УДК 342.9:343:3

Ірина Миколаївна Сопілко,
декан юридичного факультету
Національного авіаційного університету,
доктор юридичних наук, професор
ORCID: 0000-0002-9594-9280

РОЗУМІННЯ ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ: ПРАВОВИЙ АСПЕКТ

Постановка проблеми. Як відомо, 24 лютого 2022 року РФ почала активні бойові дії проти нашої держави, але реальну гібридну війну було розпочато країною-агресором ще вісім років тому. Тоді, у 2014 році, російські солдати без будь-яких знаків відмінності (так звані зелені чоловічки) віроломно захопили та окупували Кримський півострів, а також разом із найманцями розпочали наступ на схід України. Ворогом були використані різноманітні методики та інструменти ведення гібридного протистояння – економічні та дипломатичні засоби, психологічні, інформаційні та кібернетичні підривні активності. І сьогодні важливо розуміти, що таке гібридна війна за своєю сутністю, а також знати, як надати їй гідний опір, особливо на правовому рівні. І хоча концепція гібридної війни не нова, особливого значення та актуальності вона набула саме в останню декаду у зв'язку із використанням нетрадиційних методик ведення війни, залученням недержавних суб'єктів та активним впровадженням інформаційних технологій з метою підпорядкувати собі інших суб'єктів, не використовуючи прямий збройний конфлікт. Як мета гібридної війни РФ, наша держава є унікальним прикладом незламності, сміливості та сили, які Україна демонструє ще з моменту здобуття незалежності, але особливо яскраво – з 2014 року.

Аналіз останніх досліджень і публікацій. Концепт «гібридна війна» є предметом дослідження деяких вітчизняних і зарубіжних дослідників, а саме: Ю. Даника, Т. Малярчук, Ф. Хоффмана, Дж. К. Візера, Ч. Бріггса, Дж. А. Пеллеріти, Х. Дж. Салліван та ін. Автором цього дослідження, з урахуванням значення наукового доробку згаданих дослідників та інших вчених, буде зроблено переосмислення концепту «гібридна війна» задля вдосконалення такого поняття і його суті, а також визначення перспектив подальшого його розвитку в науковому напрямі.

Мета статті. Метою цієї статті є вдосконалення сутності концепту «гібридна війна» на основі аналізу провідних юридичних джерел та пошук дієвих правових механізмів протидії повномасштабній агресії РФ.

Основні результати дослідження. Ф. Хоффман у своїй роботі за 2007 рік узвичаїв поняття «гібридна війна» [1], але чи знав він тоді, що Україна дізнається значення цього терміна і відчує його на собі повною мірою? Це нам не відомо, зате введене ним поняття чітко і точно відображає те, з чим стикається наша країна вже понад вісім років.

Існує кілька підходів до визначення феномену гібридної війни. Так, Дж. К. Уізер під ним розуміє війни XXI століття, у яких беруть участь безліч суб'єктів, а традиційні відмінності між типами збройних конфліктів стираються. Як зазначає вчений, всі види ворожої діяльності РФ слід називати гібридними; до них, окрім іншого, він відносить таємне використання сил спецназу, акти економічного примусу та маніпуляції під час державних виборів в Україні [2].

Цікавим є і підхід, запропонований Е. Бро. Дослідниця використовує термін «агресія у сірій зоні», тобто ведення ворожих дій поза збройним конфліктом з метою ослабити суперника (яким може бути інша держава, формування чи альянс). Якщо до такого додати реальні бойові дії, то все разом і стане гібридною війною. Е. Бро впевнена, що практично кожну сучасну війну можна вважати гібридною, оскільки вона зачіпає як військові, так і невійськові виміри, наприклад, кібернетичний простір, а також використовує пропаганду. Але саме аспект сірої зони стає дедалі помітнішим, адже за сучасних умов сіяти хаос легше у зв'язку із меншим ризиком настання відплати. Як приклад такого дослідниця наводить кібератаку, призвідника якої зазвичай важко встановити остаточно [3].

