ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2017. Випуск 43. С. 54–63
Visnyk of the Lviv University. Series International Relations. 2017. Issue 43. P. 54–63

УДК 327.5-025.26-049.5

ГІБРИДНІ ЗАГРОЗИ МІЖНАРОДНІЙ БЕЗПЕЦІ ТА ШЛЯХИ ПРОТИДІЇ

Софія Федина

Львівський національний університет імені Івана Франка,
вул. Університетська,1, м. Львів, Україна, 79000,
тел. (032) 239-4132, (050) 9897440, e-mail: ukrainesinger@yahoo.com

Проаналізовано підходи до осмислення поняття «гібридна загроза» як новітнього феномена у міжнародних відносинах, особливості його виникнення та впливу на міжнародні процеси. Розглянуто існуючі концепти протидії гібридним загрозам у сучасному світі (ЄС, НАТО, Україна).

Ключові слова: гібридні загрози; гібридна агресія; гібридна війна; безпека; протидія; боротьба; пропаганда; кібербезпека; нові форми співпраці; інформаційна війна.

Постановка проблеми. Останніми роками світ зіштовхнувся з фактом повної деконструкції існуючого стану справ: переформатування системи міжнародних відносин, розбалансування системи міжнародної безпеки, активізація нових акторів, недієздатність системи міжнародного права і майже цілковита відсутність відповідальності за порушення міжнародних договорів і базових принципів міжнародного права.

Мета. Визначити основні підходи до розуміння гібридних загроз та окреслити зусилля міжнародної спільноти у протидії таким загрозам.

Основні результати дослідження. Виклики міжнародним відносинам, що виникли 2014 року, породили також нові явища і ситуації, які можна охарактеризувати як незрозумілі, непередбачувані та нестандартні. В медійному, а згодом і науковому середовищі вони отримали характеристику «гібридних». Зокрема про гібридний характер загроз міжнародній безпеці говорить Р. Сіле, наголошуючи, що саме 2014 рік позначив парадигму змін у світі, а українсько-московський конфлікт показав, що у Європу повернулося використання державними акторами військової сили та насильства заради досягнення політичних цілей [26, с. 2]. Автор також зазначає, що сформувався цілий спектр загрозливих тенденцій, серед яких він виокремлює: московську агресію у Східній Європі та мілітаризацію Арктики; на півдні – нестабільність на Близькому Сході та у Північній Африці; міграційну кризу; тенденцію до поширення ядерної зброї, розповсюдження зброї масового знищення, інфекційних захворювань, кібер-атак, міжнародного та національного тероризму, незаконний обіг наркотичних речовин, а також фінансову нестабільність.

Зважаючи на неймовірно широкий і різнорідних контекст виникнення загроз міжнародній безпеці, з’явилася тенденція до виокремлення поняття загроз

«гібридних». На думку В. Горбуліна, до перших сигналів виникнення гібридних загроз можемо зарахувати промову президента В. Путіна, в які він назвав розпад Совєтського Союзу найбільшою геополітичною катастрофою століття [8]. Саме вона стала рушійною силою політики ревізіонізму, який у сучасному світі реанімували через нетрадиційні засоби впливу, а також спроба самозахоплення острова-коси Тузла і конфлікт навколо нього, який вважають перевіркою реакції США та союзників (продовженням цієї перевірки були газові війни проти України (січень 2006, січень 2009) та війна у Грузії (8.08.08)) [19]. Як вважає Дж. Чемберс, гібридні загрози не є новими в історії війни, проте їхнє застосування РФ в Україні 2014 року, «Хезболлою» у війні з Ізраїлем 2006 року, а також публікації Доктрини Герасимова вивели це поняття на передову обговорення як військовими, так і науковцями [12].

Єдине визначення і трактування гібридної загрози сьогодні відсутнє. Автори М. Кофман та М. Роянскі вважають, що термін «гібридний» позначає комбінацію усіх попередньо визначених типів протистоянь, аналітичне осмислення якої є обмеженим [22].

