УДК 355.01:355/359.08:32.019.57

Ю. М. Юрчак

НАУКОВО-ПРАГМАТИЧНІ АСПЕКТИ ГІБРИДНОЇ ВІЙНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Досліджено особливості науково-прагматичних аспектів гібридної війни. Розглянуто явище гібридної війни як наукової проблеми. Розкрито становлення теорії гібридної війни, військово-теоретичні підходи до характеристики її сутності. Наголошено на необґрунтованому характері здійснення гібридної агресії Російської Федерації проти України. Подано аналіз ознак гібридної війни. Зроблено висновок, що гібридні війни є новим інструментом агресії неоімперських тоталітарних держав, спрямованої на суверенні держави, які виступають проти гегемонії Росії на пострадянських теренах. Обґрунтовано необхідність удосконалення системи забезпечення національної безпеки України з урахуванням специфіки Державної прикордонної служби України. Вивчено окремі підходи до визначення гібридної війни, визначено сутність та загальні риси гібридної війни, проаналізовано проблемні питання захисту національних інтересів на державному кордоні.

Ключові слова: *гібридна війна, національна безпека, Державна прикордонна служба України, збройна агресія.*

Постановка проблеми. У сучасних умовах різко зростає роль та значення інформаційного фактора у житті країни. Інформаційне середовище здатне прискорювати чи гальмувати розвиток усіх сфер суспільного життя, зокрема процесів, які тісно пов'язані з безпекою державного кордону.

Після початку російської агресії серед загроз національній безпеці України одні з перших місць посіли загрози інформаційного характеру, особливо небезпечні під час бойових дій. Радикальні зміни сталися після початку російської агресії проти України 2014 р. З 24 лютого 2022 р. це питання набуло ще більшого значення для безпеки державного кордону та забезпечення обороноздатності держави у цілому.

На Державну прикордонну службу України покладається завдання щодо забезпечення недоторканності державного кордону та охорони суверенних прав України у її прилеглій зоні та виключній (морській) економічній зоні [1]. Під час воєнного вторгнення постає питання охорони та захисту державного кордону, що відбувається у складних умовах збройного конфлікту, який на початковому етапі мав характер гібридної війни на сході і півдні нашої держави. Загрози національній безпеці, суверенітету держави, безпеці державного кордону пов'язані передусім із агресією Російської Федерації (РФ), яка не припиняє спроб анексувати територію України. На сьогодні у ході боїв та збройного протистояння знищено або захоплено значну кількість об'єктів прикордонної інфраструктури, техніки та озброєння. У цьому протистоянні саме Державна прикордонна служба України (ДПСУ) стоїть на передовій у відновленні суверенітету і територіальної цілісності України.

У зв'язку з цим особливої актуальності набуває пошук шляхів забезпечення реалізації функції ДПСУ, виявлення проблемних питань захисту національних інтересів на державному кордоні і пошуку шляхів їх вирішення, а також упровадження сучасних наукових поглядів та підходів у сфері прикордонної безпеки, адже сучасна, добре оснащена та ефективна Державна прикордонна служба України має виняткове значення для національних інтересів України.

Роботу побудовано як аналітичну розвідку, у якій досліджується інформація, отримана з відкритих джерел.

Проблема дослідження аспектів гібридної війни стала актуальною після вторгнення РФ в

Україну у 2014 р. Гібридна війна є сучасною формою воєнної діяльності, яка використовує комбінацію військових, політичних, економічних, соціальних, інформаційних та інших засобів, щоб досягти власних військових та політичних цілей. Це новий підхід до війни, що відрізняється від традиційної війни, в якій використовується виключно військова сила.

Однак гібридна війна стає дедалі більш поширеною та викликає загрозу для міжнародної безпеки. Вона відрізняється від традиційної війни тим, що відбувається у різних напрямах, зокрема в електронному просторі. Це вимагає від держав розроблення нових стратегій та методів захисту. Загалом гібридна війна є однією з найменш вивчених форм ведення війни.

Аналіз останніх досліджень і публікацій. У дослідженнях та публікаціях сьогодення вивчається вплив гібридної війни на планування й проведення військових операцій. Розглядається вплив гібридної війни на зміни політики, стратегії та тактики, а також принципи й практики застосування військової сили. Виявляється, що гібридна війна змінює тактику та принципи військового планування. Як свідчить аналіз наукових праць, проблема збройного гібридного конфлікту викликає значний інтерес сучасних дослідників, політиків, експертів та журналістів. Особливістю висвітлення та дослідження цього конфлікту є увага світової спільноти до збереження територіальної цілосності України.

Специфіка розв'язаної Росією війни за методами свого ведення відрізняється від традиційних воєн, що відбувались у XXI ст. Надзвичайна актуальність цієї проблеми зумовлює значний інтерес науковців.

