СОЦІАЛЬНІ КОМУНІКАЦІЇ

УДК 316.6:659.9]:004.7

О.В. Курбан

СУЧАСНА ГІБРИДНА ВІЙНА ТА ЇЇ ІНФОРМАЦІЙНА СКЛАДОВА

Мета роботи. *Дослідження, пов'язане з вивченням інноваційних засобів і методів ведення сучасної гібридної війни в контексті інформаційних технологій, зокрема соціальних онлайнових мереж. Специфіка сучасних інноваційних конфліктів вимагає активного використання інформаційних, зокрема, інтернет-технологій, що застосовують у політичних, економічних та політичних війнах.* ***Методологія*** *дослідження полягає в застосуванні таких загальнонаукових методів, як: синтез, аналіз, порівняння, а також прикладних: моделювання та прогнозування. Зазначений методологічний підхід дозволяє напрацювати практичні шляхи та визначити напрями подальших науково-теоретичних розвідок щодо запровадження інноваційних мережевих технологій у галузі інформаційних війн зокрема та гібридної в цілому.* ***Наукова новизна*** *роботи полягає в розширенні можливостей прикладного та науково-теоретичного дослідження інноваційних мережевих технологій. Практичне застосування зазначених технологій відкриє нові можливості роботи з інформацією та визначить ефективні інструменти управління комунікаційними процесами в рамках гібридних та інформаційних війн.* ***Висновки.*** *Розробка відповідних управлінських алгоритмів та адаптацій їх до реалій сьогодення, зокрема мережевих інформаційних війн, нових методів та засобів управління інформаційними потоками має пріоритетне значення на теперішньому етапі розвитку практики ведення гібридних конфліктів економічного, політичного та військового характеру. Визначення прикладних та науково-теоретичних напрямів досліджень у цьому контексті є найближчим завданням для представників профільних наукових дисциплін.*

Ключові слова: *гібридна війна, соціальні онлайнові мережі, інформаційна війна.*

А.В. Курбан

СОВРЕМЕННАЯ ГИБРИДНАЯ ВОЙНА И ЕЕ ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ

Цель работы. *Исследование связано с изучением инновационных средств и методов ведения современной гибридной войны в контексте информационных технологий, в частности социальных онлайн-сетей. Специфика современных инновационных конфликтов требует активного использования информационных, в частности, интернет-технологий, которые применяют в политических, экономических и политических войнах.* ***Методология*** *исследования заключается в применении таких общенаучных методов, как: синтез, анализ, сравнение, а также прикладных: моделирование и прогнозирование. Указанный методологический подход позволяет выработать практические пути и определить направления дальнейших научно-теоретических исследований по внедрению инновационных сетевых технологий в области информационных войн в частности и гибридной в целом.* ***Научная новизна работы*** *заключается в расширении возможностей прикладного и научно-теоретического исследования инновационных сетевых технологий. Практическое применение указанных технологий откроет новые возможности работы с информацией и определит эффективные инструменты управления коммуникационными процессами в рамках гибридных и информационных войн.* ***Выводы.*** *Разработка соответствующих управленческих алгоритмов и адаптаций их к реалиям сегодняшнего дня, в частности сетевых информационных войн, новых методов и средств управления информационными потоками имеет приоритетное значение на нынешнем этапе развития практики ведения гибридных конфликтов экономического, политического и военного характера. Определение*

прикладных и научно-теоретических направлений исследований в этом контексте − ближайшая задача для представителей профильных дисциплин.

