УДК 343.1
DOI 10.33244/2617-4154.1(10).2023.203-209

М. Є. Дирдін,
канд. юрид. наук, доцент,
заслужений юрист України
e-mail: dyrdin@ukr.net
ORCID ID 0000-0002-2284-2554;
Т. П. Яцик,
канд. юрид. наук, доцент,
Державний податковий університет
e-mail: zvezda171088@gmail.com
ORCID ID 0000-0003-4207-4633

ПРОТИДІЯ ІНФОРМАЦІЙНІЙ СКЛАДОВІЙ ГІБРИДНОЇ ВІЙНИ

У статті проаналізовано проблему інформаційної безпеки України та вплив гібридної війни на національну безпеку держави в цілому та інформаційний простір безпосередньо. Розглянуто відмінності гібридної війни від звичайної та виділено характерні її ознаки. Окреслено рівні війни, на яких можливо прослідкувати гібридну війну. Проаналізовано причини, що створюють сприятливе середовище для розвитку гібридних воєн. Розглянуто наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави в інформаційній сфері. На основі позитивного міжнародного досвіду запропоновано заходи протидії інформаційній складовій гібридної війни.

Ключові слова: *інформаційний простір, кіберзагрози, гібридна війна, протидія, інформаційна складова гібридної війни, міжнародний досвід.*

Метою статті є визначення ефективного механізму протидії інформаційній складовій гібридної війни.

Постановка проблеми. Розвиток інформаційної цивілізації потребує від суспільства суттєвих змін щодо формування інформаційної політики та інформаційної безпеки держави з метою захисту інформаційного простору від несанкціонованих втручань.

Останнім часом у світі зросла потреба в посиленні інформаційної безпеки у зв'язку зі стрімким розвитком цивілізації, новітніх технологій та збільшенням рівня впливу на суспільство та його думку інформації, яку здебільшого можна порівняти зі зброєю, тому що вона здатна завдавати не менш руйнівних наслідків, ніж військові дії. Тому важливо сформувати ефективний механізм протидії інформаційній складовій гібридної війни.

Аналіз останніх досліджень і публікацій. Проблеми захисту інформаційного простору досліджувалися у працях багатьох науковців, а саме: А. Марущака,

В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова та ін. Проблемні питання забезпечення кібербезпеки досліджували Р. Лук'янчук, В. Бурячок, А. Бабенко, В. Гавловський, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев та ін. Проте вказані науковці досліджували природу інформаційної безпеки в цілому, не виділяючи інформаційних загроз та не досліджуючи технологій ведення інформаційно-психологічних війн і операцій, а також визначення та обґрунтування методів протидії інформаційно-психологічним негативним впливам.

Виклад основного матеріалу. Гібридна війна – це особливий тип конфлікту, в якому поєднано принципово різні типи і способи ведення воєнних дій.

Чим же відрізняється гібридна війна від традиційної та в чому її особливість? Які загрози вона несе для сьогодення?

Гібридна війна та її стратегія – поняття не нові. Багато практичних працівників стверджують, що вони виникли ще з появою традиційної війни. Проте останніми роками вони набули значної популярності та актуальності, оскільки держави для ведення гібридної війни мають можливість використовувати як державні, так і недержавні ресурси та суб'єкти, інформаційні технології, щоб приборкати своїх супротивників під час прямого збройного конфлікту, а часто і без його наявності, тоді присутній лише один з елементів гібридної війни – інформаційна війна.

Науковці чітко не розділяють поняття «гібридної війни» та «війни», тому що перша – це один із видів війни, який виник через стрімкий розвиток суспільства в цілому та інформаційних систем зокрема.

Для того щоб зрозуміти, що мається на увазі під терміном «гібридна війна», необхідно проаналізувати війну щодо її ієрархічних рівнів.

На рівні стратегії кожна війна є гібридною. Будь-яка держава та її влада використовують усі наявні інструменти та методи (включаючи невійськові) для досягнення своїх політичних та інших цілей.

На цьому рівні, війна завжди за своєю природою інтерактивна, з обох сторін є спроби подавити та зламати волю супротивника. Тому немає сенсу говорити про гібридну війну на цьому рівні. Що робить війну гібридною, можемо вже побачити, проаналізувавши інші її рівні.

