Розділ VIII

ПРОБЛЕМИ МІЖНАРОДНОГО ПРАВА

DOI: 10.33663/1563-3349-2022-33-516-529
УДК: 341.322

О. В. КРЕСІН,
доктор юридичних наук,
*старший науковий співробітник**
ORCID: 0000-0002-4016-6596

ІНСТИТУЦІЙНО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У НАТО ТА ЄС

Правове забезпечення НАТО у сфері протидії гібридним загрозам характеризувалося формальним обмеженням розуміння безпеки та нападу переважно воєнними питаннями. Але, починаючи з 2014 р., у нормативно-правових актах НАТО послідовно розвиваються концепти стійкості та цивільної готовності, стираються межі між гібридними, природними і техногенними загрозами. Як і НАТО, ЄС з 2015 р. 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.

Ключові слова: *гібридні загрози, гібридна війна, право міжнародних організацій, право міжнародної безпеки, стійкість, цивільна готовність.*

Kresin Oleksii. **Institutional and organizational bases of countering hybrid threats in NATO and the EU**

NATO's legal provisions in the field of countering hybrid threats were characterized by formal restrictions of the understanding of security and attack mainly by military issues. But since 2014, NATO's regulations have consistently developed the concepts of resilience and civilian preparedness, blurring the lines between hybrid, natural and man-made threats. Like NATO, the EU since 2015 declares countering hybrid threats primarily the responsibility of member states, but is responsible for coordinating their policies, setting and enforcing unified standards, gathering information and conducting forward-looking analytical research.

Key words: *hybrid threats, hybrid war, law of international organizations, law of international security, resilience, civil preparedness.*

* ***Kresin Oleksii****, Doctor of Juridical Sciences, Senior Research Officer*

Протягом багатьох десятиліть «холодної війни» ключовою для спільної політики держав-членів НАТО щодо протидії зовнішнім загрозам 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[1].

Звичайно, стратегічні документи НАТО і національне законодавство держав-членів 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 відповідне фінансування було суттєво зменшено[2]. 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[3].

Поняття гібридної загрози як поєднання державами та недержавними акторами конвенційних і неконвенційних засобів ворожих дій було включене до Стратегічного концепту НАТО і «Доктрини Кепстоун» НАТО у 2010 р.[4]

Але можна стверджувати, що саме нові виклики, насамперед з боку Російської Федерації та дії ІДІЛ, спонукали НАТО звернути увагу на гібридні загрози. Зокрема, у 2014 р. генеральний секретар НАТО А. Расмуссен звинуватив Росію у веденні гібридної війни, яку визначив як «комбінацію воєнних дій, прихованих операцій і агресивної програми дезінформації»[5].

У 2015 р. на саміті міністрів закордонних справ держав-членів НАТО було ухвалено стратегію щодо ролі цієї організації у протидії гібридній війні, в якій підкреслюється основна відповідальність держав-членів 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-членам виявляти їх вразливості та посилювати їх 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-членів від будь-якої загрози[6]. Зокрема, очевидно вперше у цьому документі гібридні напади було кваліфіковано як вид агресії, що є підставою для колективної оборони (застосування ст. 5 Вашингтонського договору)[7].

Ще важливішими є документи, ухвалені за підсумками Варшавського саміту Північноатлантичної ради 2016 р., тобто зустрічі всіх глав держав і голів урядів держав-членів. Зокрема, у комюніке саміту гібридну війну було визначено як широку, складну та гнучку комбінацію конвенційних і неконвенційних засобів, відкритих і прихованих воєнних, парамілітарних і цивільних заходів протистояння, що використовуються державами та недержавними акторами у високоінтегрований спосіб для досягнення їх цілей. Було підтверджено поширення на можливі випадки гібридної війни зобов'язання щодо колективної оборони[8].

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 зміни 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»[9].

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 адресатів, 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)[10].

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[11].

У Декларації Брюссельського саміту Північноатлантичної ради 2018 р. було зазначено, що метою гібридної діяльності держав і недержавних акторів є створення непевності та стирання межі між миром, кризою та конфліктом. У документі було підкреслено готовність НАТО за рішенням Північноатлантичної ради допомагати державам-членам 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[12].