Проблему гібридної війни досліджували Д. Купрієнко, А. Братко, В. Торічний, Т. Білецька, М. Машовець, О. Литвиненко, О. Турчинов, О. Лещенко, В. Маркітантов, О. Рибщун, Ю. Столяр, Г. Херд, Р. Шутов, В. Вейбел та інші вчені.

Питання протидії негативному інформаційно-психологічному впливу на персонал органу охорони державного кордону в контексті інформаційної війни розглядали В. Демський, Ю. Юрчак. Разом з тим актуальною залишається проблема чіткого визначення ролі і місця ДПСУ у забезпеченні національної безпеки та суверенітету держави під час неоголошеної війни, формування питань захисту національних інтересів на державному кордоні і пошуку шляхів їх вирішення. Також розглядаються питання захисту та безпеки державного кордону під час гібридної війни. Аналізуються ризики й можливі підходи до розвитку захисту від гібридних атак, а також механізми протидії їм.

Метою статті є дослідження актуальних науково-прагматичних аспектів гібридної війни у контексті діяльності Державної прикордонної служби України у системі протидії агресії Російської Федерації.

Виклад основного матеріалу. Актуальне значення у сучасних умовах має філософське осмислення такого нового та порівняно маловивченого явища, як гібридна війна. Відомо, що гібрид (від лат. *hibrida, hybrida* – помісь) – продукт схрещування генетичних форм, котрі різняться. Спочатку термін використовувався у ботаніці та зоології. Потім це поняття отримало широке застосування у різних сферах, включно з військовою. Звернення до проблематики гібридних воєн обумовлено, з одного боку, кризою теорії і практики класичних воєн та різноманіттям сучасних форм збройних конфліктів. Узагальнюючи сучасні тенденції у сфері ведення воєн, гібридна агресія Росії розглядається військовими фахівцями різних країн як така, що має глобальний характер. Точкою відліку для формування гібридного світоустрою стала агресія РФ проти України, яка спричинила руйнівні наслідки для європейської та глобальної безпеки. На думку експертів, Україні необхідно формувати комплексні стратегічні підходи у протидії російській гібридній агресії, створювати гнучкі й ефективні механізми реагування та протистояння загрозам. Саме гібридна війна та гібридні загрози визначають багато сучасних тенденцій у розвитку миру та війни. З іншого боку, зберігається дискусійний характер розуміння гібридної війни у військово-теоретичній та соціально-філософській думці. Бракує єдності поглядів на природу, генез, сутність, структуру, специфіку гібридної війни. Сьогодні питання про те, що таке гібридна війна і чим вона відрізняється від інших типів військових конфліктів, є неоднозначним. Поняття гібридної війни залишається неопераціоналізованим [2]. Разом з тим у загальному, схематичному вигляді її характеризують як тип конфлікту, що виник у змішуванні сил, засобів, способів, тактики звичайної та іррегулярної війни. Також з моменту виникнення і до сьогодні відбувається помітна трансформація уявлень про суб'єкти гібридної війни.

З позицій сучасного досвіду очевидно, що такий підхід не вичерпує усіх проявів і видів. Гібридна війна як конфлікт XXI ст. – це складніший набір використовуваних у ній

інструментів сил та засобів. Водночас гібридні війни недержавних, незаконних збройних формувань проти суверенних держав та законних збройних сил не витратили повністю свій потенціал у сучасному світі.

Для успішного протистояння гібридній агресії Росії украй необхідне передусім внутрішнє зміцнення держави. Цього можна досягти шляхом удосконалення демократичного врядування, нормативно-правової бази та системи політичних і спеціальних інститутів забезпечення безпеки, подолання корупції і створення умов для функціонування організацій громадянського суспільства.

Слід визначити основні проблемні питання захисту національних інтересів на державному кордоні на початковому етапі збройної агресії з боку Росії:

– погана готовність сил і засобів до дій в абсолютно новій оперативній і криміногенній обстановці на державному кордоні України;

– невідповідність новим загрозам побудови системи охорони державного кордону;

– недостатня кількість випереджувальної інформації про можливе збройне вторгнення на державному кордоні;

– обмежене забезпечення військ і персоналу;

– недостатня укомплектованість підрозділів охорони державного кордону особовим складом, озброєнням та військовою технікою.

Необхідне проведення збалансованої міжетнічної і міжконфесійної політики, широке інформування суспільства про чутливі теми, зокрема історичні, які використовуються або можуть використовуватись агресором для досягнення своїх цілей. Такий комплексний усеохоплюючий підхід дасть змогу консолідувати суспільство і убезпечити його, може стати зразком для інших країн, які потерпають від гібридних загроз [3], причому, здійснюючи дії між миром і війною так, щоб не переступити поріг розв'язування звичайної війни і «маскуючи своє втручання» під воєнну операцію [4]. Особливості гібридної війни дозволяють використовувати різні способи військового і невійськового насильства поступово, потай і опосередковано. Під час прихованої дії застосовуються нерегулярні військові формування, ведеться війна «чужими руками», використовуються приватні військові компанії, що дає можливість приховувати справжніх ініціаторів конфлікту. Так, гібридна війна стає податливим простором між війною та злочинністю на перетині нетрадиційних засобів, незаконних методів та міжнародних норм, порядку та анархії [5].