Після рівня стратегії слідує рівень виконання цієї стратегії. Більшість науковців, які досліджують поняття та суть гібридної війни, посилаються саме на цей рівень, який дає можливість виділити характерні риси гібридної війни. На цьому рівні (тактичному) гібридну війну можна відрізнити від звичайної за рахунок використання нових збройних (військових) систем і технологій та застосування їх регулярними, нерегулярними і недержавними силами. Це зі свого боку надає не тільки тактичні можливості, але також сприяє появі нових загроз. Гібридна війна на тактичному рівні означає, що системи озброєнь нині здатні досягати непропорційно високих стратегічних наслідків [1, с. 32].

Інформатизація суспільства – це всеохоплюючий і неминучий процес у розвитку людської цивілізації в цілому та кожної особи зокрема. За інформатизацією стоїть майбутнє, але це і виклик, який постав перед людством щодо приборкання такої

потужної рушійної сили. Інформатизація суспільства передбачає використання більш ширшого кола інформаційних технологій у всіх сферах держави і суспільства з метою підвищення їх розвитку. Проте така діяльність породжує не тільки позитивні моменти, але і негативні.

Оскільки останні десятиліття супроводжувалися стрімким розвитком інформаційних технологій, обмін інформацією значно пришвидшився. У зв'язку з розбудовою мережі «Інтернет» з'явилися нові можливості поширення інформації [2, с. 119].

Гібридна війна досить розповсюджений вид війни у XXI столітті, за допомогою якої можна досягти масштабних наслідків, використовуючи скромні засоби.

Такий вид війни передбачає взаємодію або злиття звичайних і нетрадиційних інструментів влади та тактик ведення війни. Ці інструменти та тактики поєднуються синхронізовано, щоб використовувати вразливі місця противника та досягати синергічного ефекту.

Мета поєднання різних інструментів і тактик полягає в тому, щоб завдати шкоди воюючій державі оптимальним чином. Крім того, є дві відмінні характеристики гібридної війни. По-перше, межа між воєнним і мирним часом стає розмитою. Це означає, що важко ідентифікувати або розрізнити вид війни і навіть інколи взагалі складно стверджувати, що ведеться війна, тому що вона стає невловимою. Потрібно звернути увагу на те, що гібридна війна за порогом війни або прямого відкритого насильства приносить досить ґрунтовні і швидкі «дивіденди», тому що стратегія її ведення простіша, процес втілення стратегії дешевший та менш ризикований, ніж відкритий збройний конфлікт. Тут досить доречними є слова давнього китайського стратега і мислителя, автора знаменитого трактату про військову стратегію «Мистецтво війни» Сунь Цзи: «Вищим мистецтвом війни є підпорядкування ворога без бою». Праця цього мислителя є ще одним підтвердженням, що поняття гібридної війни з'явилося разом з поняттям звичайної війни.

Друга визначальна характеристика гібридної війни стосується неоднозначності та неможливості визначення суб'єкта, який вчиняє атаки. Гібридні атаки зазвичай відрізняються великою нечіткістю та хаотичністю. Така невідомість свідомо створюється та розширюється суб'єктами, які ведуть гібридну війну, щоб ускладнити процес їх виявлення, ідентифікації та застосування відповіді на їх дії. Іншими словами, країна, яка є мішенню, часто не в змозі виявити вчасно ознаки гібридної атаки або визначити державу, що може вчиняти або спонсорувати такі дії. Це зі свого боку ускладнює процес розробки державної політики та обрання стратегічних заходів щодо протидії таким негативним явищам [3].

Для повного розуміння, що являє собою гібридна війна, потрібно проаналізувати її основну особливість.

Однією з ключових особливостей гібридної війни є її інформаційна складова, яка передбачає використання інформації як зброї.

Вважаємо вдалим твердження американського дослідника М. Маклюена, що «...істинно тотальна війна – це війна за допомогою інформації» [4].

Якщо розглядати інформаційну складову гібридної війни росії проти України, то можна прослідкувати чітко сплановану кампанію, метою якої насамперед було зниження довіри громадян України до влади країни за допомогою ведення інформаційної війни, спрямованої на дискредитацію державних органів та Збройних сил України, а також заохочення збільшення злочинності, сепаратизму та колабораціонізму. Ця інформаційна кампанія сприяла соціально-політичній дестабілізації у країні і сьогодні продовжує негативно впливати на окремі категорії осіб у державі. Проте є і позитивні моменти, вона вже не впливає так тотально на країну в цілому.