Вимоги Варшавської резолюції 2016 р. уточнювалися у наступних 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[13].

У комюніке Брюссельського саміту Північноатлантичної ради у червні 2021 р. було проголошено створення Всеохопної політики кібернетичного 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-членів, рівнозначним збройному нападу, що передбачає колективну оборону. Значну увагу приділено енергетичній безпеці, зокрема диверсифікації та інтеграції шляхів постачання енергоносіїв, захисту критичної інфраструктури[14].

У резолюції «Посилені зобов'язання щодо стійкості», ухваленій під час цього саміту як доповнення до Варшавської резолюції 2016 р., передбачається розробка державами-членами 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».

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 промисло-

вості, 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-членів (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[15].

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 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[16].

Аналітики НАТО відзначають, що згідно із сучасним розумінням ст. 3 Північноатлантичного договору «кожна держава – член НАТО має бути стійкою, щоби протистояти та відновлюватися після значних ударів, таких, як природна катастрофа, відмова критичної інфраструктури, гібридний чи збройний напад. Стійкість є здатністю суспільства протистояти і відновлюватися від таких ударів і поєднує як цивільну готовність, так і військову спроможність. Цивільна готовність є центральною опорою стійкості союзників та критичною передумовою колективної оборони Альянсу, і НАТО підтримує союзників у досягненні й посиленні їх цивільної готовності». Стійкість розглядається як насамперед і здебільшого відповідальність кожного члена. Шляхами підвищення стійкості є збільшення національної оборонної спроможності, гарантування доступу до критичної інфраструктури, розробка планів на випадок криз, постійна перевірка здатності забезпечити життєво необхідні послуги й підтримка збройних сил за допомогою цивільних, комерційних та інших засобів[17].

М. Рюле і К. Робертс визначають такі сучасні інструменти НАТО щодо протидії гібридним загрозам:

– покращення ознайомленості з обстановкою (створення спеціального підрозділу в складі Об'єднаного відділу розвідки і безпеки, який займається моніторингом і аналізом гібридних загроз; обмін державами-членами інформацією про внутрішні й зовнішні події; обмін розвідданими);

– адаптація навчань НАТО (запровадження гібридних елементів та сценаріїв; залучення високопоставлених представників органів державної влади);

– посилення стійкості членів Альянсу (дорадча допомога державам-членам щодо посилення стійкості інфраструктури; встановлення стандартних вимог оцінки в цій сфері);

– поліпшення кіберзахисту (вироблення рекомендацій щодо варіантів стратегічних відповідей на значну зловмисну кібердіяльність за допомогою політичних, військових, дипломатичних і економічних інструментів; запровадження зобов'язань держав-членів щодо вдосконалення кіберзахисту національних мереж та інфраструктури; поглиблення державно-приватного партнерства в цій сфері; створення «спільнот довіри» для обміну інформацією про кіберзагрози та протидію ним);

– створення команд підтримки протидії гібридній війні (невідкладне направлення спеціальних команд цивільних та військових фахівців до держав-членів у разі звернення);

– стримування гібридних загроз (підвищення ціни гібридних нападів для агресора – санкції, висилка дипломатів тощо);

– зближення цивільних і військових інструментів (розвиток набору комплексних варіантів дій із запобігання і реагування на гібридні загрози, координація виконання таких дій між політичними і військовими структурами НАТО, узгодження цих дій з іншими дійовими особами і зацікавленими сторонами);

– використання можливостей нових технологій штучного інтелекту і аналізу великих даних (виявлення і протидія кампаніям фейкових новин, підривній і диверсійній діяльності в Інтернеті; посилення можливостей розвідки, створення для цього спеціалізованих структур; співпраця з приватним сектором);

– виявлення і протидія дезінформації (розробка механізмів швидкого реагування; розвиток власної мережі інформування різними мовами; взаємодія зі ЗМІ; комунікація на випередження із вразливою аудиторією);

– розширення співпраці органів держав-членів на різних рівнях (залучення до роботи Північноатлантичної ради радників з питань національної безпеки і керівників національних органів, що відповідають за протидію гібридним загрозам з метою обміну інформацією і досвідом);

– поглиблення відносин між НАТО і ЄС (розробка так званих правил гри і оперативних протоколів щодо обміну інформацією про дезінформаційну діяльність; співпраця у рамках Європейського центру передового досвіду з протидії гібридним загрозам);

– розширення співробітництва з партнерами[18].