Важливо додати, що гібридні війни не слід співвідносити з діями будь-якої держави у конфліктах XXI ст. Гібридні війни – це інструмент агресії неоімперських держав і країн, які прагнуть зберегти колоніальний порядок у світі, здійснити новий територіальний переділ на користь контролю світових ресурсів, десуверенізації суб'єктів світової політики, розвалу країн, що опираються, а також мілітаристських держав, націлених на розширення сфери геополітичного впливу, силове вирішення територіальних суперечок, реалізацію експансіоністських територіальних домагань. Суттєвою рисою гібридної війни є її асиметричний характер, оскільки протиборство у ній ведеться між державою та недержавними суб'єктами, у військових силах яких є значний дисбаланс (асиметрія) або які застосовують кардинально різні стратегії та тактику. Ці асиметричні методи та дії характеризують також і невійськову сферу протиборства, оскільки гібридна війна – це збройний конфлікт, який здійснюється поєднанням невійськових та військових засобів з їхнім синергетичним ефектом. Загалом слід зазначити, що гібридна війна все ж таки не тотожна поняттю «асиметрична війна» і має більш складний характер.

В умовах гібридної війни Росії проти України особливо важливим завданням є вибір стратегічних партнерів і союзників, спираючись на допомогу яких можна забезпечити успішну протидію агресії Кремля. Для виживання і тим більше перемоги нашої країни у довгостроковій гібридній війні Україна повинна посилювати безпекові та оборонні спроможності, забезпечувати для цього розвиток економіки та залучати допомогу міжнародного співтовариства. Як слабша сторона конфлікту Україна максимально зацікавлена в інтернаціоналізації [6].

Аналіз досвіду ведення певними державами та підконтрольними їм недержавними суб'єктами показує, що гібридна війна є загрозою державному суверенітету, територіальній цілісності та безпеці держав, насамперед тих, які проводять незалежний від Росії та її союзників політичний курс, не приймає їхню гегемонію, роль старшого брата.

Вертикальна ескалація агресії проти суверенних держав, спрямованої на дезорганізацію системи державного та військового управління, економіки, соціальних інститутів, повалення легітимного правлячого керівництва методами збройного вторгнення, брехливої масованої пропаганди, підтримки внутрішньої проросійської опозиції та екстремістів усіх мастей, розпалювання міжконфесійної ворожнечі, реалізації

терористичних акцій, ракетних обстрілів критичної інфраструктури та цивільного населення, державних переворотів, громадянської війни, кібератак, відбувається з подальшим проведенням спеціальної воєнної операції на межі війни та миру з використанням високоточних авіаційних та ракетних ударів, сил спеціального призначення, збройних формувань недержавних суб'єктів з метою встановлення влади маріонеткового уряду та забезпечення геополітичного контролю за територією та ресурсами України. Сутність недержавних засобів гібридної війни втілюється в екстремістській та терористичній агресії проросійських політичних сил, їхніх незаконних збройних формувань та несилових компонентів, що підтримуються ззовні зацікавленими неоімперськими та мілітаристськими державами проти конституційного ладу, легітимних ідеологічних цілей і політичних програм, непідконтрольних Кремлю.

Гібридна війна – це доволі нове поняття, що виникло у нашому столітті. Це війна, яка поєднує принципово різні типи та способи її ведення, що скоординовано застосовуються задля досягнення поставлених цілей. При цьому сторона-агресор може офіційно не оголошувати війну та намагатися публічно залишатися непричетною до розв'язаного нею конфлікту.

Типовим для гібридної війни є використання як класичних прийомів ведення бойових дій (застосування регулярних підрозділів збройних сил, сучасного озброєння та військової техніки), так і нерегулярних збройних формувань (терористів, диверсантів, партизан, провокаторів тощо), а також інших форм і методів нанесення противнику суттєвих втрат – економічних, енергетичних, екологічних у поєднанні із застосуванням потужних інформаційних та кібернетичних атак. Інакше кажучи, цей спектр достатньо широкий, починаючи від керованого кривавого терору і диверсій та завершуючи фінансуванням брудних інформаційних кампаній і радикальних політичних проєктів. Мета у гібридної війни одна – поєднуючи зовнішню агресію та внутрішню дестабілізацію, знищити противника або примусити його до прийняття необхідних агресору рішень [7, 8].

Політики, керівництво Росії відкрито висловлюють наміри знищити Україну або анексувати її окремі, насамперед прикордонні регіони, заохочуючи та використовуючи внутрішні сепаратистські сили і настрої.