Чи не вперше тривогу щодо гібридних загроз відобразили у Стратегічній концепції НАТО 2010 р. [9], інкорпорованій у базову концепцію НАТО. У ній гібридні загрози визначено як такі, що «створюються супротивниками, з можливістю одночасно застосовувати традиційні та нетрадиційні засоби, залежно від потреби для досягнення своїх цілей» [27].

У робочій доповіді Європейської служби зовнішньої дії (2015) зазначено, що гібридну війну / гібридну загрозу легше описати, аніж дати їй визначення: її можна охарактеризувати як централізоване і контрольоване застосування різноманітних відкритих і таємних тактик, які впроваджують військовими та невійськовими засобами, починаючи від інтелектуальних та кібер-операцій через економічний тиск до використання конвенційних сил. Агресор, використовуючи гібридні тактики, намагається підірвати та дестабілізувати опонента за допомогою як підривних, так і примусових засобів, зокрема різних форм саботажу, зривів комунікацій та інших послуг, включаючи постачання електроенергії, підтримку партизанських рухів, приховане вторгнення під виглядом «гуманітарної інтервенції». Важливим елементом є масові кампанії з дезінформації, призначені для формування і контролю думок. Все це зроблено з метою досягнення політичного впливу, навіть домінування над країною в підтримку загальної стратегії [13].

Наукова служба Європейського парламенту розглядає «гібридну загрозу» як метафору, що охоплює всі складнощі та дилеми, пов’язані зі зміною глобального світового порядку. У її доповіді наголошено, що часто термін «гібридна загроза» взаємозамінно вживають із поняттям «гібридна війна», відображаючи взаємопов’язану природу викликів (етнічний конфлікт, тероризм, міграція, слабкі інституції), різноманіття залучених акторів (регулярні, нерегулярні, кримінальні групи…), і широкий спектр традиційних та нетрадиційних засобів (військові, дипломатичні, технологічні) [27].

У Спільному рамковому документі Європейського парламенту і Ради (2016) гібридні загрози визначають як «поєднання примусової та підривної діяльності, традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть скоординовано використати держави чи недержавні суб'єкти для досягнення конкретних цілей, залишаючись на рівні нижче порогу формально оголошеної війни» [21].

На описовості концепту «гібридної загрози» акцентує також проект MCDC «Розуміння гібридної війни». У аналітичній доповіді станом на січень 2017 р. зазначено, що гібридна війна передбачає синхронне використання військових та невійськових засобів, спрямованих на найбільш вразливі місця супротивника. Інструментарій гібридної війни може розширюватися чи скорочуватися, залежно від потреби [15].

Значна частка підходів до осмислення природи «гібридних загроз» здійснюється через призму діяльності Російської Федерації, яка, на думку багатьох політиків і вчених, поклала початок явищу сучасної гібридної війни. Зокрема, у доповіді Європейського парламенту «Протидія гібридним загрозам: Співпраця ЄСНАТО» від березня 2017 р. чітко зазначено, що «поняття гібридної загрози наповнилося змістом відносно дій РФ в Україні та операцій ІДІЛ далеко за межами Сирії та Іраку» [14]. Отже, в ЄС Російську Федерацію, поряд із ІДІЛ, уже починають визначати як причину гібридних загроз.

У доктрині збройних сил США зазначено, що існуюча гібридна загроза побудована на діях Москви у Східній Європі, які створюють прецедент на майбутнє: вона використовує значну кількість гібридних способів і засобів проти слабкої або ослабленої держави (України), щоб примусити її підкорятися своїй волі. Традиційні гібридні загрози зосереджені на змішуванні різних можливостей на тактичному та операційному рівнях війни. Однак Російська Федерація сьогодні використовує не лише військовий інструментарій, а й економічні, інформаційні та дипломатичні засоби, конструюючи гібридну загрозу для подальшого загострення проблеми [17, с. 39–42].

Андіс Кудорс, виконавчий директор Центру Східноєвропейських політичних досліджень, даючи визначення гібридним загрозам, наголошує, що це інструмент, який офіційна Москва використовує для зміни існуючого світового устрою, нагадуючи про свої регіональні та глобальні амбіції, в такий спосіб здійснюючи значно більший політичний тиск на міжнародному рівні [20].