Гібридна війна росії характеризується використанням не лише інформаційної складової, а й поєднанням її із психологічними діями, які реалізуються саме через інформаційну складову гібридної війни та завдають глобальних збитків державі та суспільству.

Інформаційна складова гібридної війни – це не тільки вчинення кіберзлочинів, хоча звичайно, вони є її частиною. Це також некоректні маніпуляції з інформацією або її підтасовування, а в деяких випадках і подача завідомо помилкових, неправдивих фактів, внаслідок чого відбувається залякування населення, нав'язування параноїдальних думок [5, с. 55].

Держава-агресор здійснює систематичний політичний, економічний та військовий тиск щодо України з метою запобігання можливості української євроінтеграції. Вибравши конфронтаційну модель розвитку ситуації, росія відкрито використовує жорстку інформаційну складову гібридної війни та військову силу для досягнення своїх цілей з метою дискредитації України в очах міжнародної спільноти.

Крім того, росія також вживає заходів для досягнення своїх цілей в Україні, щоб змінити чинний уряд країни, український політичний курс та заручитися підтримкою більшості суспільства, яке відреагувало на інформаційну складову гібридної війни.

Російська влада намагається досягти своїх цілей за допомогою таких заходів:

— стимулювання федералізації України з подальшим проведенням референдумів щодо зміни політичного порядку;

— застосування морального тиску на українське суспільство шляхом демонстрацій (за допомогою лояльних засобів масової інформації та агентів впливу) неспроможності української влади реалізувати ідею державності;

— підтримки протестів та створення умов для розколу цілісності нації;

— порушення балансу в політичній системі країни та деморалізації державних чиновників та державних установ з метою запобігання їм належним чином виконувати свої функції;

— активізації таємної діяльності проросійського лобі в державних структурах і стимулювання різноманітних конфронтацій, суперечок та конфліктів у межах України;

— використання мережі спеціальних агентів для дискредитації відомих українських політиків, які підтримують державність і національні позиції України [6, с. 27–28].

Якщо проаналізувати всі ці заходи, то можна помітити, що вони реалізовувалися і реалізуються за допомогою інформаційної складової гібридної війни (затрачалися досить незначні ресурси, а досягалися масштабні наслідки. Проте з початком ведення

агресивної війни росієї проти України ситуація дещо змінилася. Державі-агресору доводиться затрачати значні ресурси для ведення гібридної війни, тому що ввесь світ нарешті зрозумів, що вся інформація, яка подається російськими засобами масової інформації, є неправдивою та направлена на дестабілізацію ситуації не тільки в Україні, але і в усьому світі).

Як можна протидіяти гібридній війні в цілому та її інформаційній складовій безпосередньо?

Україна вже зробила вагомі кроки до зміцнення своєї державності, обороноздатності для безпеки в кіберпросторі:

— налагодження комунікації держави (органів державної влади, місцевого самоврядування та їх посадових осіб з громадянами країни та міжнародною спільнотою). З цією метою в Україні 2021 року створено Центр стратегічних комунікацій та інформаційної безпеки за прикладом Європейського Союзу, який 2016 року ухвалив резолюцію «Стратегічні комунікації ЄС як протидія пропаганді «третіх сторін», згідно з якою було створено Центри стратегічних комунікацій (StratCom) у Ризі, Польщі, Литві, а також Центр протидії гібридним загрозам.у Фінляндії);

— напрацювання системи національної стійкості (яка була затверджена Указом Президента України від 27 вересня 2021 року № 479/2021) – досвід Естонії.

Якщо взяти досвід Азербайджанської Республіки у війні проти Вірменії, то потрібно звернути увагу на законодавчі застереження щодо використання фото- та відеоматеріалів із зображенням військових або військової техніки, зокрема з використанням геолокації. В українському законодавстві такі застереження з'явилися лише у 2022 році.

