УДК 351.862.4

БЛАГОДАРНИЙ Андрій Миколайович,
ШТЕЛЬМАХ Оксана Віталіївна

ОРГАНІЗАЦІЙНІ АСПЕКТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ЯК СКЛАДОВІЙ ГІБРИДНОЇ ВІЙНИ

Постановка проблеми. В умовах становлення інформаційного суспільства та глобального інформаційного простору, стрімкого розвитку суспільних комунікацій, інформаційно-комп'ютерних і телекомунікаційних технологій актуалізується проблема інформаційної агресії. У контексті зазначеного вкрай *актуальним завданням* постає дослідження природи інформаційної агресії, що має тенденцію до поширення в сучасному світі [9].

Аналіз останніх досліджень і публікацій засвідчує, що проблемам дослідження змісту, характеру та особливостей інформаційної агресії як складової гібридної війни присвячували свої праці такі вітчизняні та іноземні автори, як С. Корнієнко, Є. Магда, А. Парубій, М. Сенченко, В. Черниш, О. Гіда, Джон Девіс, Франк ван Каппен, Даниель Ласица, Нейтан Фраєр, Франк Хоффман, а також інші фахівці різних галузей знань, але у зв'язку із динамічним розвитком подій ці питання потребують подальшого вивчення, передумовою якого є дослідження інформаційної агресії як складової гібридної війни та основних аспектів протидії.

Враховуючи невирішені раніше частини загальної проблеми змісту, характеру та особливостей гібридної війни, яка розпочата проти нашої країни, зазначимо, що новизна статті полягає в дослідженні питань застосування державними органами України заходів щодо протидії інформаційній агресії, тому **метою** роботи є дослідження інформаційної агресії як складової гібридної війни та основних аспектів протидії їй. Для цього необхідно виконати наступні завдання: дослідити поняття гібридної війни та інформаційної агресії як її складової; дослідити мету, план дій та складові гібридної війни; з'ясувати мету, властивості, етапи реалізації інформаційної агресії та визначити аспекти протидії їй.

Виклад основного матеріалу. Найчастіше гібридна війна (англ. Hybrid warfare) визначається як сукупність заздалегідь підготовлених і оперативно реалізованих державою дій військового, дипломатичного, інформаційного характеру, спрямованих на досягнення стратегічних цілей [2]. Гібридна війна – це війсь-

кова стратегія, яка об'єднує звичайну війну, малу війну і кібервійну. Термін «гібридна війна» використовують для опису атак за допомогою ядерної, біологічної та хімічної зброї, саморобних вибухових пристроїв та інформаційної війни. Такий підхід до ведення конфліктів є потужним й складним різновидом війни. Також цей термін використовується у випадках, коли потрібно охарактеризувати гнучку і складну динаміку бойового простору, що передбачає гнучку реакцію, яка легко адаптується [9].

Концепція «гібридного» типу не є офіційною та вживається американськими військовими для характеристики такого механізму, методу або способу ведення війни, коли має місце поєднання звичайного та нестандартного типів. Визначення «гібридна війна» відсутнє в міжнародно-правових документах. Доктрина збройних сил США офіційно визнає лише два типи ведення війни: звичайний та нестандартний. Більше того, такого поняття не існує й у Воєнній доктрині України – документі, що є національною системою керівних поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів [10].

Держава, яка веде гібридну війну, співпрацює з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується [5].

Про зміну парадигми війни в сенсі залучення до неї невійськових структур говорить і Ф. ван Каппен: «„Гібридна війна" – це змішування класичного типу війни з використанням нерегулярних військових формувань. Держава, яка веде „гібридну війну", реалізує угоду з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими повністю заперечується. Ці виконавці можуть здійснювати такі речі, яких сама держава здійснювати не може… Усю брудну роботу можна перекласти на плечі недержавних формувань» [3].