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-членів[19].

Європейський Союз 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. Зазвичай акцент робиться на використанні вразливостей цілі та на генеруванні неоднозначності для перешкоджання процесам прийняття рішень. Масові кампанії дезінформації, які використовують соціальні медіа для контролю політичного наративу або радикалізації, залучення та спрямування проксі-акторів, можуть стати засобами реалізації гібридних загроз… Гібридні загрози спрямовані на використання вразливостей країни і часто на підрив основоположних демократичних цінностей і свобод»[20].

Стверджуючи національну специфіку гібридних загроз і відповідальність за протидію їм держав – членів ЄС, доповідь наголошує на потребі координації їх 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. Новітні шляхи комунікації створюють можливість ідентифікації та рекрутування вразливих осіб, їх радикалізації, маніпулювання ними за допомогою пропаганди. Це передбачає елементи контролю щодо поширення інформації і протидії пропаганді, роботу з радикалізованими та вразливими особами, підготовку фахівців, обмін практиками та інформацією між державами, цілеспрямовану роботу правоохоронних органів, як і розуміння і усунення економічних, політичних та соцієтальних чинників, що сприяють розвитку екстремізму і радикалізму[21].

Як зазначається у доповіді Європейського Парламенту «Протидія гібридним загрозам: співпраця ЄС – НАТО» (березень 2017 р.), концепт гібридної загрози актуалізувався у зв'язку з діями Росії проти України та діяльністю ІДІЛ. Він охоплює «взаємопов'язану природу викликів (зокрема, етнічний конфлікт, тероризм, міграція, слабкі інституції), множинність залучених акторів (зокрема, регулярні та нерегулярні збройні формації, кримінальні угруповання) та різноманітність використання конвенційних і неконвенційних засобів (зокрема, військові, дипломатичні, технологічні)»[22].

Залежно від інтенсивності гібридної небезпеки та намірів залучених акторів документ виокремлює: гібридну загрозу («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»), гібридну війну («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[23].

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[24].

У Доповіді Європейської Комісії «Підвищення стійкості та підтримка спроможностей для відповіді на гібридні загрози» 2018 р. було зазначено, що гібридні загрози походять від держав та недержавних акторів і спрямовані, зокрема, на «дестабілізацію країн через підрив довіри громадськості до урядових інституцій та піддання сумніву ключових цінностей суспільств». Гібридні операції визначаються як складні для виявлення та атрибуції «багатовимірні, що поєднують насильницькі та підривні методи, використовують конвенційні та неконвенційні засоби й тактики (дипломатичну, військову, економічну і технологічну) для дестабілізації противника»[25].

Важливим елементом відповіді на гібридні загрози доповідь 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[26]. Чотирма сферами пріоритетного співробітництва ЄС і НАТО щодо протидії гібридним загрозам є: ситуаційне оповіщення, стратегічні комунікації, кібербезпека, запобігання і врегулювання криз[27].

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 зі 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[28].

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 поєднання 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, центральним для запобігання 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[29].

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 Європейської служби зовнішньої діяльності. 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[30].

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 і арабомовного світу[31].

Здійснюються заходи щодо перевірки стійкості різних сфер життєдіяльності європейських держав. Зокрема, у 2018 р. Європейська Комісія організувала дослідження прогалин у готовності держав ідентифікувати та запобігати загрозам хімічних, біологічних, радіологічних та атомних нападів. Разом із НАТО з 2017 р. відбуваються тестування готовності європейських держав відповідати, а інституцій ЄС – здійснювати координаційні функції в умовах масштабних гібридних криз. У 2017 р. було прийнято спільний план дій вищих органів ЄС щодо стійкості, стримування та оборони у сфері кібербезпеки, а передбачені ним положення протягом року було імплементовано у національні законодавства держав-членів. Оперативні питання взаємодії структур регулює протокол ЄС з протидії гібридним загрозам «EU Playbook» 2016 р. У 2016 і 2017 рр. прийнято директиви ЄС щодо безпеки мережевих та інформаційних систем[32].