Як зазначають Ю. Даник та інші, важливим під час гібридної війни є вплив дій агресора, що посилює внутрішню нестабільність у різних сферах, у т. ч. провокування недовіри до державних інститутів та загальноприйнятих цінностей, змішання ідеологічних та інших факторів, підрив економічної стабільності та розвитку. Дослідники вказують також на відмінність аналізованого типу війни від традиційних, що проявляється в особливостях стратегії її розв'язування та засобах ведення. Гібридна війна, як і війна нерегулярна, зазвичай передбачає використання нерегулярних чи невійськових сил або тих, що всіляко приховують свою національну належність. У ході таких операцій також задіяні диверсійно-розвідувальні групи (ДРГ) та спецпідрозділи. Нерідко до зазначеного додається проведення спеціальних інформаційних або пов'язаних із кібернетичним простором дій, і в ході таких руйнуються або зазнають суттєвої шкоди критично важливі вузли; і таких «результатів» ворог не міг би досягти за допомогою традиційних військових засобів [4].

А. Білал також зазначає, що гібридна війна передбачає симбіоз традиційних і нетрадиційних інструментів сили та ведення підривної діяльності, які об'єднуються на основі певної синхронізації з метою досягти синергетичних ефектів за допомогою тиску на вразливість супротивника. Використання кінетичних і некінетичних методик, у його розумінні, допомагає завдати шкоди найбільш оптимальним для ворога чином. Крім того, гібридну війну відрізняють такі характеристики:

– стирання межі між війною та мирним станом, тобто визначити поріг війни складно. Таким чином, відсутність прямого видимого насильства показує себе противнику більш вигідною, при цьому таке є і менш ризикованом та витратним, ніж кінетичні операції. Мається на увазі те, що, наприклад, ввести танки на територію чужої держави буде витратніше і, напевно, буде засуджуватися світовою громадськістю, тоді як спонсорування і поширення фейків спричиняє мінімальні витрати і ризики, але цілком реальні збитки;

– наявність двозначності та атрибуції. Гібридні військові активності зазвичай характеризуються високим ступенем невизначеності, що створюється навмисно, тим самим ускладнюючи атрибуцію і реакцію. Таким чином, держава-жертва або взагалі не може виявити гібридну атаку, або не може співвіднести її із державою-агресором. Відповідно, постраждалій країні буде складно розробити стратегію і політики у відповідь [5].

Найбільш точно гібридну війну визначили як військову стратегію, що використовує політичну війну у поєднанні із війною «ковенційною», тобто звичайною в загальноприйнятому розумінні, іррегулярною війною і кібернетичною та іншими методами впливу, наприклад, такими як засилля фейкових новин, спеціальні дипломатичні активності, використання правових інструментів і втручання у державні вибори з боку іноземних агентів [6]. Ця концепція здобула не тільки схвалення, а й критику через свою розпливчастість і ймовірні історичні спотворення, але все ж таки саме вона буде взята за основу в цьому науковому дослідженні.

Згадана нерегулярна війна як один із елементів гібридного протистояння, відповідно до спільної доктрини США, це «жорстока боротьба між державними та недержавними суб'єктами за легітимність та вплив на відповідні групи населення». Зазвичай у ході такої використовується широкий спектр військових та інших методик, інструментів для того, щоб подолати волю супротивника, підірвати його силу, мінімізувати вплив [7].

Також часто, особливо з розвитком інформаційних технологій і зростанням ролі Інтернет-мережі, гібридна війна супроводжується проявами кібервійни. І тут безпосередні дії проти жертви ворог веде у кіберпросторі. Найчастіше на слуху у українців DDoS-атаки як один із інструментів ведення такої війни. Кібербезпека держави не менш важлива, ніж фізична безпека її кордонів, відповідно, важливо підтримувати її на високому рівні. Так, згідно із В. Філінович для цього необхідно здійснювати дії по управлінню ризиками в кібернетичному домені, для чого потрібна участь як окремих організацій, так і цілих урядів; необхідність зазначеного полягає у забезпеченні цілісності, конфіденційності, доступності даних та інших інформаційних активів у кіберпросторі [8, с. 39].

Таким чином, концепт гібридної війни все ще залишається спірним, відповідно, не існує єдиного уніфікованого її визначення. Але загальне розуміння даного феномену дає нам уявлення про сучасні та майбутні проблеми державної безпеки.

За останні вісім років, протягом яких РФ веде проти нас гібридну війну, Україна серйозно досягла успіху в протидії такій агресії. Були задіяні не лише військово-розвідувальні сили та методики, а й економічні, соціальні, правові. І саме останні вимагають особливо пильної уваги.