Україна у Концепції розвитку сектора безпеки і оборони України 2016 р. засвідчила, що сучасну гібридну загрозу для України створює «комбінація різноманітних і динамічних дій регулярних сил РФ, що взаємодіють зі злочинними озброєними угрупованнями та кримінальними елементами, діяльність яких координується і здійснюється за єдиним замислом і планом із активним застосуванням засобів пропаганди, саботажу, навмисного завдання шкоди, диверсій і терору» [4].

Підсумовуючим можна назвати визначення, яке запропонував М. Гончар, президент Центру глобалістики «Стратегія XXI»: «Гібридна – це така загроза, яка не ідентифікується як загроза. Троянський кінь – історичний приклад.

Енергетичний московсько-європейський проект Північний потік–2 – сучасний приклад такої загрози» [7].

Зрештою, відповідно до аналітичних матеріалів НАТО, на практиці будь-яка загроза може бути гібридною, якщо вона не обмежується однією формою і виміром ведення бойових дій. Коли будь-яку загрозу або застосування сили називають гібридними, цей термін втрачає своє значення і створює плутанину замість прояснення «реалій» сучасної війни [2].

Також в осмисленні гібридних загроз з'явилося поняття «гібридних акторів», які, на думку Р. Сіле, є небезпечнішими, оскільки не прив'язані до фізичного поля бою, а використовують кожну нагоду проникнути у всі сфери життя, включно зі ЗМІ [26, с. 3]. Як зазначає М. Саарелайнен, ті, хто використовує гібридні методи та заходи зазвичай слабкі держави або актори, які уникають відкрито оголошеної війни. Без гібридної діяльності вони б не змогли реалізовувати свої інтереси [24].

Станом на 2015 рік аналітичні структури ЄС виокремлювали такі види і сфери виникнення гібридних загроз як тероризм, кібербезпека, організована злочинність, морські суперечки, космос, дефіцит ресурсів та приховані операції [27].

Натомість міністр із питань тимчасово окупованих територій і внутрішньо переміщених осіб України В. Черниш до головних «гібридних загроз» зачислює: агентурні мережі і політичні рухи, які залежать від Москви; вплив Російської Федерації на український ринок; підтримку антиукраїнських рухів; спекуляцію та маніпуляцію історією; юридичні війни (позови, заперечення проти них, створення доказової бази на майбутнє); розгойдування міжнаціональних конфліктів (обстріли консульств, руйнування пам'ятників). Він наголошує на створенні гібридних загроз як в Україні, так і в Європі: «на Заході Москва займається руйнуванням спілок на підтримку України, всередині країни намагається створити протистояння» [1].

Зазначимо, що загальноєвропейський та український підходи у визначенні гібридних загроз значно відрізняються, оскільки, на думку керівника міжнародних програм Центру глобалістики «Стратегія XXI» В. Мартинюка, ЄС все ще обережно підходять до визначення Російської Федерації як агресора та джерела гібридних загроз. В Україні акцент роблять на сфери застосування засобів гібридної війни, а в ЄС класифікують сфери, уразливі до таких загроз [5].

Європейські документи вказують, що основною характеристикою гібридних атак вважається те, що вони створені для експлуатації слабкостей держави. Зокрема, щодо України 2015 р. аналітики ЄС звертали увагу на слабке урядування та неефективні національні інститути, корупцію, брак довіри та підтримки безпековим та оборонним структурам від населення, присутність значного відсотка російськомовного населення і критичний рівень залежності від Російського імпорту та постачання енергоносіїв [13]. Натомість В. Горбулін наголошує, що досвід України у гібридній війні підказує, що найважливіше зрозуміти те, що такі війни починаються задовго до того, як пролунають перші

постріли. На початковій стадії важко розпізнати і зрозуміти її ознаки: коли свобода слова перетворюється на агресивну пропаганду, коли протести в країні інспіровані зовнішніми силами, коли агресор використовує абсолютно демократичні інструменти, щоби втручатися у внутрішні справи суверенної держави, щоб заблокувати діяльність міжнародних організацій, націлених на запобігання або розв'язання конфліктів і так далі [3].