Ключевые слова: *гибридная война, социальные онлайн сети, информационная война.*

O.V. Kurban

MODERN WAR AND ITS HYBRID COMPONENT INFORMATION

The purpose of the work. *Research related to the study of innovative means and methods of modern hybrid war in the context of information technology and in particular onlany social networks. Specificity and innovative features of modern conflicts requires active use of information and particularly Internet technology that is accompanying political, economic, and political wars.* ***Research methodology*** *is to apply scientific methods such as: synthesis, analysis, comparison and application: modeling and forecasting. The above methodological approach allows us to work out practical ways and identify areas for further research and theoretical investigations concerning the introduction of innovative network technologies in information warfare and particularly hybrid war overall.* ***The scientific novelty*** *of the work is to empower and applied scientific and theoretical research of innovative network technologies. Practical application of these technologies open up new possibilities of information and identify effective tools of communication processes within the hybrid and information warfare.* ***Conclusions.*** *Development of appropriate management algorithms and their adaptation to the realities of the present, including the network of information warfare, new methods and tools for information management is a priority at the current stage of the conflict hybrid practices of economic, political and military. Definitions applied and theoretical scientific research areas in this context, the immediate task for representatives of relevant disciplines.*

Keywords: *hybrid warfare, online social networks, the information war.*

Актуальність. Трансформація технологій, специфіка соціальних, економічних та політичних умов розвитку сучасного світового співтовариства впливають на специфіку ведення сучасних війн. Провідні країни світу виділяють сьогодні на оборону значні бюджетні кошти, що дозволяє їм отримувати мільйонні армії, мати найсучаснішу зброю, зокрема таку, що належить до категорії зброї масового знищення. У цих умовах конфлікт двох або кількох таких країн, пов'язаних з іншими подібними країнами різними угодами та союзами, може автоматично перетворитися на глобальну війну і, можливо, навіть із застосування ядерної зброї. У таких умовах виникає потреба пошуку більш безпечного засобу вирішення конфліктних ситуацій, що не призведе до негативних глобальних наслідків. Таким засобом стала гібридна війна, що являє собою комбіноване, інтегроване військово-політичне та економічне протистояння у вигляді безстатусного, часто прихованого конфлікту.

Мета статті. Актуальність та затребуваність інноваційних методів ведення військових, політичних, економічних, інформаційних та культурних протистоянь вимагає системного дослідження теорії та практики сучасної гібридної війни. Саме висвітлення певних аспектів цього питання є метою статті.

У форматі реалізації зазначеної мети, *завданнями статті* є:

1. Розглянути історіографічний аспект теми.
2. Проаналізувати практику ведення гібридних війн провідними країнами світу.
3. Дослідити складові частини та етапність реалізації гібридних конфліктів.
4. Розглянути інформаційну складову сучасної інформаційної війни.

В США поняття гібридної війни запровадив Ф. Гофман, визначивши її як військові конфлікти, що поєднують у собі летальний характер державних конфліктів із фанатичним і тривалим запалом нерегулярної війни [9].

Значні методологічні напрацювання за досліджуваною тематикою запропонував радник міністра оборони США, Н. Фрейєр, який визначив ключові види нетрадиційної війни, зокрема й мережеву [14].

Питанням мережевої складової сучасної гібридної війни присвятив свої роботи, зо-

крема книгу «Соціальні мережі та мережеві війни», Е. Акрила [13].

Однією з провідних країн, яка активно використовує сьогодні інструменти гібридної війни, є Росія. Узагальнивши досвід гібридних конфліктів кінця XX – початку XXI ст., які вели США, провідні країни ЄС та азійського регіону, профільні російські фахівці розробили нову концепцію таких війн і застосували її на практиці проти своїх сусідів, намагаючись боротися за відновлення системи двополярного світу, який існував за часів СРСР (холодної війни).