Так, у листі МОН України № 1/9-79 «Про використання в загальноосвітніх навчальних закладах методичних рекомендацій» від 16.02.2016 містяться Методичні рекомендації для проведення в загальноосвітніх навчальних закладах заходів до Дня початку кримського спротиву. У цьому акті, зокрема, дано визначення гібридної війни як такої, що поєднує в собі «принципово різні типи та способи ведення військових дій, які скоординовано застосовуються для досягнення спільних цілей». При цьому названі такі її типові компоненти, а саме: класичні прийоми ведення війни, тобто з використанням військової сили та відповідної техніки, нерегулярні збройні формування та інші прийоми на кшталт кібернетичної війни. Важливе уточнення: в такій ситуації цілком здатна зберігатись публічна непричетність до конфлікту сторони-агресора [9].

У світлі повномасштабного наступу РФ на Україну, розпочатого 24 лютого 2022 року, український нормативно-правовий масив суттєво поповнився. Так, варто згадати рішення РНБО «Про реалізацію єдиної інформаційної політики в умовах військового стану», яке ввів у дію своїм Указом від 19 березня 2022 року Президент Зеленський. Як зазначено в документі, з урахуванням активного поширення країною-агресоркою дезінформації та з метою донесення правди про реальність війни саме реалізацію єдиної інформаційної політики слід вважати пріоритетним питанням національної безпеки. Забезпечити таке допоможе об'єднання всіх загальнонаціональних телеканалів інформаційного та інформаційно-аналітичного спрямування у єдину інформаційну платформу стратегічної комунікації [10]. Це було реалізовано у вигляді цілодобового інформаційного марафону під назвою «Єдині новини #UAразом».

Також президентськими указами № 363/2022 та № 362/2022 від 24 травня 2022 року було введено в дію рішення РНБО «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». З посиланням на ст. 5 Закону України «Про санкції» РНБО підтримала пропозиції Кабінету Міністрів та СБУ щодо застосування персональних спеціальних економічних та інших обмежувальних заходів. Реалізувати та стежити за виконанням зазначеного КМУ допоможе СБУ та Нацбанк, а українське МЗС інформуватиме про відповідні санкції компетентні органи ЄС, США та інших країн [11; 12].

Також протягом останніх восьми років велася активна законотворча діяльність із метою протидії гібридній війні. Тією чи іншою мірою це питання було порушено у таких нормативно-правових актах, як: Закон України № 75/98-ВР «Про Концепцію Національної програми інформатизації» (від 04.02. 2019), Закон України № 2469-VIII «Про національну безпеку України» (від 21.06.2018), Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017), рішення РНБО «Про Доктрину інформаційної безпеки України» (від 29.12.2016) та ін. Окремо вкажемо на зазначене рішення РНБО, яке введено в дію президентським Указом № 47 від 25.02.2017 року, що визначило повноваження відповідних органів захисту суспільних інтересів в інформаційній сфері та окремо в національному інформаційному просторі. Тут також уточнюються основи здійснення та формування держполітики в інформаційному полі, головна роль у чому відведена протидії деструктивному російському інформаційному впливу [13].

Не меншу важливість має і рішення РНБО «Про Стратегію інформаційної безпеки», введене в дію Указом № 685 В. Зеленського у грудні минулого року. В акті визначено поточні виклики та загрози національній безпеці нашої країни в інформаційному середовищі, названі завдання та цілі протидії таким загрозам. Як сказано в документі, його мета полягає в посиленні можливостей забезпечення інформаційної безпеки української держави та її інформаційного простору, відповідно, в такому разі будуть рівно захищені державний суверенітет, територіальна цілісність країни, її демократичний конституційний устрій, а також забезпечуватимуться дотримання прав і свобод українців [14].

Таким чином, Україна активно протистоїть російській військовій агресії, зокрема, і на правовому рівні. Зрозуміло, багато що ще тільки належить зробити, але і вже наявне правове регулювання відрізняється якісністю та своєчасністю.

Висновки. Отже, Україна веде активну правотворчу та правозастосовну діяльність у боротьбі із російською повномасштабним вторгненням. Видаються укази та постанови, розробляється більш сучасне та адекватне законодавство. Крім зазначеного, важливо і реформування у сферах безпеки та оборони, а також у сфері протидії корупції, щоб у ворога не було жодного шансу «натиснути» на нас.