Так, у 2016 р. Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу», а депутати Європарламенту ухвалили Резолюцію «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін», у якій містяться положення про співпрацю з НАТО у протидії ворожій Євросоюзу пропаганді [9].

Сучасні конфлікти вже не потребують суворого розмежування військових і невійськових зусиль, концентрації великих сил воюючих сторін. Вони здебільшого навіть формально не оголошуються. Натомість такі протистояння характеризуються неоголошенням війни, гібридними операціями, у яких поєднуються воєнні та невоєнні дії, і невеликими силами, які точково націлюються на критичну інфраструктуру противника [10]. Водночас сучасна війна сфокусована на розвідці і домінуванні в інформаційному просторі. Характерно, що у моделі для сучасної російської війни «Роль невійськових методів у резолюції міждержавних конфліктів» саме тривала інформаційна кампанія є основою насильницького впровадження інтересів Росії за кордоном, а силовому ресурсу відводиться лише підсилююча, допоміжна роль на окремих етапах війни [11].

Слід зазначити ще один важливий рівень проблеми – Росія застосовує інформаційно-пропагандистський ресурс не точково, така диверсифікація дає змогу їй маскувати свої дійсні цілі, а часто – вирішувати завдяки комплексній інформаційно-пропагандистській кампанії низку завдань як на близьку, так і на більш віддалену перспективу. Комплексною ж метою російських інформаційних операцій є зміна стратегічної ситуації у Європі, яка відновить її позиції як глобального гравця на рівні із сучасними США, Китаєм та ЄС.

Так, у період 2000 – 2010 рр. Росія провела серію взаємопов'язаних кампаній, де пропаганда була одним із ключових ресурсів, на рівні із політичними (політична воля вищого державного керівництва, легітимована інститутами парламенту, Конституційного Суду, російською православною церквою та ЗМІ) і силовими (насамперед військова розвідка, яка здійснювала оперативний контроль за ситуацією через угрупування місцевих комбатантів). Такими стали операції у Криму, на Донбасі, у країнах Балтії, Молдові, Грузії, Білорусі. Водночас на більш глобальному, стратегічному рівні цілями Росії є навіть не анексія окремих територій малих пострадянських країн чи політико-економічний тиск на них з метою досягнення певних преференцій, а створення і використання

розломів серед країн західного блоку, делегітимація НАТО та ослаблення ЄС.

Як визначив Е. Вільсон, професор українських досліджень Школи слов'янських та східноєвропейських досліджень Університетського коледжу Лондона, інформаційно-пропагандистська складова виконує чотири взаємопов'язані завдання:

– відволікає та дезорієнтує західну аудиторію;

– підсилює вже сформовану громадську думку;

– мобілізує проросійську аудиторію;

– формує «альтернативну дійсність».

При цьому інструментами для реалізації окреслених вище завдань є російські державні та проросійські недержавні ЗМІ, «фабрики тролів», маріонеточні громадянські асоціації (особливо вагомими вони є у зонах затяжних конфліктів, як-от Придністров'я, Крим, Донбас, Абхазія, Північна Осетія, Нагірний Карабах, Північний Кавказ, Північний Кіпр, Сирія), російська православна церква.

Додатковими інструментами є фінансові ресурси, через які підтримуються політичні і партійні групи за кордоном, особливо активно – у Європі, причому не лише проросійського спрямування, але й у цілому спроможні дестабілізувати наявні політичні системи. Наприклад, угорські «Jobbik Magyarországért Mozgalom», «Fidesz – Magyar Polgári Szövetség», британські «United Kingdom Independence Party, UKIP», «British National Party, BNP», грецькі «Λαϊκός Σύνδεσμος – Χρυσή Αυγή», «ΣΥΡΙΖΑ», німецькі «Alternative für Deutschland, AfD», «Patriotische Europäer gegen die Islamisierung des Abendlandes», болгарська «Атака», французька «Rassemblement national», фракція «Europe of Nations and Freedom» у Європарламенті. В основі дискурсів, які проводяться через пропагандистські канали, лежать політизована історія, питання національних розбратів, мовної і релігійної належності, культивування символічних статусів історичної спадщини російського та радянського минулого [12].

У той час, коли у Росії формувалася доктрина новітньої війни, в Україні головні акценти інформаційної політики було сконцентровано на стратегіях побудови нового громадянського суспільства та інтеграції України до євроспільноти, що, на жаль, не дозволило вчасно й ефективно протидіяти агресії у 2014 р.

Так, проаналізувавши контент аналітичних матеріалів Інституту стратегічних досліджень у розділі «Інформаційна політика» за 2010–2013 рр. [13], зазначимо, що головними їх темами були: розвиток електронної демократії; інформаційна політика з питань євроінтеграції; інформаційні технології як фактор суспільних перетворень; протидія кіберзлочинності та ін.