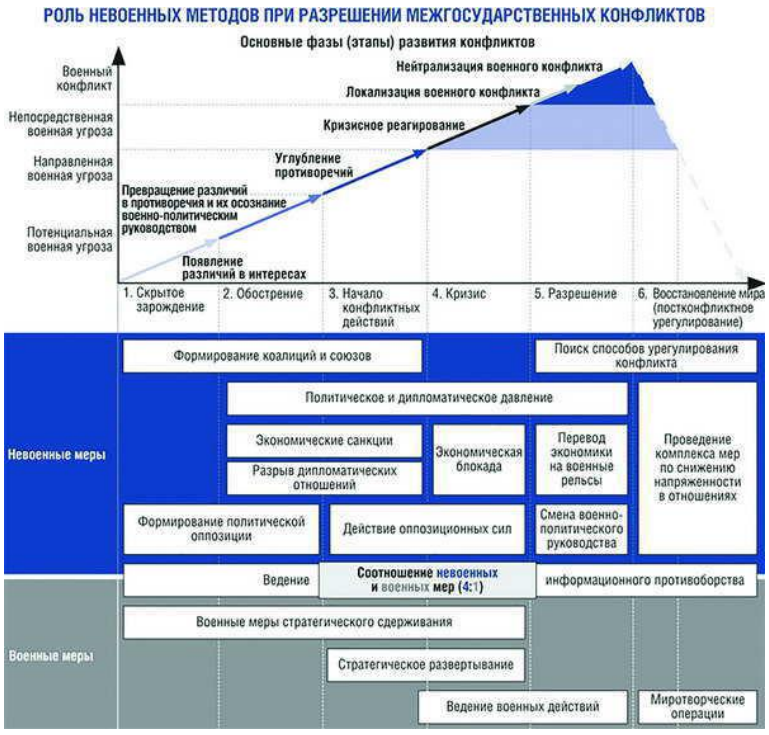
Одним із перших питання нетрадиційних, гібридних або асиметричних засобів ведення війни почав ще за радянських часів досліджувати Г. Іссерсон. Свої напрацювання він виклав у книзі «Нові форми боротьби» (1940 р.). Зокрема, він пропонував приховані методи мобілізації, здійснення прихованих атакуючих дій, партизанський рух та діяльність громадсько-політичних організацій, які легітимізують певні атакуючі дії [4].

Також значний внесок у справу вивчення та розробки управлінських рішень у гібридній війні зробив інший радянський військовий теоретик Є. Месснер. Цей дослідник робив головний акцент у сучасних військових конфліктах на захопленні не територій, а свідомості населення протилежної сторони [7].

В Україні дослідженням питань гібридної війни присвячували свої роботи В. Горбулін, Г. Почепцов, Є. Магда [3; 9; 6].

Базові складові частини російської стратегії і тактики сучасної гібридної війни сформулюють у 2013 р. начальник генерального штабу ВС РФ В. Герасимов *(мал.1)* [10].

Саме на основі цих принципів було сплановано та реалізовано напад на Україну, захоплення Криму та розв'язання війни на Донбасі. Серед ключових складових російської концепції зазначалися збільшення ролі невійськових методів тиску на противника, насамперед, за допомогою політичних (дипломатичних), економічних і гуманітарних елементів. Що стосується інформаційної складової, то вона визначалася як основа діяльності на всіх етапах конфлікту: його зародження, супроводу і в постконфліктний період. Особлива увага в концепції відводиться й «асиметричним заходам», до яких були віднесені: діяльність підрозділів спеціального призначення; підтримка внутрішньої опозиції і колабораціоністів, а також збільшення цілеспрямованого інформаційного впливу на об'єкт нападу.



Мал.1. ***Схема гібридної війни (російське бачення)***

Послідовними, типовими складовими етапами гібридної війни в концепції було визначено такі [10]:

– ***інноваційна агресія*** (кібервійна, економічний тиск, інформаційно-психологічні атаки тощо);

– ***застосування нерегулярних збройних формувань, або приватних армій*** (повстанський, партизанський рух, тероризм);

– ***офіційні військові дії, або демонстрація сили*** (ідентифікована уніформа, зброя, офіційне визнання участі у конфлікті).

Перший етап гібридної війни починається з ***інноваційних агресій,*** які зазвичай мають ***прихований характер***.