За словами підполковника корпусу морської піхоти США Білла Неметті, гібридна війна – це такий вид партизанської війни, який об'єднує сучасні технології та сучасні методи мобілізації. Нейтан Фраєр з Центру стратегічних і міжнародних досліджень одним із перших визначив ключові загрози, які включає в себе гібридна війна: традиційні, нестандартні, катастрофічний тероризм і підривні, коли використовуються технології для протидії перевазі у військовій силі. Девід Кілкаллен, автор книги «Випадкова герилья», стверджує, що гібридна війна – це найкраще визначення сучасних конфліктів, але підкреслює, що воно включає в себе комбінацію партизанської та громадянської воєн, а також заколоту і тероризму. Журналіст Ф. Хоффман вбачає гібридну війну у вигляді будь-яких дій ворога, який миттєво й злагоджено використовує складну комбінацію дозволеної зброї, партизанську війну, тероризм і злочинну поведінку на полі бою, щоб домогтися політичних цілей. Заступник секретаря ВМС США Роберт Ортон Ворк стверджує, що ворожі війська можуть використову-

вати «гібридних військовослужбовців», що конспіративно знаходяться серед цивільного населення [9].

Тобто гібридна війна поєднує в собі принципово різні типи і способи ведення війни, а саме: класичну війну з використанням армії та озброєння, дезінформацію населення та агітацію за допомогою співпраці з нерегулярними збройними формуваннями (повстанці, терористи, партизани), інформаційну та кібервійну.

Наразі питання протидії гібридній війні є дуже актуальним. Багато дослідників, політичних діячів висловлювали свої думки з приводу цього у наукових роботах, статтях. Ще в 1975 році британський учений-міжнародник Е. Макк зробив важливий висновок: у більшості сучасних конфліктів сильні країни не зазнали військової поразки, вони зазнали поразки в політичному сенсі – не зуміли нав'язати свою волю противнику. Політична перемога слабкої сторони полягала в тому, що вона – шляхом застосування асиметричних способів ведення військових дій (переважно партизанських) – спромагалася виснажити волю сильного ворога до продовження війни та досягнення поставлених цілей [5].

Метою військових дій у гібридній війні є не завоювання чи втримання території, а хаос, неперервний конфлікт і постійне генерування провокацій і постановочних військових подій для ЗМІ [4].

Успіх гібридної війни досягається завдяки не лише докладно розробленому плану дій, а й слушно вибраному моменту для його реалізації, зокрема:

– ослаблення центральної влади та часткове «безвладдя» на тлі зміни влади;

– зростання суперечностей (актуалізація вже наявних) між центром і регіонами;

– незадовільний психологічний і матеріально-технічний стан структур безпеки;

– антагонізм між різними силовими структурами;

– активна інформаційно-пропагандистська робота протягом довгого періоду часу [3].

Хоча військова складова конфлікту об'єктивно залишається основним чинником його розгортання, масштаби застосування інформаційної складової стають дедалі більшими [11, с. 395].

Інформаційний фронт гібридної війни розгортається одразу на кількох напрямах. Передусім серед населення в зоні конфлікту; серед населення країни, проти якої здійснюється агресія, однак, територія якої не охоплена конфліктом; серед громадян країни агресора і серед міжнародного співтовариства [3].

Важливим компонентом ведення такої війни є і вплив на інформаційну сферу суспільства [3]. Зокрема, прояв інформаційної агресії до країни, яка є об'єктом гібридної війни.

Інформаційну агресію можна визначити як незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на завдання супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального за своїми масштабами застосування сили.

Сучасна людина піддається інформаційній агресії щоденно сотні раз. Інтернет, радіо, телебачення, газети й журнали нав'язують своє розуміння життя, що завдяки маніпулятивному ефекту впливає і на наш світогляд. Основна мета інформаційної агресії – це вплив не тільки на свідомість, а й на підсвідомість, щоб «скоригувати» громадську думку всередині як країни-жертви, так і країни-агресора. Все робиться для того, щоб основні переконання цієї маніпуляції залишили незгладимий слід у душі особи і надійно закріпилися в ній.

Процеси маніпулювання масовою й індивідуальною свідомістю за допомогою засобів масової інформації, особливо електронних, шляхом інформаційної агресії набувають усе більш широкого розмаху [8].

Загалом можна виокремити такі основні властивості інформаційної агресії:

1) несиловий характер (за рахунок ЗМІ);

2) швидкість розповсюдження;

3) пандемічність, опосередкований характер і потаємність впливу (інформаційна дія має глобальний характер й на відміну від фізичного впливу, може бути абсолютно непомітною);

4) віртуальний характер дії (крихкість інформаційного світу, легкість доступу, можливість зламу інформаційних систем) [8].