Зазначимо також, що для протидії гібридним загрозам було засновано Європейський центр вдосконалення протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) – міжнародний незалежний аналітичний мережевий центр, який також є тематичною платформою взаємодії між ЄС та НАТО. Він базується у Гельсінкі й пропагує ідею запобігання і протидії на основі об'єднання зусиль влади і суспільства. Центр поширює кращі практики, розробляє нові підходи, пропонує програми тренування. Нині у його роботі бере участь мережа з 1200 експертів – практиків і вчених[33]. Як зазначається у новій монографії, підготовленій фахівцями Центру, «гібридні загрози стали невід'ємною частиною європейської безпеки», протидія їм потребує «загальносуспільного підходу, який об'єднує цивільних, військових та політичних акторів і належно веде до нової екосистеми безпеки»[34].

На підставі нашого дослідження можна зробити деякі висновки. Для концептів та орієнтирів НАТО у сфері протидії гібридним загрозам було характерне формальне обмеження розуміння безпеки та нападу переважно воєнними 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 більша увага приділяється безпеці цивільних спроможностей як «першої лінії оборони», а в межах концептів стійкості та цивільної готовності стираються 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-членів.

НАТО проголошує протидію гібридним загрозам насамперед сферою відповідальності держав-членів, 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) видом збройної агресії, що передбачає можливість колективної оборони. Крім того, НАТО визначила сферою своєї діяльності збирання і поширення інформації, консультування, методичну та експертну допомогу в сфері протидії гібридним загрозам.

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 і 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 ключовими є розвиток публічно-приватного співробітництва з метою збереження довіри до європейських та національних інституцій, відданості спільним цінностям, усві-

домлення і реалізація безпекового виміру будь-якої сфери політики держав та ЄС, неподільності внутрішнього і зовнішнього вимірів безпеки суспільства.

1. The North Atlantic Treaty. Washington D.C. 4 April 1949. URL: https://www.nato.int/cps/en/natohq/official_texts_17120.htm **2.** Roepke W.-D., Thankey H. Resilience: the first line of defence. NATO Review. 27 February 2019. URL: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html **3.** Resilience and Article 3. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm **4.** BI-SC Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats (25 August 2010). URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf **5.** Тарасюк В. Застосування інформаційних технологій в умовах гібридної війни: монографія. Beau Bassin: GlobeEdit, 2020. С. 58. **6.** NATO's response to hybrid threats. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en **7.** Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. Київ: НІСД, 2017. С. 36. **8.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid **9.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_133180.htm **10.** Resilience and Article 3… **11.** Roepke W.-D., Thankey H. Op. cit. **12.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21 **13.** Resilience and Article 3… **14.** 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. URL: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en **15.** Strengthened Resilience Commitment. https://www.nato.int/cps/en/natohq/official_texts_185340.htm **16.** Roepke W.-D., Thankey H. Op.cit. **17.** Resilience and Article 3… **18**. Рюле М., Робертс К. Розширення інструментарію НАТО з протидії гібридним загрозам. 19 березня 2021. URL: https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennya-nstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html **19.** Resilience and Article 3… **20.** Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response / European Commission. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN **21.** Ibidem. **22.** Countering hybrid threats: EU-NATO cooperation / European Parliamentary Research Service Briefing. March 2017. EPRS_BRI(2017)599315_EN. **23.** Ibidem. **24.** Ibidem. **25.** 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. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016 **26.** Ibidem. **27.** Joint Staff Working Document EU operational protocol for countering hybrid threats 'EU Playbook'. Brussels, 5.7.2016. SWD(2016) 227 final **28.** 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. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 **29.** Ibidem. **30.** Joint Staff Working Document EU operational protocol for countering hybrid threats… **31.** Joint Communication to the European Parliament, the European Council and the Council.