Аналізуючи перебіг багатьох гібридних конфліктів, зауважимо, що іноді доволі складно виявити й ідентифікувати приховану економічну атаку, яка може бути замаскованою під виглядом конкуренції та боротьби за лідерство між країнами та транснаціональними корпораціями в окремих секторах або галузях економіки. Так само не завжди у просуванні національної культури однієї країни на терени іншої можна простежити акт агресії. Схожа ситуація має місце й у просуванні ЗМІ, які здійснюють боротьбу за цільові аудиторії та зони впливу, що можуть поширюватися на сусідні держави та навіть окремі континенти.

Навіть у разі можливості відстеження зазначених тенденцій украй важко обґрунтувати й довести звинувачення та змусити опонента припинити агресивні дії. До цього залучаються міжнародні третейські інституції, присуди яких виносяться роками та мають нечіткі рішення. Крім того, процедура ухвалення рішень такими структурами є доволі тривалою, тоді як гібридні атаки здійснюються швидко.

Етап інноваційної агресії іноді може бути розтягненим на роки і десятиліття. Класичним прикладом цьому може бути така агресія Росії проти України. Типовими ознаками її були газові й торговельні війни, намагання захопити стратегічні підприємства, поширити вплив власних ЗМІ, тиск на політичному рівні в питаннях захисту прав російськомовного населення, просуванні елементів російської культури (кіно, література, твори мистецтва тощо).

Саме на цьому етапі відбувається закладання конкретних масових психологічних установок, які згодом, у моменти переходу конфлікту до відкритої фази, використовують для послаблення сторони, проти якої здійснюється агресія.

Другий етап гібридної війни набуває характеру певної відкритості, з якого вже стає зрозумілим, хто є ініціатором агресії, утім формулювати обвинувачення доволі складно, бо атакуюча сторона не розкриває остаточно своїх карт.

На цьому етапі головними засобами здійснення гібридної агресії є:

− створення атмосфери бездуховності, накручування конфліктних ситуацій, знищення авторитету державної влади;

− дестабілізація політичної ситуації (конфлікти, репресії, терор);

− блокування інформаційної діяльності органів центральної влади та місцевого самоврядування;

− підрив авторитету та дискредитація органів державної влади усіх рівнів;

− провокування соціальних, політичних, національних, релігійних зіткнень – аж до розв'язання громадянської війни;

− ініціювання масових протестних акцій і безладів на вулицях, погромів офіційних установ та громадських структур.

Фактично всі представлені вище засоби були випробувані російською стороною під час захоплення Криму, розпалювання війни на Донбасі та дестабілізації ситуації в середині України з кінця 2013 р. і дотепер.

Характерною ознакою другого етапу є застосування ***нерегулярних збройних формувань, або приватних армій,*** які діють під виглядом партизанських груп, повстанських об'єднань або терористичних організацій.

У більшості випадків на другому етапі держава-агресор може виказати себе через:

− офіційну політичну підтримку сепаратистських рухів на рівні публічних заяв чи шляхом відстоювання інтересів повстанців у міжнародних установах;

− надання матеріально-технічної допомоги у вигляді техніки, зброї, продуктів харчування, коштів та інших ресурсів.

На цьому етапі держава-агресор у боротьбі з противником спирається вже не тільки на окремих інсайдерів і певні групи впливу в се-

редині країни, проти якої здійснює агресію, але й починає застосовувати власні закамуфльовані війська або залучає приватні армії. У війні, яку розпалила Росія на Сході України, були ідентифіковані такі угруповання [8]:

1. Козаки (щось середнє між поліцією і солдатами).

2. Військовослужбовці регулярної армії («зелені чоловічки»).

3. Чеченські найманці (підрозділи, створені А. Кадировим).

4. Інші найманці (представники арабських країн та деяких країн ЄС).

5. Колишні співробітники «Беркута» (розформований спецпідрозділ МВС України).

6. Місцеві етнічні росіяни, що живуть в Україні.

8. Російські «туристи» (колишні військовослужбовці, що діють як найманці).