Інформаційна агресія передбачає реалізацію «теракту» не в реальності, а у свідомості. Робота ЗМІ полягає в тому, щоб здійснювати вплив на споживача інформації, нав'язувати йому певну ідею. Споживач свідомо цьому піддається, пасивно сприймаючи все те, що йому надходить.

Тим часом методи і технології інформаційного впливу на нього вдосконалюються з небувалою швидкістю. Інформаційне протистояння панівної ідеології, дійсно, стає ще більш агресивним. Зазвичай, інформаційна агресія відбувається у три етапи:

1 **Створення ядра.** З'являється досить велика кількість людей, які не сприймають стан речей, що склався, які мають цінності, несумісні з панівним світоглядом, і незадоволені своєю пасивною роллю в системі відносин, що сформувалася, причому налаштованих при цьому зовсім непримиренно. Це робиться якомога агресивніше, щоб не загубитися в навколишньому інформаційному шумі, з помітним акцентом на заперечення фактичного стану речей; альтернативу, зазвичай, окреслюють досить схематично. Ідеологи інформаційного протистояння на цьому етапі орієнтуються на тих, хто потерпає від відсутності інформації та від її нерозуміння. Найголовніше завдання цього етапу вони вбачають у тому, аби показати, що альтернатива не тільки можлива, а й неминуча, що її прихильники діють; озброїти словом і надією тих, хто цього потребує.

2 **Створення середовища.** Люди різних опозиційних настроїв поєднуються для того, щоб підтримувати одне одного. При цьому організовуються вони на цьому етапі не за принципом «за», а за принципом «проти». Найголовніша мета полягає в тому, щоб створити альтернатив-

ний інформаційний простір, зі своїми установками і табу, аж до рефлексів, й реалізувати відповідну інформаційну агресію, що переважає агресію супротивника.

3 **Створення атмосфери.** Створити певну інформаційну атмосферу, змінюючи суспільну думку спрямованими точковими ударами з різних боків. Як тільки кількість активістів і симпатиків стане достатньою для того, щоб забезпечити масованість і постійність цих ударів, щоб інформаційну битву було виграно [7].

Щоб не допустити реалізації інформаційної агресії на території своєї країни потрібно вміти як попередити її, так і оборонятися від неї. Оскільки її метою є маніпулювання людською свідомістю і створення хаосу серед населення для полегшення керування ним. Протидія цій агресії потребує також міцного інформаційного фундаменту в національній свідомості й поглядах народу.

Згідно стратегії гібридної війни та ознак і методів інформаційної агресії як її складової, можемо виділити такі аспекти протидії:

– постійний контроль інформаційного простору (преса, телебачення, радіо, інтернет);

– недопущення створення на своїй території недержавних військових організацій для знищення людського, економічного та інфраструктурного потенціалу держави чи регіону;

– обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає інформаційний простір держави-жертви не цілком, а тільки його частину) [6, с. 99];

– посилення авторитету своєї влади та уряду, армії серед населення країни, щоб перешкодити переходу на бік ворога та підтримці ідей, які він нав'язує;

– ефективна інформаційна політика: стратегічна спрямованість та зворотний зв'язок із суспільством [1].

Висновки і перспективи подальших досліджень. Підсумовуючи, необхідно сказати, що при веденні гібридної війни супротивником застосовуються всі можливі методи. Вона поєднує в собі класичну війну із використанням армії та озброєння, новітні технології, кібервійну, інформаційну війну. Інформаційна агресія є складовою гібридної війни. Її мета – не тільки вплив на свідомість і підсвідомість населення, а також маніпуляція його думками і діями. Її дія поетапна і цілеспрямована. Після створення ядра, ідея інформаційної агресії швидко поширюється серед певної маси людей, на яку вона розрахована, для створення середовища й атмосфери в певному регіоні, щоб держава-агресор могла ефективно провадити свою політику. Для недопущення наслідків інформаційної агресії необхідні не лише заходи, спрямовані на зміцнення військового та економічного потенціалу країни, а й посилення впливу державної влади у всіх сферах життєдіяльності, особливо тих, через які найлегше можна вплинути на свідомість

населення держави. В подальшому *основним напрямом досліджень* у вказаній сфері є удосконалення правової регламентації застосування заходів протидії інформаційній агресії в умовах гібридної війни.