Increasing resilience and bolstering capabilities to address hybrid threats… **32.** Ibid. **33.** What is Hybrid CoE. https://www.hybridcoe.fi/who-what-and-how/ **34.** The Landscape of Hybrid Threats: A Conceptual Model Public Version. Luxembourg: Publications Office of the European Union, 2021. P. 43.

References

1. The North Atlantic Treaty. Washington D.C. 4 April 1949. URL: https://www.nato.int/cps/en/natohq/official_texts_17120.htm **2.** Roepke W.-D., Thankey H. Resilience: the first line of defence. NATO Review. 27 February 2019. URL: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html **3.** Resilience and Article 3. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm **4.** BI-SC Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats (25 August 2010). URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf **5.** Tarasiuk V. Zastosuvannia infornatsiynyh tehnologiy v umovah hibrydnoi viyny: Monohrafia. Beau Bassin: GlobeEdit, 2020. P. 58. [ukr]. **6.** NATO's response to hybrid threats. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en **7.** Svitova hibrydna viyna: ukrainskyi front: Monohrafia / Ed. by V. P. Horbulin. Kyiv: NISD, 2017. P. 36. [ukr]. **8.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid **9.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_133180.htm **10.** Resilience and Article 3… **11.** Roepke W.-D., Thankey H. Op. cit. **12.** 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. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21 **13.** Resilience and Article 3… **14.** 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. URL: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en **15.** Strengthened Resilience Commitment. https://www.nato.int/cps/en/natohq/official_texts_185340.htm **16.** Roepke W.-D., Thankey H. Op.cit. **17.** Resilience and Article 3… **18.** Riule M., Roberts K. Rozshyrennia instrumentariyu NATO z protydii hibrydnym zahrozam. 19 March 2021. [ukr]. URL: https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennya-nstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html **19.** Resilience and Article 3… **20.** Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response / European Commission. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN **21.** Ibidem. **22.** Countering hybrid threats: EU-NATO cooperation / European Parliamentary Research Service Briefing. March 2017. EPRS_BRI(2017)599315_EN. **23.** Ibidem. **24.** Ibidem. **25.** 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. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016 **26.** Ibidem. **27.** Joint Staff Working Document EU operational protocol for countering hybrid threats 'EU Playbook'. Brussels, 5.7.2016. SWD(2016) 227 final **28.** 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. URL:

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 **29.** Ibidem. **30.** Joint Staff Working Document EU operational protocol for countering hybrid threats… **31.** Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats… **32.** Ibid. **33.** What is Hybrid CoE. https://www.hybridcoe.fi/who-what-and-how/ **34.** The Landscape of Hybrid Threats: A Conceptual Model Public Version. Luxembourg: Publications Office of the European Union, 2021. P. 43.

Kresin Oleksii. **Recognition, regulation and countering hybrid threats in NATO and the EU**

Introduction*. Effective development of legal provisions for countering hybrid threats in the context of Russia's aggression against Ukraine should pressuppose studying the relevant experience of leading international organizations and the compatibility of Ukrainian legislation with the EU and NATO as fa as the European and Euro-Atlantic choice is stated in the Constitution. The aim of the article is to summarize the development and current state of legal provisions for countering hybrid threats in NATO and EU strategic documents, as well as to identify and analyze the main concepts of these documents that define their legal ideology. Results. The article presents a generalized vision of the legal framework for countering hybrid threats in NATO and EU strategy documents based on the application of dogmatic and comparative analysis methods, as well as reconstruction and structural-functional approach.*

Conclusions*. NATO's legal provisions in the field of countering hybrid threats were characterized by formal restrictions of the understanding of security and attack mainly by military issues. But since 2014, NATO's regulations have consistently developed the concepts of resilience and civilian preparedness, blurring the lines between hybrid, natural and man-made threats. Like NATO, the EU since 2015 declares countering hybrid threats primarily the responsibility of member states, but is responsible for coordinating their policies, setting and enforcing unified standards, gathering information and conducting forward-looking analytical research.*

Key words*: hybrid threats, hybrid war, law of international organizations, law of international security, resilience, civil preparedness.*