Західні країни поступово усвідомлюють масштаб уражень гібридними загрозами та важливість протистояти таким загрозам. Як наголошував ще на початках російської агресії в Україні Дж. Іслам, президент Vidder, каліфорнійської компанії, що спеціалізується на безпеці, «те, з чим зараз стикається Україна – це провісник подій у США, а також у країнах їхніх союзників» [6]. Зрештою, і Європа, і США 2017 року на собі відчули тиск гібридних загроз, які значно дестабілізували як внутрішню, так і зовнішньополітичну ситуацію.

Як визначено у стратегічному безпековому аналізі Женевського центру безпекової політики, гібридна війна/гібридні загрози спеціально розмивають межу поміж війною та миром, в результаті постраждалим від гібридної агресії країнам важко знайти політичну відповідь, яка була б і вдалою, і вчасною. Багатоскладова гібридна загроза вимагає залучення усіх прошарків суспільства в оборонні заходи. Міжурядових та міжвідомчих зусиль вже недостатньо [11].

У квітні 2016 року Європейська комісія прийняла Спільну стратегію боротьби із гібридними загрозами, у якій перебачено 22 оперативні дії для підвищення рівня інформованості про гібридні виклики, підвищення стійкості стратегічних секторів, реагування на кризу та відновлення системи. Також у рамках цієї Стратегії створено аналітичну структуру під назвою Hybrid Fusion Cell, яка формуватиме єдину базу для аналізу гібридних загроз [21].

У Фінляндії у вересні 2017р. відкрився Європейський центр із протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats), ініціаторами створення та засновниками якого виступили США, Велика Британія, Франція, Німеччина, Швеція, Польща, Фінляндія, Латвія та Литва. Відкриваючи цей Центр, міністр закордонних справ Фінляндії Тімо Сойні зазначив: «Вразливості до гібридних загроз не обмежуються лише національними кордонами. Ми вважаємо, що гібридні загрози потребують узгодженої реакції також на рівні ЄС та НАТО. Співпраця на основі отриманих уроків та обміну знаннями сприятиме узгодженню національної політики, доктрин та концепцій» [23].

До завдань Центру належать:

- налагодження на стратегічному рівні діалогу та консультацій поміж учасниками центру, ЄС та НАТО;
- проведення досліджень та аналізу гібридних загроз та методів протидії таким загрозам;
- розробка доктрини, проведення тренувань, спрямованих на посилення індивідуальних та спільних можливостей протистояти гібридним загрозам;

- залучення до діалогу урядових та неурядових експертів та професіоналів із різних сфер;
- залучення і співпраця з групами за інтересами, фокусуючись на специфічній діяльності, що можуть позиціонувати гібридну загрозу [18].

Створенню цього центру передувало заснування центрів досконалості НАТО (NATO Center of Excellence) в країнах Балтії, що стало значним кроком до запобігання невійськових ризиків: Центр кібернетичного захисту в Естонії, Центр енергетичної безпеки в Литві та Центр стратегічних комунікацій в Латвії вже посилюють безпеку всіх держав-членів НАТО. У листопаді 2017 р. у Фінляндії при міністерстві закордонних справ запроваджено позицію посла із питань гібридних загроз, як додаткову до посади посла із кібербезпеки, заснованої ще 2014 р.

Водночас у ЄС постало питання про активізацію військової співпраці. Отож 13 листопада 2017 р. міністри закордонних справ та міністри оборони 23-х держав підписали лист про своє приєднання до PESCO – Програми постійної структурованої співпраці, яка передбачає створення нових оборонних можливостей і проведення спільних операцій, а також створення своєрідної «шенгенської зони» для військових.