9. Реальні актори (використовують з метою пропаганди або навмисно шукають західні камери, щоб розіграти драматичну роль і викласти свою порцію фальсифікації).

10. Колишні українські солдати й офіцери (дезертирували з української армії чи служать в ній, але є зрадниками/шпигунами).

11. Місцевий криміналітет, що пройшов військлву підготовку й отримав зброю.

13. Місцеві жителі, які були змушені воювати (через гроші, примус або під впливом пропаганди).

14. Російські кримінальники або ув'язнені, що потрапили під амністію в обмін на найманство для війни в Україні.

16. Агенти ФСБ.

17. Російські генерали та вищий офіцерський склад, що «координують припинення вогню» на українській стороні фронту.

18. Іноземні журналісти, що збирають цінну інформацію та створюють негативні сюжети про Україну.

Щоб зрозуміти, що сьогодні являють собою типові приватні армії, треба проаналізувати діяльність потужних транснаціональних корпорацій, які для захисту своїх економічних інтересів залучають до співпраці певні незалежні озброєні групи або створюють власні формування.

Традиційно такі військові групи визначають як ***приватні військові компанії*** (далі – ПВК) – комерційні підприємства, що пропонують послуги, пов'язані з охороною, захистом певних об'єктів або персон. Доволі часто вони беруть активну участь у збройних конфліктах, а також здійснюють збирання розвідувальних даних, надають послуги зі стратегічного планування, логістики та консультують [5].

У квітні 2001 р. була створена міжнародна організація Peace Operations Association, головним завданням якої є координація та представництво інтересів усіх її членів на різних рівнях. Після початку війни в Іраку було створено Private Security Company Association of Iraq – асоціацію приватних військових та охоронних компаній, що контролювали ситуацію в цій країні. До складу зазначеної структури увійшло понад 40 компаній [11, 74].

Серед прикладів типових послуг, які надають приватні армії, є такі, як [2, 348]:

− набір особового складу для контингенту міжнародних поліцейських місій та управління ними (DynCorp);

− захист об'єктів, зокрема тих, що мають важливе стратегічне значення (наприклад, DynCorp забезпечувала охорону стратегічно важливого нафтового резерву США);

− охорона нафтових родовищ і трубопроводів, енергетичної системи (Hart Group, Blackwater Security Consulting, Erinys Iraq Limited);

− захист посольств і керівників держави (Triple Canopy);

− супроводження конвоїв ООН (Kroll);

− навчання особового складу урядових збройних сил, поліції та інших сил безпеки (наприклад, у лютому 2002 р. 70 співробітників ізраїльської компанії Levdan займалися навчанням збройних сил Конго);

− надання послуг військових перекладачів (CACI);

− охорона в'язниць (Titan Corporation);

− розмінування мінних полів і знищення боєприпасів (RONCO, MAG, BACTEC, Armor Group, Minetech, EODT);

− протипожежний захист (Group 4 Falck);

− тилове постачання військ (KBR);

− авіарозвідка (AirScans Inc., Eagle Aviation Services & Technology);

− збройний супровід і захист морських суден від піратів (Global Marine Security Systems).

Варто зазначити, що поступово роль і значення ПВК зростає. Приміром, станом на 2007 р. близько 25% усіх розвідувальних операцій для силових структур США забезпечували саме такі структури [2, 355].

У західних країнах діяльність таких приватних військових формувань суворо регламентується законом та контролюється. Сьогодні у світі сформувався чітко структурований ринок військових послуг із загальним обсягом понад $100 млрд. Серед найбільш відомих нині є такі компанії, як: Hulliburton, Blackwater, DynCorp, Logicon, Brown&Root, MPRI, Control Risks, Bechtel, ArmorGroup, Erinys, Sandline International, International Defense and Security [2, 350].