Підкреслимо, що «Стратегія забезпечення кібернетичної безпеки України» напередодні війни була лише у проєкті [14], тобто фактично бракувало готовності до застосування Збройних Сил України в умовах кібервійни. Також мали місце недостатні можливості для відбиття збройної агресії з урахуванням нових викликів і загроз в інформаційній сфері, недостатня захищеність інформаційної інфраструктури (зокрема військового та подвійного призначення) від реальних та потенційних кіберзагроз. Фактично не було системи підготовки кадрів у сфері кібербезпеки для потреб Збройних Сил України та інших складових сектору безпеки і оборони України.

Невідповідною вимогам часу була також і Доктрина інформаційної безпеки України від 2009 р. [15], у якій недооцінено ймовірність розв'язання проти України інформаційної війни та бракувало вимоги підготовки відповідних сил і засобів для протидії й оборони в інформаційній сфері.

Наслідками цих процесів стало те, що з початком російської агресії у 2014 р. Україна не змогла повноцінно протидіяти, передусім саме в інформаційній сфері. Наприклад, уже у ході анексії Кримського півострова росіяни провели потужну інформаційно-психологічну кампанію, завданнями якої були деморалізація та формування на рівні масової свідомості «зрадницьких настроїв», вербування формальних і неформальних лідерів, презентація викривленого медіа-бачення подій, що відбувалися, морально-психологічна підтримка населення з проросійськими настроями та моделювання спільного «щасливого майбутнього». Цільовими аудиторіями було визначено: персонал органів законодавчої, виконавчої та судової влади Автономної Республіки Крим, зокрема особовий склад Збройних Сил та правоохоронних органів України, а також проросійсько налаштоване та лояльне до російської влади населення Криму.

Було задіяно широкий спектр інформаційних каналів (традиційні та електронні ЗМІ, інтернет-ЗМІ, соціальні мережі) та методів інформаційно-психологічної боротьби. Як зазначено в аналітичному звіті «Щодо інформаційно-психологічної складової агресії російської федерації проти України (за результатами подій 1–2 березня 2014 року)»

[16], протидія з боку України виявилася украй слабкою: бездіяльні офіційні сайти ключових державних інститутів, недостатня активність основних медіа-ресурсів (наприклад, у проблемні дні 1–2 березня 2014 р. значна частина вітчизняних телеканалів не змінювала сітку мовлення, обмеживши лише двомовним банером «Єдина Україна!/Единая страна!»). Однією з поодиноких дієвих форм опору стала стрімка реакція громадських активістів, але її виявилось явно недостатньо для повноцінної протидії агресору.

Ситуація загострювалася також і тим, що в Україні у цілому з моменту її незалежності питання побудови системи інформаційної безпеки на рівні законодавчої влади майже не порушувалося. Зазнавши активної інформаційно-пропагандистської агресії, новосформований «революційний» політичний режим виявився практично недієздатним у цій сфері. Державні функції забезпечення інформаційної безпеки були розсіяні між низкою «конкуруючих» між собою міністерств і відомств, які у певних питаннях дублювали функції. Водночас недостатніми були загальна координація та моніторинг за системою забезпечення інформаційної безпеки. Як наслідок цих процесів, перші рішення у часи анексії Криму та деморалізації населення Східного Донбасу були вкрай примітивними, наприклад, обмеження трансляції російського телебачення.

Так, уже у березні 2014 р. в Україні було заборонено 5 російських телеканалів, а до грудня 2015 р. під забороною стало вже 25.

Надалі було впроваджено серію обмежувальних заходів на частку російськомовного продукту на українських телеканалах, а з березня 2015 р. на законодавчому рівні табуйовано перелік фільмів російсько-пропагандистського змісту.

Усвідомлення того, що проти України розпочата нова за своїм характером агресія, яка згодом буде означена як гібридна війна, примусило до вироблення основ побудов нової системи безпеки та оборони, у якій чільне місце було відведене саме питанням інформаційної безпеки.

Вже навесні 2014 р. загрози та виклики в інформаційно-психологічній сфері було віднесено до загроз національній безпеці України [17]. Розпочинається активне вивчення спроб протидії іноземній інформаційній агресії [18]. Переосмислюється пропаганда як інструмент інформаційних спецоперацій. Здійснюються спроби виробити дієві механізми контрпропаганди [19].

Із серпня 2014 р. розпочинається планомірна інституціоналізація системи забезпечення інформаційної безпеки. Причому однією з проблем тут стало намагання не допустити дії, які б надалі могли бути розцінені порушенням в Україні свободи слова як однієї із фундаментальних основ сучасної ліберальної демократії.

Так, у грудні 2014 р. створюється Міністерство інформаційної політики, розробляється Концепція інформаційної безпеки України, запускається низка патріотичних інформаційних кампаній, зокрема «Крим – це Україна», «Захищаючи Україну» та ін.