Створюючи відповідальні структури, надзвичайно важливо осмислити шляхи і способи протидії гібридним загрозам, зокрема створюючи можливості їхньої нейтралізації. У рамках комплексного підходу ЄС у сфері безпеки та оборони Спільна рамкова програма визначила низку заходів, спрямованих на запобігання, подолання та пом'якшення зростаючої проблеми гібридних загроз, а саме: покращення обізнаності про загрози, забезпечення стійкості структур, захист європейців у мережі Інтернет, посилення співробітництва з третіми країнами, розробка операційного протоколу ЄС для запобігання та реагування на кризи, а також інтенсифікація співпраці ЄС та НАТО [25]. Віце-президент Європейської комісії Ю. Катаінен наголосив, що гібридні загрози не стримуються внутрішніми чи зовнішніми кордонами, тому держави-члени ЄС можуть зіштовхнутися із загальними загрозами, що спрямовані на транскордонні мережі або інфраструктуру. Відповідь на такі виклики не може бути ефективною, якщо вона не є послідовною та спільною [28].

Натомість майор Збройних сил США Дж. Девіс виокремлює потребу розвитку гібридного мислення, яке мало б зосереджуватися на взаємодії чотирьох психічних характеристик: розумінні стратегічного контексту, цілісному підході до операцій, зосередженні уваги на потенційних можливостях та охопленні природної складності операційного середовища [16]. Співзвучний з ним і державний секретар Міністерства інформаційної політики України Артем Біденко, який наголошує, що специфіка будь-якої гібридної війни полягає в тому, що перемогти в ній, відповідаючи симетричними методами, майже неможливо. «Суть гібридної війни в тому, що ворог постійно випереджає і постійно використовує свої ресурси на тих фронтах і ділянках, де його не чекають, або не мають можливості відповісти» [10]. Український досвід засвідчує, що гібридні загрози найактивніше проявляються у попередньо

створеній паралельній реальності. Отож, як зазначає Є. Бистрицький, виконавчий директор Міжнародного фонду «Відродження», відповіддю у цій війні має бути на рівні з високоорганізованою військовою відсіччю руйнація фіктивної реальності [7].

Висновки. Осмислюючи останні події протягом кількох років, можна дійти висновку, що світ виявився неготовим протистояти реаліям, які позначають як гібридні загрози міжнародній безпеці. На перший план виходить проблема усвідомлення природи загрози та її джерела, і на сьогодні провідні think-tanks лише на початку шляху. Досвід України у протистоянні російській агресії тривалий час взагалі не розглядали. Окрім того, дії Російської Федерації (зокрема, щодо України) не позиціонувалися як такі, що продукують новітній вимір загроз.

Хоча протиправні дії Москви – анексія Криму, окупація Донбасу – сьогодні розцінюють як гібридну війну і гібридну загрозу міжнародній безпеці, проте, на жаль, Україну й досі не долучили до європейської системи пошуку засобів протидії гібридним загрозам (проект ЄС із оцінки ризику гібридної загрози реалізується в Молдові, а не в Україні, яка безпосередньо протидіє таким загрозам зі Сходу) [5].

Значні відмінності мають підходи Заходу та України щодо усвідомлення гібридних загроз у країнах, що позначається, передусім, на шляхах протидії: ЄС акцентує увагу на кібер-безпеці, протидії організованій злочинності, нейтралізації ризиків, посиленні стійкості суспільства, інформаційній безпеці. Україна ж акцентує на природі конкретних атак, вимірах і природі гібридних загроз, які непомітно атакують і захоплюють національний, культурний, освітній та інформаційний простори, від чого рівень створюваної ними небезпеки збільшується в рази, а протидіяти їй значно важче.

Водночас залишаються без відповіді питання, чи «гібридні загрози» – це явище, спрямоване лише проти країн ліберально-демократичного світу, і наскільки ліберальні демократії здатні протистояти гібридним загрозам, породженим недемократичним світом, та наскільки реальна така ж сама гібридна стратегія проти країн, які розпочали гібридну війну? Необхідно визначити, чи гібридна війна/гібридна агресія/гібридні загрози негативні явища світового масштабу, чи вони передусім спрямовані проти локальних противників, наскільки прогресуючою буде «гібридність загроз» і які заходи протидії будуть найефективнішими?