Але, на нашу думку, сьогодні для регулювання питання безпекового середовища в інформаційному просторі доцільно використовувати сукупність позитивних практик зарубіжних країн, а саме:

— модернізацію та гармонізацію законодавства України щодо протидії кібер-загрозам, гібридній війні;

— блокування каналів фінансування суб'єктів гібридних загроз;

— співпрацю держави з міжнародними партнерами у рамках спеціальних операцій щодо протидії таким загрозам.

Висновки. Підсумовуючи вищевикладене, можна констатувати, що інформаційна складова гібридної війни досить потужна рушійна сила та швидко розвивається, що може призвести до надзвичайних наслідків. Тому вже сьогодні країнам потрібно об'єднуватися і розробляти стратегії боротьби, а бо хоча б контролю інформаційної складової гібридної війни.

На нашу думку, зменшення впливу інформаційної складової гібридної війни можна досягти шляхом підвищення довіри осіб до діяльності держави в цілому та її посадових осіб зокрема, тому що найчастіше мішенню гібридних війн є саме цивільне населення, точніше їхня думка про державу, в якій вони проживають чи перебувають. Якщо ворогові вдається за допомогою інформаційної складової гібридної війни вплинути на

населення (внести зерно сумніву) щодо довіри до держави, то це в цілому впливає на зниження економічного, політичного, соціального та військового потенціалу держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pikner I., Zilincik S. Military concepts and hybrid war. Forum Scientiae Oeconomia. 2016. Volume 4. Special Issue № 1. URL: file:///C:/Users/Home/Desktop/forum-002.pdf

2. Яцик Т. П., Бодунова О. М. Розповсюдження фейкової інформації як загроза інформаційній безпеці України. *Протидія фейкам в Україні як складова інформаційної безпеки держави*: міжвідомчий круглий стіл, 20 травня 2021 року. Київ: ІСТЕ СБУ, 2021. 126 с.

3. Arsalan Bilal. Hybrid Warfare – New Threats, Complexity, and «Trust» as the Antidote. Opinion, analysis and debate on security issues. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

4. Що таке інформаційна війна. URL: my.elvisti.com/sergandr/iv.html

5. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право).* 2014. № 2(65).

6. Horbulin V. The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from Ukrainian. Kharkiv: Folio, 2017. 158 p.

REFERENCES

1. Pikner I., Zilincik S. (2016). Military concepts and hybrid war. Forum Scientiae Oeconomia. Volume 4. Special Issue № 1. URL: file:///C:/Users/Home/Desktop/forum-002.pdf

2. Yatsyk T. P., Bodunova O. M. Rozpovsiudzhennia feikovoi informatsii yak zahroza informatsiinii bezpetsi Ukrainy. *Protydiia feikam v Ukraini yak skladova informatsiinoi bezpeky derzhavy*: mizhvidomchyi kruhlyi stil, 20 travnia 2021 roku. Kyiv: ISTE SBU, 2021. 126 s.

3. Arsalan Bilal. Hybrid Warfare – New Threats, Complexity, and «Trust» as the Antidote. Opinion, analysis and debate on security issues. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

4. Shcho take informatsiina viina. URL: my.elvisti.com/sergandr/iv.html

5. Yatsyk T. P. (2014). Osoblyvosti informatsiinoho teroryzmu yak odnoho iz sposobiv informatsiinoi viiny. *Naukovyi visnyk Natsionalnoho universytetu DPS Ukrainy (ekonomika, pravo)*, 2(65).

6. Horbulin V. The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from Ukrainian. Kharkiv: Folio, 2017. 158 p.

M. Dyrdin, T. Yatsyk. Counteracting the Information Component of Hybrid Warfare

The article analyzes the problem of information security of Ukraine and the impact of hybrid war on the national security of the state as a whole and the information space directly. The differences between hybrid war and conventional war are considered and characteristic features of hybrid war are highlighted. The levels of war at which it is possible to observe a hybrid war are outlined. The reasons that create a favorable environment for the development of hybrid wars are analyzed. The existing and potentially possible phenomena and factors that create a danger to the vital interests of man and citizen, society and the state in the information sphere are considered. On the basis of positive international experience, countermeasures against the informational component of hybrid warfare are proposed.

Key words: *information space, cyber threats, hybrid war, countermeasures, information component of hybrid war, international experience.*

Стаття надійшла до редколегії 9 січня 2023 року