У жовтні 2015 р. за окремим законом вітчизняні телетранслюючі компанії були зобов'язані надати відкриту інформацію щодо їхніх власників та спонсорів.

Проте дієвість усіх цих заходів, як показали дослідження громадської думки тих часів, виявилась украй слабкою. Наприклад, за результатами опитувань Київського міжнародного інституту соціології, 42 % населення південної України були переконані, що події Майдану – це насильницьке захоплення влади; 28 % – що на сході України триває громадянська війна [20].

З 2016 р. перед українською владою постає нова проблема – реінтеграція у вітчизняне культурне та інформаційне середовище населення деокупованих та звільнених територій [21].

Пізніше, коли збройний конфлікт на сході України набув характеру позиційного із невисокою інтенсивністю, проблематика інформаційного протиборства поступово трансформувалась у забезпечення стійкості населення до деструктивних інформаційно-психологічних впливів, наприклад, на основі обміну досвідом формування державно-приватного партнерства у сфері кібербезпеки, упровадження медіаграмотності для окремих цільових груп тощо.

Труднощі, перед якими постала Україна за наслідком опору російській гібридній агресії, націлюють на пошук моделей дієвої протидії російській пропаганді в інших країнах. Такі, зокрема, сформовано у країнах Балтії.

Так, ще у 2007 р. у відповідь на демонтаж пам'ятника радянським воїнам Росія застосувала комбіновану атаку проти Естонії, поєднавши інформаційно-пропагандистський вплив, дипломатичний і торгово-економічний тиск,

потенціал місцевих громадсько-політичних груп, а також масивні кібератаки.

Зважаючи на це, Естонія обрала шлях, спрямований на:

– збільшення фінансування для створення збалансованих джерел інформації, які продукуючи «позитивні повідомлення», були б спроможні контрдіяти російським і проросійським медіа;

– створення EastStratCom Team – постійно діючого інформаційного підрозділу ЄС;

– підтримку свободи преси у країнах-учасниках «Східного партнерства»;

– забезпечення доступності своїх інформаційних матеріалів для російськомовної аудиторії [22].

Латвія, у якій проживає чимала кількість етнічно російського і російськомовного населення (до 26 % населення), з метою протидії наративам проросійських ЗМІ (насамперед, інформагентству RT) активно використовує підтримку Центру передового досвіду НАТО у сфері стратегічних комунікацій, який розміщено у Ризі. Характерно, що в ЄС існує аналогічний ресурс – Оперативна робоча група зі стратегічних комунікацій, до завдань якої входять висвітлення та розвінчання російської пропаганди.

За результатами аналізу подій в Естонії (2007 р.), Грузії (2008 р.) та в Україні узагальнимо таке.

1. Головним методом російської пропаганди у ситуації конфлікту є дезінформація. При цьому об'єкти агресії засуджуються з метою їх дискредитації в очах як російської, так і зовнішньої аудиторії.

2. Інформаційно-пропагандистські канали містять увесь наявний спектр засобів масової комунікації: російські державні телеканали, проросійські медіа на території країни-об'єкта агресії, онлайн-медіа, веб-ресурси (наприклад, LiveJournal, Liveinternet), масштабний інтернет-тролінг у соціальних мережах, інформаційні канали сепаратистських асоціацій, навіть мережі мобільних операторів.

3. На інформаційно-пропагандистський супровід Росія витрачає величезні фінансові ресурси, неспівмірні з можливостями малих постраждянських країн.

Корисними для України можуть стати також заходи, рекомендовані для європейських країн, у внутрішньополітичному житті яких періодично простежується російський слід [23]:

– відслідковувати вплив російської пропаганди на громадську думку;

– деконструювати та оприлюднювати факти російських інформаційно-пропагандистських акцій;

– підвищувати рівень інформаційної компетентності своїх громадян;

– спростовувати і роз'яснювати основні пропагандистські тези;

– більш активно інституціювати «інформаційну безпеку».

Тут варто ще раз обумовити, що в цілому інформаційно-пропагандистська кампанія, яку проводить Росія упродовж останніх десятиліть, спрямовується крім безпосередніх об'єктів, також проти усього консорціуму провідних країн західного світу та їхніх основних асоціацій – ЄС та НАТО. При цьому дискурс пропаганди часто переплітається у дивні химери, коли, наприклад, донбаський сепаратизм подається ледь не історично обумовленим сепаратизмом іспанських басків чи ольстерських ірландців, питання захисту російськомовного населення узгоджуються із питаннями захисту прав і свобод у Західній Європі. Водночас такий дискурс підсилюється адресними інформаційними атаками щодо проблем, зумовлених міграцією у Німеччині, процесами Brexit, хибами виборчих перегонів у США тощо.