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Війна на всіх фронтах: у Кабміні назвали головні «гібридні загрози» Росії [Електронний ресурс]. – 04 серпня 2017. – Режим доступу : https://www.obozrevatel.com/ukr/politics/vijna-na-vsih-frontah-u-kabmini-nazvali-golovni-gibridni-zagrozi-rosii.htm.

2. Гібридна війна – чи вона взагалі існує? [Електронний ресурс]. – Режим доступу : https://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/UK/index.htm.

3. *Горбулін В.* Російська гібридна війна змінює світоустрій [Електронний ресурс] / В. Горбулін. – Режим доступу : https://zbruc.eu/node/63861.

4. Концепція розвитку сектору безпеки та оборони України [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/92/2016.

5. *Мартинюк В.* ЄС у протидії гібридним загрозам та Україна: нечіткість у підходах [Електронний ресурс] / В. Мартинюк // Дзеркало тижня. – Режим доступу : https://dt.ua/internal/yes-u-protidiyi-gibridnim-zagrozam-ta-ukrayina-nechitkist-u-pidhodah-253570_.html.

6. *Петерсон Н.* Гібридна війна. Що Росія тестує на Україні [Електронний ресурс] / Н. Петрсон. – Режим доступу : http://nv.ua/ukr/opinion/peterson/gibridna-vijna-shcho-rosija-testuje-na-ukrajini-2129865.html.

7. Протидія гібридним загрозам в Україні [Електронний ресурс]. – Режим доступу : http://www.irf.ua/allevents/news/protidiya_gibridnim_zagrozam_v_ukraini/.

8. Путин: Распад СССР – крупнейшая геополитическая катастрофа века [Электронный ресурс]. – Режим доступа : https://www.youtube.com/watch?v=d4Xlwd91IlY&t=5s.

9. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору прийнята главами держав та урядів у Лісабоні 19 листопада 2010 року [Електронний ресурс]. – Режим доступу : https://www.nato.int/natostaticfl2014/assets/pdf/pdfpublications/20120214_strategic-concept-2010-ukr.pdf.

10. Що таке гібридна війна та гібридні загрози і як їм протидіяти [Електронний ресурс]. – Режим доступу : http://www.polradio.pl/5/39/Artykul/333519.

11. *Cederberg A.* How can Societies Be Defended against Hybrid Threats? [Electronic resource] / A. Cederberg, P. Eronen // STRATEGIC SECURITY ANALYSIS SEPTEMBER, 2015. – No 9. – Access mode : http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf.

12. *Chambers J.* Countering gray-zone hybrid threats. Analysis of Russia's 'New Generation Warfare' and Implications for the US Army [Electronic resource] / J. Chambers. – October 18, 2016. – Access mode : https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

13. Countering Hybrid Threats. Food-for-thought paper. Working document of the European External Action Service of 13/05/2015 [Electronic resource]. – Access mode : http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.

14. Countering hybrid threats: EU-NATO cooperation [Electronic resource]. – March, 2017. – Access mode : http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf.

15. Countering Hybrid Warfare Project: Understanding Hybrid Warfare a Multinational Capability Development Campaign project [Electronic resource]. – Access mode : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

16. *Davis J.R. Jr.* Continued evolution of hybrid threats. The Russian Hybrid Threat Construct and the Need for Innovation [Electronic resource] / J.R. Davis. – Access mode : http://www.ileridunya.com/wp-content/uploads/2016/02/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf.

17. Doctrine for the Armed Forces of the United States // Department of Defense, Joint Publication (JP) 1, Washington D.C. : Department of Defense, 2013. – P. 39–42.

18. European Centre of Excellence [Electronic resource]. – Access mode : https://www.hybridcoe.fi/about-us/.

19. *Horbulin. V.* How Russia has prepared for aggression against Ukraine for 10 years. Instruments of Hybrid war: diplomacy, media, culture, religion [Electronic resource] / V. Horbulin. – Access mode : http://uaposition.com/analysis-opinion/russia-prepared-aggression-ukraine-10-years-instruments-hybrid-war-diplomacy-media-culture/.