На відміну від європейської та американської практики, у Росії специфіка діяльності таких організацій має дещо інший характер. Перші приватні армії з'явилися в Росії у 2007 р., у складі компаній «Транснефть» та «Газпром» [3], з метою захисту від зазіхань криміналітету. Втім згодом вони перетворилися на неформальні силові структури, що діють під прикриттям та за настановами ФСБ й особисто кремлівського керівництва. Формально вони регулюються профільними нормативно-правовими актами, але в реальності їх діяльність повністю контролює офіційна влада. Саме такі російські структури починали агресію на Донбасі та виконували допоміжні функції при захопленні Криму.

На **третьому етапі гібридної війни** боротьба фактично набуває відкритої форми і може перейти в офіційний збройний конфлікт.

Це здійснюється або у форматі відкритої інтервенції, або під виглядом введення миротворчих сил. В обох випадках головним офіційним приводом є намагання зупинити внутрішньо національні конфлікти або припинити неправомірні дії офіційної влади, що суперечать сучасним нормам і принципам захисту прав людини, встановленим і закріпленим у міжнародних угодах та деклараціях ООН, ЮНІСЕФ, Ради Європи та ін.

Маємо зазначити, що складні для офіційного контролю форми діяльності ПВК ідеально підходять для застосування у так званих ***гуманітарних інтервенціях***, що є типовою ознакою гібридної війни [2, 364]. Такі інтервенції визначають як примусові дії особливої форми, які застосовують міжнародна спільнота або окремі держави [2, 365].

Найбільш легітимним сьогодні для здійснення миротворчих операцій або камуфлювання під них вважається мандат Ради Безпеки ООН, який сприяє:

− розгортанню сил для запобігання конфлікту і його виходу через кордони;

− стабілізації конфліктної ситуації після припинення вогню;

− створенню умов для досягнення угоди про встановлення міцного миру між сторонами;

− здійсненню всеосяжних мирних угод;

− сприяння країнам чи територіям у подоланні перехідного періоду і створенні стабільного уряду на основі демократичних принципів, ефективного управління та економічного розвитку.

Слід зазначити, що саме наприкінці XX – на початку XXI ст. кількість таких гуманітарних інтервенцій зросла у рази, що можна пояснити такими факторами, як [2, 365]:

− зникнення біполярної конфронтації США та СРСР, яка ускладнювала діяльність Ради Безпеки ООН щодо питань санкціонування миротворчих операцій;

− різке зростання геополітичного впливу США та їхнє прагнення до встановлення власних правил гри на міжнародній арені;

− посилення тиску на слаборозвинуті країни, що володіють стратегічними ресурсами (газ, нафта та ін.) чи вигідним геополітичним положенням;

− наявність країн із антидемократичними режимами та терористичних організацій світового масштабу, з якими необхідно вести боротьбу;

− зміна норм міжнародного права щодо збільшення уваги до проблем захисту прав людини.

На відміну від загальновизнаного світовим співтовариством мандата на миротворчі операції, іноді країни-агресори намагаються використовувати квазімандати або локальні міждержавні угоди, під прикриттям яких здійснюють окупацію чужих територій. Саме так було, коли Росія використала своїх «миротворців» у Придністров'ї (1992 р.), Абхазії (1994 р.), Південній Осетії (2008 р.).

Специфіка сучасної гібридної війни стимулює створення нових форм військово-

політичної агресії, які мають усі необхідні формальності або забезпечуються ґрунтовним юридичним прикриттям. Саме так відбулося під час захоплення Криму. Анексія частини української території була легітимізована шляхом проведення народного референдуму − волевиявлення, яке контролювали та забезпечували сили спеціальних операцій ВС РФ [1].

Під час здійсненні російської агресії на Донбасі в 2014 р. кремлівське керівництво планувало застосувати технології миротворчої місії за мандатом Організації договору про колективну безпеку (ОДКБ, або Ташкентська угода) [12]. Втім реакція світової спільноти та економічні санкції завадила реалізації цих планів, і Росія зупинилася на варіанті відкритої, але офіційно не визнаної військової агресії.