Не менш важливим є підтримання балансу між безпекою та забезпеченням загальноприйнятих демократичних свобод, що часом буває дуже ускладненим. Як приклад можна згадати блокування російських вебресурсів Яндекс і ВКонтакте, зроблене з метою недопущення поширення дезінформації. Але водночас ця подія викликала шквал критики у зв'язку із можливим обмеженням свободи слова. Зрозуміло, що протидія активностям країни-агресора – дуже складна справа, але важливо розуміти, що будь-яка недоробка чи помилка української влади не просто завдасть шкоди нам, а й дасть додаткові очки ворогові.

І на завершення окремо відзначимо наше незламне громадянське суспільство. Росія не змогла передбачити, як український народ об'єднається і виступить єдиною силою проти країни-окупанта. Таким чином, можна сміливо говорити, що Україна дуже успішно рухається до перемоги у розгорнутій проти неї гібридній війні.

Список використаних джерел

1. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies, 2007. 72 p.
2. Wither J. K. Defining Hybrid Warfare, per Concordiam. *Journal of European Security Defense* Issues 10, No. 1, 2020. P. 7–9.
3. What is hybrid war, and is Russia waging it in Ukraine? URL: https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine
4. Danyk Y., Maliarchuk T., Briggs C. Hybrid War: High-tech, Information and Cyber Conflicts. Connections: *The Quarterly Journal* 16, no. 2, 2017. P. 5–24.
5. Bilal A. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html
6. Aitoro J. R. Defense lacks doctrine to guide it through cyberwarfare. URL: http://www.nextgov.com/nextgov/ng_20100913_7634.php?oref=topnews
7. The Insufficiency of U. S. Irregular Warfare Doctrine. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-93/jfq-93_104_110_Pelleriti-et-al.pdf
8. Філінович В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. 3(60). С. 38–44.
9. Про використання у загальноосвітніх навчальних закладах методичних рекомендацій МОН України; Лист, Рекомендації від 16.02.2016 № 1/9-79. URL: https://zakon.rada.gov.ua/rada/show/v9-79729-16#Text
10. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5295.html
11. Про рішення Ради національної безпеки і оборони України від 24 травня 2022 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 24 травня 2022 року № 362/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5499.html
12. Про рішення Ради національної безпеки і оборони України від 24 травня 2022 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 24 травня 2022 року № 363/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5500.html
13. Про Доктрину інформаційної безпеки України: Рішення РНБО від 29.12.2016 № n0016525-16. URL: https://zakon.rada.gov.ua/laws/show/n0016525-16#n2 (дата перегляду: 14.03.2022)
14. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України; Стратегія від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата перегляду: 14.03.2022)

References

1. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies, 2007, 72 p.

2. Wither J. K. Defining Hybrid Warfare, per Concordiam. *Journal of European Security Defense* Issues 10, No. 1, 2020. P. 7–9.
3. What is hybrid war, and is Russia waging it in Ukraine? URL: https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine
4. Danyk Y., Maliarchuk T., Briggs C. Hybrid War: High-tech, Information and Cyber Conflicts. Connections: *The Quarterly Journal* 16, no. 2, 2017. P. 5–24.
5. Bilal A. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html
6. Aitoro J. R. Defense lacks doctrine to guide it through cyberwarfare. URL: http://www.nextgov.com/nextgov/ng_20100913_7634.php?oref=topnews
7. The Insufficiency of U. S. Irregular Warfare Doctrine. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-93/jfq-93_104_110_Pelleriti-et-al.pdf
8. Filinovych, V. Kiberbezpeka ta zahrozy aviatsiinii sferi: pravovyi aspekt. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia:* Yurydychnyi visnyk «Povitriane i kosmichne pravo», 2021, 3(60). S. 38–44.
9. Pro vykorystannia u zahalnoosvitnikh navchalnykh zakladakh metodychnykh rekomendatsii MON Ukrainy; Lyst, Rekomendatsii vid 16.02.2016 № 1/9-79. URL: https://zakon.rada.gov.ua/rada/show/v9-79729-16#Text
10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 bereznia 2022 roku «Shchodo realizatsii yedynoi informatsiinoi polityky v umovakh voiennoho stanu»: Ukaz Prezydenta Ukrainy vid 19 bereznia 2022 roku № 152/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5295.html
11. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 24 travnia 2022 roku «Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii)»: Ukaz Prezydenta Ukrainy vid 24 travnia 2022 roku № 362/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5499.html
12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 24 travnia 2022 roku «Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii)»: Ukaz Prezydenta Ukrainy vid 24 travnia 2022 roku № 363/2022. URL: https://www.rnbo.gov.ua/ua/Ukazy/5500.html
13. Pro Doktrynu informatsiinoi bezpeky Ukrainy: Rishennia RNBO vid 29.12.2016 № n0016525-16. URL: https://zakon.rada.gov.ua/laws/show/n0016525-16#n2 (data perehliadu: 14.03.2022)
14. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky": Ukaz Prezydenta Ukrainy; Stratehiia vid 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (data perehliadu: 14.03.2022)