Звісно, станом на сьогодні напрацьовано вже чималий західний досвід протидії російській пропаганді та дезінформації. Зокрема, для України вкрай корисними можуть стати: «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» [24] – узгоджувальний акт держав-членів ЄС із протидії гібридним загрозам, зокрема інформаційного характеру; резолюція Європарламенту «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» [25], що ґрунтується на Action Plan on Strategic Communication та у якій презентовано основні аспекти інформаційно-пропагандистської діяльності РФ.

Не менш важливо підтримувати тісні зв'язки з Оперативною робочою групою ЄС зі стратегічних комунікацій (East Strat Com Task Force) – зовнішньополітичною службою ЄС, серед основних завдань якої визначено протидію дезінформації та надання інформаційної підтримки низці постраждянських країн, серед яких і Україна. Важливо відмітити, що інформаційно-аналітичний ресурс відомства – uvsdisinfo.eu – є доволі дієвим інструментом контрпропаганди, вітчизняними аналогами якого можна вважати [26] та інші.

Висновки

За результатами проведеного аналізу можемо вважати підтвердженими такі висновки: готуючись та здійснюючи акт воєнно-політичної агресії проти України, Російська Федерація застосувала модернізований стратегічний підхід, у межах якого інформаційно-пропагандистська складова мала одну із домінуючих позицій; на момент початку гібридної агресії проти державного суверенітету та територіальної цілісності Україна не була готовою до масованої інформаційно-пропагандистської атаки як складової воєнного конфлікту нового покоління; застосовувані Україною контрзаходи в інформаційній сфері виявилися недостатніми через відсутність подібного досвіду, підготовленого особового складу та належних ресурсів, застарілість інформаційної інфраструктури і несистематизовані дії під час забезпечення інформаційної безпеки; за умов, коли головною особливістю воєнно-політичної кампанії Росії проти України була саме її інформаційно-пропагандистська складова, системна неготовність України до опору пропаганді стала однією з основних передумов початку російської агресії та еволюції до збройного конфлікту.

Разом з тим розвинутими демократичними країнами, які мали досвід протидії російській пропаганді, накопичено апробований арсенал ефективних форм і організаційно-технічних заходів, які можуть бути використані в інтересах побудови національної системи забезпечення інформаційної безпеки як однієї зі складових беспеки державного кордону. Водночас імплементація цього досвіду має відбуватися з урахуванням двох важливих застережень: запозичення досвіду не має стати «сліпим» копіюванням, адже слід враховувати культурно-історичні, інституційні та інші реалії сучасного стану в Україні; російська пропаганда швидко еволюціонує у своїх формах і технологіях, має суттєві ресурси, які на неї спрямовуються, через що потребує регулярного моніторингу й аудиту дієвості сценаріїв контрпропаганди розвинутих демократичних країн.

Перспективами подальшого дослідження є визначення критеріїв оцінювання рівня негативного інформаційного впливу на військовополоненого з боку ворога, а також дослідження шляхів протидії негативному інформаційному впливу на особовий склад у полоні противника**.**

Перелік джерел посилання

1. Про Державну прикордонну службу України : Закон України від 03.04.2003 р. № 661-IV. *Відомості Верховної Ради України*. 2003. № 27. Ст. 208.

2. Машовець М. К. Гібридна війна росії – виклик і загроза для Європи. Київ, 2016. 88 с. URL: https://bit.ly/3ppWeBd (дата звернення: 21.04.2023).

3. Литвиненко О. Тотальна війна по-путінські: «гібридна» війна рф проти України. «Гібридна» війна росії – виклик і загроза для Європи / Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. URL: https://bit.ly/3ik9IwV (дата звернення: 21.04.2023).

4. Турчинов О. Т. Тероризм. Гібридна війна. Росія. URL: http://surl.li/krmbr (дата звернення: 21.04.2023).

5. Лещенко О. Я. Трансформація системи цивільного захисту України в умовах сучасних воєнно-політичних конфліктів гібридного типу : монографія. Київ : Державний видавничий центр «Україна», 2020. С. 293.

6. Європейський інформаційно-дослідницький центр. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. Інформаційна довідка, підготовлена на запит народного депутата України. URL: http://surl.li/krmbz (дата звернення: 21.04.2023).

7. Демський В. В., Юрчак Ю. М. Проблема захисту від негативного інформаційно-психологічного впливу на персонал відділу охорони державного кордону в контексті інформаційної війни. *Збірник наукових праць Національної академії Державної прикордонної служби України. Психологічні науки.* Хмельницький : НА ДПСУ, 2019. Вип. 1 (12). С. 83–94.

8. Демський В. В., Юрчак Ю. М. Особливості впровадження методики протидії негативному інформаційно-психологічному впливу на особовий склад Могилів-Подільського прикордонного загону. *Збірник наукових праць Національної академії Державної прикордонної служби України. Психологічні науки.* Хмельницький : НА ДПСУ, 2019. Вип. 3 (14). С. 91–106.