Після невдалих спроб здійснення фронтальних атак на позиції українських силовиків на Донбасі, як це було, приміром, під час п'ятиденної війни в Грузії, Росія в Україні перейшла до іншої тактики: активності переважно у форматі діяльності диверсійно-розвідувальних груп і провокативних артилерійських обстрілів. Також застосовується тактика партизанської боротьби.

Крім того, слід зазначити, що російські підрозділи на Донбасі сьогодні активно застосовують так звану тактику «трьох кварталів», що передбачає скомбінованість дій одного і того ж підрозділу, який в одному кварталі міста може виконувати загальновійськові функції, у другому – здійснювати поліцейські функції, у третьому – виконувати гуманітарні місії [3]. Цю тактику ми сьогодні наочно спостерігаємо в діях ополченських підрозділів так званих «ДНР» та «ЛНР».

Інформаційна складова гібридної війни на усіх її етапах виконує функцію забезпечувального характеру. На першому етапі вона створює умови для виникнення конфліктної ситуації, на другому – забезпечує привід для опосередкованого втручання держави-агресора у внутрішні справи атакованої країни, на третьому – створює відповідний медійний фон для легітимізації дій агресора.

Цільовими групами для інформаційних атак є [3]:

− цивільне населення, що знаходиться в зоні конфлікту;

− цивільне населення атакованої країни в цілому;

− цивільне населення країни агресора;

− представники світової спільноти.

За змістом, інформаційна складова гібридної війни має вигляд «війни сенсів» із застосуванням передових методів агітації та пропаганди. Зокрема, активно використовуються так звані **симулякри** – ***образи, яких в природі не існує*** [2]. Головна мета таких дій – нав'язати атакованій стороні бачення та психологічні установки, які допомагатимуть агресору в реалізації його планів [3].

У форматі зазначеного особливої ваги набуває завдання встановлення контролю над інформаційним простором країни, проти якої здійснюється агресія, а також тих держав, які можуть якимось чином впливати на перебіг конфлікту.

Як допоміжний засіб використовують діяльність різноманітних громадських структур: благодійних фондів, аналітичних центрів, культурних товариств тощо. У цьому контексті особливого значення набувають технології web 2.0, які надають атакуючій стороні (країні-агресору) необмежені можливості у здійсненні впливу на населення країни, проти якої застосовано агресію. Згадані можливості мають широкий спектр: від впливу на масову аудиторію до здійснення інформаційного контакту на індивідуальному рівні, тобто адресно.

Висновки. Сучасна практика міжнародних гібридних конфліктів має в основі потужну теоретичну та методологічну основу, розроблену зусиллями військових теоретиків і практиків США, Росії, країн ЄС та держав-лідерів Азійського регіону (Китай, Південна Корея, Пакистан, Індія). Ці розробки дають нам чітке уявлення про специфіку ведення війн такого типу у військовій, економічній, політичній, інформаційній і культурній площині. Зокрема, виділяють три базові етапи: латентний, напіввідкритий і відкритий. У форматі цих етапів, як свідчить практика останніх десятиліть, зокрема війна в Іраку, Югославії, Придністров'ї, Грузії, Криму, Донбасі, розгортаються основні економічні, ідеологічно-інформаційні та військово-політичні протистояння. Важливою складовою частиною такої війни є інформаційна – дія на свідомість противника через ЗМІ, офлайн та онлайн соціальні мережі.

Підбиваючи підсумки нашого дослідження, маємо ще раз наголосити на важливості порушеного питання, що нині є складовою частиною потужного виклику, з яким зіткнулася сьогодні Україна. Цей виклик – випробування системи національної безпеки і, насамперед, в інформаційному контексті. Вирішити цю проблему цілком реально. Для цього необхідно ретельно вивчити досвід здійснення гібридних війн таких країн, як США, Росія, ЄС та Китай. Також необхідно розробити власну національну стратегію протидії гібридним та асиметричним агресіям і почати працювати на випередження, а не локалізацію та нейтралізацію проблем, коли вони вже виникли та перейшли у відкриту фазу.