Сопілко І. М. Розуміння гібридної війни проти України: правовий аспект

Стаття присвячена дослідженню поняття «гібридна війна» з урахуванням новітніх досліджень в юридичній науці. Детально досліджено сутність і характеристики гібридної війни, яку проводить РФ проти України з 2014 року. Надано визначення гібридної війни, іррегулярної війни, кібервійни та пов'язаних з ними правових категорій. Важливість визначення концепту гібридної війни пояснюється необхідністю на його основі формулювання уявлення про сучасні та майбутні проблеми державної безпеки України. За основу в статті взяте розуміння гібридної війни як військової стратегії, що використовує політичну війну у поєднанні із війною «конвенційною», тобто звичайною в загальноприйнятому розумінні, іррегулярною війною і кібернетичною та іншими методами впливу, наприклад, такими як засилля фейкових новин, спеціальні дипломатичні активності, використання правових інструментів і втручання у державні вибори з боку іноземних агентів. Проаналізовано основні національні нормативно-правові джерела, які містять норми щодо протидії гібридній війні. Надані авторські рекомендації щодо методів боротьби із агресією РФ у правовому полі.

Ключові слова: гібридна війна, інформаційна війна, інноваційна війна, кібервійна, російське вторгнення в Україну.

Sopilko I. M. Comprehending the hybrid war against Ukraine: the legal aspect

The article is devoted to the study of the concept of "hybrid war" taking into account the latest research in legal science. On February 24, 2022, the Russian Federation began active hostilities against our state, but the real hybrid war was started by the aggressor country 8 years ago. Then, in 2014, Russian soldiers without any insignia (the so-called "little green men") treacherously seized and occupied the Crimean peninsula, and, together with hired soldiers, launched an offensive into eastern Ukraine. The enemy used various methods and tools for conducting a hybrid confrontation – economic and diplomatic means, psychological, informational, and cybernetic subversive activities. And today it is important to understand what a hybrid war is in its essence, as well as to know how to put up worthy resistance to it, especially at the legal level. And although the concept of hybrid warfare is not new, it has gained particular importance and relevance precisely in the last decade due to the use of non-traditional

warfare methods, the involvement of non-state actors, and the active introduction of information technologies to subjugate other actors without using direct armed conflict. As the target of the hybrid war of the Russian Federation, our state is a unique example of the invincibility, courage, and strength that Ukraine has been demonstrating since independence, but especially brightly since 2014.

The paper, among other things, examines in detail the essence and characteristics of the hybrid war that the Russian Federation has been conducting against Ukraine during the last 8 years. The definition of hybrid warfare, irregular warfare, cyber warfare, and related legal categories is given. The importance of defining the concept of hybrid war is explained by the need to formulate ideas about the current and future problems of Ukraine's state security on its basis. The article is based on the understanding of hybrid warfare as a military strategy that uses political warfare in combination with "conventional" warfare, i.e. , the use of legal instruments and interference in state elections by foreign agents The main national legal and regulatory sources containing the norms of countering hybrid warfare are analyzed. The author's recommendations on methods of combating the aggression of the Russian Federation in the legal field are given.

Key words: hybrid warfare, information war, innovative warfare, cyber war, russian invasion of Ukraine.

DOI: 10.33663/2524-017X-2022-13-24