Список використаних джерел

1 Брецко Ф. Російська гібридна війна проти України і світу [Електронний ресурс] / Ф. Брецко . – Режим доступу : http://rionews.com.ua.

2 Гібридна війна: як це працює [Електронний ресурс]. – Режим доступу : http://www.csr.org.ua.

3 Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу [Електронний ресурс] / В. Горбулін. – Режим доступу : http://gazeta.dt.ua/internal/gibridna-viyna.

4 Дацюк С. Стратегія перемоги України у війні з Росією [Електронний ресурс] / С. Дацюк. – Режим доступу : http://blogs.pravda.com.ua/authors/datsuk/.

5 Корнієнко С. Путін веде в Україні гібридну війну [Електронний ресурс] /С. Корнієнко. – Режим доступу : http://www.radiosvoboda.org/content/article/.

6 Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.

7 Мироненко В. Інформаційна агресія й інформаційне протистояння [Електронний ресурс] / В. Мироненко. – Режим доступу : http://personal.in.ua.

8 Пилипчук В. Г. Проблема агресії і насильства: світоглядно-інформаційний вимір / В. Г. Пилипчук, О. П. Дзьобань // Український науковий журнал «Освіта регіону». – 2014. – № 2. – С. 171.

9 Чекаленко Л. Про «гібридну» війну [Електронний ресурс] / Л. Чекаленко. – Режим доступу : http://uaforeignaffairs.com/ua/blog/usi-blogi/view/article/pro-gibridnu-viinu.

10 Черниш В. Що відбувається на Сході України. Ще раз про термінологію [Електронний ресурс] / В. Черниш. – Режим доступу : http://osvita.mediasapiens.ua/media_law/law/scho_vidbuvaetsya_na_skhodi_ukraini_sche_raz_pro_terminologiyu.

11 Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни / О. В. Штельмах // Актуальні проблеми управління державною безпекою : зб. матер. наук-практ. конф. (Київ, 19 березня 2015 р.). – К. : Центр навч., наук. та період. видань НА СБ України, 2015. – 512 с. – С. 393–396.

Рецензенти:
кандидат юридичних наук
О. Розвадовський,
кандидат юридичних наук, доцент
В. Окіпнюк

Аннотация: Согласно стратегии гибридной войны и признакам информационной агрессии как ее составляющей определены такие аспекты противодействия: контроль информационного пространства, предупреждение создания на своей территории негосударственных военных организаций, усиление авторитета государственной власти, эффективная информационная политика.

Ключевые слова: гибридная война, информационная агрессия, информационная безопасность.

Abstract: According to the «hybrid war» strategy and the features of information aggression as its constituent part the article covers such aspects of counteraction: the monitorship of media scene; prohibition of armed non-state actors formation; enhancing the authority of government and army in the country; effective information policy.

Key words: hybrid war, information aggression, information security.

УДК 342.951:351.746.1(477)

ГРИЩЕНКО Ірина Володимирівна

ЕТАПИ СТАНОВЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Постановка проблеми. На сучасному етапі перед українською державою постає ціла низка викликів як зовнішніх, так і внутрішніх, які становлять загрозу для економічної та інформаційної безпеки, територіальної цілісності, обороноздатності, державного суверенітету. Держава має адекватно реагувати на подібні ситуації, охороняючи відомості, що містять державну таємницю з метою захисту національних інтересів. Ефективне розв'язання цієї проблеми можливе завдяки створенню відповідної системи охорони державної таємниці на основі врахування досвіду міжнародної спільноти і власних надбань на різних етапах державного розвитку України. Отже, на часі вивчення досвіду функціонування системи охорони державної таємниці в Україні з метою актуалізації в сучасних умовах.

Аналіз останніх досліджень і публікацій. На сьогодні вивченням інституту державної таємниці, проблем становлення та функціонування системи її охорони в нашій державі на різних етапах займались українські і зарубіжні вчені О. Абадаш [1], В. Артемов [2], О. Ботвінкін [3], В. Сідак [16], О. Шамсутдінов [18],