Використані джерела

1. Березовець Т. Анексія: острів Крим. Хроніки «гібридної війни» [Текст] / Т. Березовець. – К. : Брайт Стар Паблішінг, 2015. – 392 с.

2. Вєдєнєєв Д.В. Гострі кігті орла. Сили спеціальних операцій США: історія та сучасність [Текст] : монографія / Д.В. Вєдєнєєв, Г.С. Биструхін, А.І. Семука. – К. : К.І.С., 2010. – 400 с.

3. Горбулин В. «Гибридная война» как ключевой инструмент российской геостратегии реванша [Електронний ресурс] / Зеркало недели: [сайт], 23.11.2015. – Режим доступу: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html

4. Иссерсон Г. С. Новые формы борьбы / Г. С. Иссерсон. – М. : Военная мысль, 1940. – 226 с.

5. Кашников Б. Н. Частные военные компании и принципы «jus in bello» [Текст] / Б. Н. Кашников // Военно-юридический журнал. – № 12. – 2010. – С. 27-32.

6. Магда Є. Гібридна війна. Вижити і перемогти [Текст] / Є. Магда. – К. : Віват, 2015. – 304 с.

7. Месснер Е. Э. Всемирная мятежевойна / Е. Э. Месснер. – М. : Военная мысль, 2004. – 243 с.

8. Переслегин С. О влиянии литературы на общество и об ответственности писателя [Електронний ресурс] / С. Переслегин // Интерпресскон [сайт]. – Режим доступу: http://www.rusf.ru/interpresscon/1998/doclad/do98prsl.htm.

9. Поцепцов Г. Из истории понятия гибридной войны в США и России [Электронный ресурс] / Г. Почепцов // ПСИ-ФАКТОР [сайт]. – Режим доступа: http://psyfactor.org/psyops/hybridwar6.htm

10. Радковец Ю. «Гибридная политика» современной России как стратегия реализации ее национальной геополитики [Електронний ресурс] / Ю. Радковец // Борисфен Интел [сайт]. – Режим доступу: http://bintel.com.ua/ru/article/gibrid-politics/

11. Сотников Г. Деятельность американских охранных фирм в Ираке [Текст] / Г. Сотников // Зарубежное военное обозрение. – № 12 (729). – 2007. – С. 76.

12. Миротворцы ОДКБ готовы к возможности участия в миссии на Украине [Електронний ресурс] // РИА Новости [сайт]. – Режим доступу: http://ria.ru/world/20140829/1021900972.html

13. Arquilla J. Networks and netwars / J. Arquilla, D. Ronfeldt. – Santa Monica, 2001. – 324 p.

14. Freier N.P. Known unknowns: unconventional «strategic shocks» in defense strategy development / N.P. Freier. – Carlisle, 2008. – 236 p.

Reference

1. Berezovets, T. (2015). Annexation Island of Crimea. Chronicles of «hybrid warfare». Kyiv: Bright Star Publishing [in Ukrainian].

2. Vyedyenyeyev, D.V. (2010). Acute Climbing eagle. United States special operations forces: history and modernity. Kyiv: KIS [in Russian].

3. Horbulyn, B. (2015). Hybrid War As the Russian geo-strategy key tool of the revenge. Zerkalo Nedeli, 23 November. Retrieved from http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html [in Russian].

4. Ysserson, G.S. (1940). New forms struggle. Moscow: Military Thought [in Russian].

5. Kashnykov, B.N. (2010). Military part of company principles and «jus in bello». Military-legal journal, 12 [in Russian].

6. Magda, E. (2015). Hybrid war. Survive and win. Kyiv: Vivat [in Ukrainian].

7. Messner, E. E. (2004). All-World Rebellion-War. Moscow: Military Thought [in Russian].