9. Купрієнко В. Д. Рекомендації суб'єктам забезпечення прикордонної безпеки щодо стратегічного управління організаційним потенціалом прикордоння. *Збірник наукових праць Національної академії Державної прикордонної служби України. Військові та*

технічні науки. Хмельницький : НА ДПСУ, 2016. Вип. 1(67). С. 142.

10. Torichnyi V., Biletska T., Rybshchun O., Kupriyenko D., Ivashkov Y., & Bratko A. Information and propaganda component of the Russian Federation hybrid aggression: Conclusions for developed democratic countries on the experience of Ukraine. TRAMES. 2021. 25 (75/70). 3. 000–00. DOI:10.3176/tr.2021.75.02.

11. Маркітантов В., Рибщун О., Столяр Ю. Російська гібридна війна: від доктрини до тактики : навч. посіб. Кам'янець-Подільський : Друкарня «Рута», 2018. 234 с.

12. Херд Г. Гибридный конфликт 2.0. Атака на Запад. *Per Concordiam*. 2016. С. 6–15.

13. Інститут стратегічних досліджень. Інформаційна політика. URL: http://surl.li/krmci (дата звернення: 21.04.2023).

14. Стратегія забезпечення кібернетичної безпеки України. URL: http://surl.li/krmcq (дата звернення: 21.04.2023).

15. Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47. URL: http://surl.li/krmcu (дата звернення: 21.04.2023).

16. Щодо інформаційно-психологічної складової агресії російської федерації проти України (за результатами подій 1-2 березня 2014 року). Аналітична записка. URL: http://surl.li/krmcy (дата звернення: 21.04.2023).

17. Щодо окремих напрямів вдосконалення державної інформаційної політики України. Аналітична записка. URL: http://surl.li/krmdn (дата звернення: 21.04.2023).

18. Еволюція іномовлення в іноземних державах: досвід для України. Аналітична записка. URL: http://surl.li/krmdt (дата звернення: 21.04.2023).

19. Пропаганда, спрямована на розпалювання національної та міжнаціональної ворожнечі: проблеми визначення та протидії. Аналітична записка. URL: http://surl.li/krmed (дата звернення: 21.04.2023).

20. Шутов Р. Російська пропаганда в Україні: Києву не вистачить інструментів для боротьби з фантомами, народженими москвою. Per Concordiam. 2016. С. 37, 38.

21. Зрозуміла мова. Plain language у забезпечення комунікативного зв'язку. Влада – громадськість на окупованих та звільнених територіях. URL: http://surl.li/krmek (дата звернення: 21.04.2023).

22. Вейбел В. Росія маніпулює ЗМІ як засобом психологічної війни. *Per Concordiam*. 2016. С. 14–19.

23. Смоленова І. Компанія з проросійської дезінформації в Чехії та Словаччині. *Per Concordiam*. 2016. С. 26–29.

24. Joint Framework on countering hybrid threats a European Union response. URL: http://bit.ly/2t0ywSh (Accessed: 21.04.2023).

25. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. URL: http://surl.li/krmex (Accessed: 21.04.2023).

26. Новини та аналітика України. URL: http://surl.li/krmfg (дата звернення: 21.04.2023).

Стаття надійшла до редакції 12.06.2023 р.

UDC 355.01:355/359.08:32.019.57

Yu. Yurchak

SCIENTIFIC AND PRAGMATIC ASPECTS OF HYBRID WARFARE

The article explores the peculiarities of the scientific-pragmatic aspects of hybrid warfare. The phenomenon of "hybrid warfare" is considered as a scientific problem, and the development of the theory of hybrid warfare and military-theoretical approaches to its essence are discussed. The necessity to enhance Ukraine's national security system was substantiated, taking into account the specificities of the State Border Guard Service of Ukraine. Various approaches to defining hybrid warfare were examined, elucidating the essence and common features of hybrid warfare, while analyzing the problematic issues of protecting national interests at the state border. The unfounded nature of the implementation of "hybrid aggression" by the Russian Federation against Ukraine is emphasized, and an analysis of the characteristics of "hybrid warfare" is provided. It is concluded that "hybrid warfare" is a new instrument of aggression by neo-imperial totalitarian states aimed at sovereign states that oppose Russian hegemony in the post-Soviet territories. The necessity of improving the system for ensuring the national security of Ukraine, taking into account the specifics

of the State Border Guard Service of Ukraine, is justified. The article is devoted to studying individual approaches to defining "hybrid warfare"; the essence and general features of "hybrid warfare" are determined; and problematic issues of protecting national interests at the state border are analyzed.

Keywords: *hybrid warfare, national security, State Border Guard Service of Ukraine, armed aggression.*

Юрчак Юрій Миколайович – викладач кафедри загальновійськових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького

https://orcid.org/0000-0002-9506-3228