", що виявляються в усвідомленні безпекової складової всіх сфер життєдіяльності, ідеї стійкості як менеджменту вразливостей і побудови спроможностей; запозиченням безпекових стандартів і концепцій НАТО; відмовою від виключних переліків категорій загроз, адже гібридизація агресії зробила це неактуальним; поступовим формуванням інтегральної або загальносуспільної концепції безпеки, елементом якої є, зокрема, ідея всеохоплюючої оборони; розширенням і модернізацією розуміння предмета регулювання законодавства, що дала змогу врахувати поряд із фізичним також віртуальний простір протистояння з притаманними для нього загрозами.

Водночас законодавство у сфері захисту національної безпеки, і зокрема від гібридних загроз, має й суттєві недоліки. Зокрема, цілком статистично-описовою і декларативною є Стратегія людського розвитку, схвалена у 2021 р., що за змістом не зовсім відповідає передбаченому для неї статусу документа довгострокового планування у сфері національної безпеки. В інших сучасних нормативно-правових актах втрачено попередні пропозиції щодо конкретних механізмів громадського контролю і залучення громадськості до вироблення і реалізації політики національної безпеки, розробки індикаторів оцінки захищеності національних інтересів, регулярного проведення порівняльно-правового моніторингу законодавства держав-сусідів і провідних держав світу (запропоновані, наприклад, у Стратегії національної безпеки 2007 р.) та ін. Практично не розкритими у законодавстві залишаються форми й механізми взаємодії держави з приватним сектором.

Можливо, однією з найважливіших сутнісних характеристик сучасного визначеного у законодавстві бачення захисту національної безпеки є його, як це дивно не звучало б, гібридність. Усвідомлення сутності й механізмів гібридних загроз привело до діалектичної відповіді – синтезу традиційної й нової гібридної стратегії протистояння. Саме тому сучасна українська безпекова стратегія заснована на цілком гібридному поєднанні регулярних та іррегулярних методів ведення бойових дій, кібероперацій та інших засобів протистояння. Це виявляється у концепціях стійкого опору, асиметричних і непрямих дій, мережоцентричного підходу до ведення бойових дій, наступальних дій у кіберпросторі тощо.

ПРАВО УКРАЇНИ • 2022 • № 1 • 131-155

REFERENCES

Bibliography

Authored books

1. Fleming B, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. Fort Leavenworth* (United States Army Command and General Staff College 2011) (in English).
2. Tarasiuk V, *Zastosuvannia informatsiinykh tekhnolohii v umovakh hibrydnoi viiny* (GlobeEdit 2020) (in Ukrainian).

Edited books

3. Sari A (ed), *Hybrid threats and the law: Concepts, trends and implications* (The European Centre of Excellence for Countering Hybrid Threats 2020) (in English).
4. *Hibrydni zahrozy Ukraini i suspilna bezpeka. Dosvid YeS i Skhidnoho partnerstva. Analitychnyi dokument* (Martyniuk V red, 2018) (in Ukrainian).
5. Horbulin V (red), *Svitova hibrydna viina: ukrainskyi front* (NISD 2017) (in Ukrainian).

Journal articles

6. Pyrozhkov S, Bozhok Ye, Khamitov N, 'Natsionalna stiikist (rezylientnist) krainy: stratehiia i taktyka vyperedzhennia hibrydnykh zahroz' (2021) 8 Visnyk NAN Ukrainy (in Ukrainian).

Websites

7. Roepke W-D, Thankey H, 'Resilience: the first line of defence' (*NATO Review*, 27.02.2019) <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html> (accessed: 10.01.2022) (in Ukrainian).
8. Gerasimov V, 'Cennost' nauki v predvidenii. Novye vyzovy trebujut pereosmyslit' formy i sposoby vedenija boevyh dejstvij' *(Voenno-promyshlennyj kur'er*, 27.02.2013) <http://www.vpk-news.ru/articles/14632> (accessed: 10.01.2022) (in Russian).
9. Horbulin V, 'Iakyi Feniks narodytsia zi zgharyshcha svitovoi hibrydnoi viiny?' (*Dzerkalo tyzhnia*) <https://zn.ua/ukr/article/print/internal/yakiy-feniks-naroditsya-zi-zgarischa-svitovoyi-gibridnoyi-viyni-259112_.html> (accessed: 10.01.2022) (in Ukrainian).

Oleksiy Kresin

COUNTERING HYBRID THREATS: INTERNATIONAL EXPERIENCE AND UKRAINIAN LEGISLATION

Abstract. Confrontation between states and various non-state actors throughout human history has never been reduced to purely military means and has not been limited to periods of officially declared wars. The history of hybrid methods of warfare is not only a field, but also a promising area of research. But in the context of immediate practical needs, it is advisable to analyze modern forms of their use and understanding. An important prerequisite for the emergence of hybrid warfare was the prohibition of war under international law, which, of course, reflected significant changes in the worldview of much of humanity. The modern and general form of prohibition of war under

international law is enshrined in the UN Charter. These principles have been consistently disclosed and improved in subsequent UN acts.

Hybrid warfare can be defined as a new type of confrontation between states and non-state actors, dialectically linked to the prohibition of conventional warfare in international law as a means of national policy. In the narrow sense of the word for military analysts, hybrid warfare is a combination of regular and irregular methods of warfare. In a broader and more realistic view, hybrid warfare is a form of confrontation based on informal, unauthorized, or disguised non-military and military hostilities aimed at destroying all spheres of society, including the functioning of the state and economy, social communications, and human behavior. The following characteristics of hybrid warfare can be identified: cross-border, totality and continuity; informal nature, in which states avoid the formal declaration of war; focus on creating controlled real or subjectively felt chaos; dominance of non-military means; variety and situationality of methods that are not subject to accurate classification, but correspond to the vulnerabilities of each sphere of life and values of man and society; lack of a clear line between foreign and domestic policy in implementing and countering hybrid warfare; widespread use of methods of psychological influence on the population.

Keywords: prohibition of war; hybrid warfare; hybrid methods of warfare; countering hybrid threats.