20. Hybrid War – A New Security Challenge for Europe [Electronic resource]. – Access mode : http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf.

21. Joint communication to the European Parliament and the Council. Joint framework on countering hybrid threats. A European Union response 2016 [Electronic resource]. – Access mode : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

22. *Kofman M.* A Closer Look at Russia's 'Hybrid War [Electronic resource] / M. Kofman, M. Rojansky // Kennan Cable (Kennan Institute at the Woodrow Wilson Center, April 2015). – № 7,

April 2015. – Access mode : https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

23. Minister for Foreign Affairs of Finland Mr Timo Soini at the signing of the Memorandum of Understanding establishing the European Centre of Excellence for Countering Hybrid Threats, Helsinki 11 April 2017 [Electronic resource]. – Access mode : http://vnk.fi/documents/10616/3934867/Soini+on+hybrid+threats+11+April+clean+UMIK.pdf.

24. *Saarelainen M.* Hybrid Threats – What Are We Talking About? [Electronic resource] / M. Saarelainen. – Access mode : https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/.

25. Security and defense: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead European Commission [Electronic resource]. – Press release, Brussels, 19 July 2017. – Access mode : http://europa.eu/rapid/press-release_IP-17-2064_en.htm.

26. *Thiele R. D.* Hybrid Threats – And how to counter them [Electronic resource] / R. D Thiele // ISPSW Strategy Series: Focus on Defense and International Security. – Issue No. 448, Sep 2016. – S. 2. – Access mode : http://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf.

27. Understanding hybrid threats. Briefing European parliamentary research service [Electronic resource]. – June, 2015. – Access mode : http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.

28. Vice-President Katainen's Speech at the High Level Conference on Hybrid Threats [Electronic resource]. – Brussels, 2 October 2017. – Access mode : https://ec.europa.eu/commission/commissioners/2014-2019/katainen/announcements/vice-president-katainens-speech-high-level-conference-hybrid-threats-brussels-2-october-2017_en.

Стаття надійшла до редколегії 10.03.2017
Прийнята до друку 10.05.2017

HYBRID THREATS TO INTERNATIONAL SECURITY AND THE WAYS OF COUNTERING

Sofiya Fedyna

Ivan Franko National University of Lviv,
1, Universytetska Str., Lviv, Ukraine, 79000, tel. (032) 239-4132, (050) 9897440,
e-mail: ukrainesinger@yahoo.com

In this article the author analyses the approaches to understanding of «hybrid threat» notion as of new phenomenon in international relations, outlines peculiarities of its occurrence and influence on international processes, examines the existing approaches to countering hybrid threats in the modern world (the EU, NATO, Ukraine).

In recent years, the world has faced the complete deconstruction of the current state of affairs: reformatting the system of international relations, imbalance of the international security system, activation of new actors, inability of the system of international law and almost total lack of responsibility for violations of international treaties and basic principles of international law.

Challenges to international relations that arose in 2014 also created new phenomena and situations that could be described as unclear, unpredictable and non-standard. In the media, and subsequently in the scientific environment, they received the characteristics «hybrid».

The concept of a hybrid threat at the present stage does not have a single definition, so the approaches to its interpretation range from the abstract application of traditional and non-traditional means, depending on the need to achieve their goals, to the tool that official Moscow uses to change the existing world order, reminding of its regional and global ambitions.

The complexity of the question is also that the European and Ukrainian (since Ukraine itself was the bridgehead for Moscow Federation hybrid warfare) approaches to the interpretation of hybrid threats and, accordingly, the search for approaches to counteract are significantly different. The EU focuses on cyber-security, counteraction to organized crime, risk neutralization, increased resilience of society, and

information security. Ukraine emphasizes the nature of the specific attacks, dimensions and nature of hybrid threats that quietly attack and capture national, cultural, educational and informational spaces, from which the level of danger created by them increases at times, and it is much more difficult to counteract it.

Key words: hybrid threats; hybrid aggression; hybrid warfare; security; counteraction; fight; propaganda; cybersecurity; new forms of cooperation; information warfare.