УДК 327.8:355.01+323.269: 32.019.51(477)

Феськов І. В., НУ «ОЮА»

ОСНОВНІ МЕТОДИ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Стаття присвячена науковому аналізу змісту поняття «гібридна війна» в сучасних соціально-політичних умовах. Розглянуто складові гібридної війни та близькі за змістом поняття, такі як: «інформаційна війна», «політичне маніпулювання» тощо. Виявлені основні методи ведення гібридної війни в сучасних реаліях.

На початку XXI ст. активно входить в обіг термін «гібридна війна», що використовується поряд з такими поняттями, як «інформаційна війна», «ядерна війна», «холодна війна», «кібервійна» тощо. В останні роки поняття набуває все більш широкого вжитку через розвиток інформаційно-комунікаційних технологій, розширюється змістовна наповненість терміну. Нажаль, необхідно констатувати, що в останні кілька років все частіше поняття гібридної війни використовується по відношенню до нашої держави.

Незважаючи на широке використання наукового терміну «гібридна війна», до цього часу немає однозначного визначення цього поняття. Найчастіше використовується синтетичне, інтегративне визначення, що включає як активні військові дії з використанням спеціального озброєння (метою яких є фізичне знищення ворога та його людської сили), так і комплекс певних дій агресора по відношенню до потерпілої сторони, спрямованих на дискредитацію останнього в очах світового співтовариства, власного народу, розкол політичної еліти та суспільства в цілому. Подібні дії можуть нанести значно сильнішого удару ніж військове вторгнення, оскільки їх метою є формування певних стереотипів та установок і масовій свідомості через маніпулятивний вплив. Яскравим прикладом, що ілюструє наведену тезу, є нинішня ситуація в Україні.

Слід зазначити, що сучасні політичні та нейролінгвістичні технології дають широкий спектр способів та прийомів маніпулятивного впливу на свідомість. Означені тенденції обумовлюють актуальність дослідження феномену гібридної війни та методів її

ведення з метою побудови ефективного механізму протидії такій війні.

Аналіз останніх досліджень і публікацій. До аналізу сутності гібридної та інформаційної війни звертались в свої наукових працях як зарубіжні, так і вітчизняні вчені. Аналіз сутності інформаційного суспільства проводили у своїх працях П. Бергер, З. Бзежинський, Н. Вінер, Г. Лассуел, М. Постер, Е. Тоффлер, С. Хантінгтон та ін., особливості інформаційної безпеки розглядали Р. Абдєєв, Е. Андрєєв, Г. Грачов, О. Губарєв, О. Деркач, Д. Фролов та ін. Російський вчений А. Манойло у своїй монографії «Державна інформаційна політика в особливих умовах» визначив принципи ведення державної інформаційної політики в умовах агресії. Сутність поняття «гібридна війна» досліджували Ф. Хоффман, Д. Ласік, Дж. Девіс, Ф. ван Каппен та ін.

До вітчизняних вчених, які займаються вивченням феномену інформаційної та гібридної війни належать В. Бебик, Я. Жарков, О. Литвиненко, В. Петрик, М. Присяжнюк, І. Рабінович, Д. Фельдман, Ю. Шайгородський та інші. Також слід згадати Г. Почепцова, який здійснив аналіз інформаційної політики та безпеки, які проводять провідні країни світу, і О Гапченко, що досліджує пропагандистський дискурс як засіб маніпулювання людською свідомістю. Проте, наразі в науковій літературі не існує чіткого переліку прийомів та методів ведення гібридної війни, що визначає актуальність даного дослідження.

Метою статті є комплексний аналіз сучасного змісту поняття «гібридна війна» та методів її ведення, з урахуванням сучасного етапу суспільного розвитку – в умовах інформаційного суспільства.

Виклад основного матеріалу дослідження. На думку теоретиків гібридної війни, сучасні конфлікти розгортаються в чотирьох суміжних сферах: фізичній, інформаційній, когнітивній та соціальній. Інтегрованою стає інформаційна сфера, на яку і прагнуть впливати сторони конфлікту задля своєї перемоги.

Поняття «гібридна війна» було введено американським вченим М. Маклюеном, який вважав засоби комунікації новим ресурсом держави та довів, що сучасні війни відбуваються в інформаційному просторі [1].

На даний час існують різні варіанти визначення сутності гібридної війни:

1) військова стратегія, яка поєднує звичайну війну, малу війну та кібервійну;

2) атака з використанням ядерної, біологічної, хімічної зброї, саморобних знарядь для терористичних атак та інформаційного тиску;

3) складна та гнучка динаміка бойового простору (battlespace), яка передбачає швидку реакцію та адаптацію учасників протистояння;

4) сучасний вид партизанської війни, яка поєднує сучасні технології та методи мобілізації (Біл Неметт, підполковник Корпусу морської піхоти США);

5) основний метод у асиметричній війні, яка ведеться на трьох умовних фронтах – серед населення конфліктної зони, тилового населення та міжнародної спільноти (полковник АрміїСША Джек МакКуен) [2, с. 22-39].

Ф. Хоффман дає наступне визначення гібридної війни – повний арсенал всіх видів бойових дій, враховуючи конвенціональні можливості, іррегулярну тактику і формування, терористичні акти, що містять насилля та кримінальні безлади [3]. Автор визначив п'ять елементів гібридної війни: модальність проти структури, одночасність, злиття, комплексність і злочинність [4].

До складових гібридної війни, на нашу думку, слід віднести використання методів класичної війни (проведення збройних військових операцій), інформаційної або інформаційно-психологічної, партизанської війни, «кібервійни», елементів тероризму та підривних дій, економічного та дипломатичного впливу.

Гібридна війна небезпечна тим, що фактично стираються кордони війни, сценарії її початку та закінчення, часто буває важко визначити суперника, зміна стану з військового до мирного часто нічого не вирішує конфлікт, в подальшому ситуація може загострюватись.

На даний час поняття «гібридна війна» («hybrid warfare») і «гібридна загроза» («hybrid warfare threats») вже введені в офіційну термінологію західної військової політики. Так, в підсумковому документі, прийнятому на саміті НАТО у вересні 2014 року в Уельсі, Англія, в п.13 йдеться про необхідність підготовки Північноатлантичного військового альянсу до того, «щоб НАТО була здатна ефективно долати конкретні виклики, що виникають у зв'язку з погрозами гібридної війни, при веденні якої застосовується широкий ряд тісно взаємопов'язаних відкритих і замкнутих військових, воєнізованих та цивільних заходів» [5]. Учасники

альянсу розглядають гібридні війни як широкий набір бойових дій, таємних операцій, здійснюваних партизанськими формуваннями, з залученням цивільних компонентів, а також як боротьбу з пропагандистськими кампаніями, кібератаками і місцевим сепаратизмом. Для здійснення комунікацій та проведення навчань з відпрацювання дій в гібридної війні навіть був створений спеціальний навчальний центр в Латвії (Strategic Communications Centre of Excellence).

Переважна більшість авторів сходяться на думці про те, що провідною складовою гібридної війни є інформаційна війна. Це доводить і практика. Так, постійний розвиток системи масової комунікації призводить до стирання кордонів, широких можливостей для здійснення маніпулятивного впливу на свідомість населення країни-суперника з насаджуванням власних ідей. Так, в україно-російській інформаційній війні це – боротьба так званого «руського миру» (ідеологія відновлення радянської системи) та пост майданної України (з новими політичними проектами та постколоніальним синдромом) [6, с. 50].

Слід зазначити, що термін «інформаційна війна» використовував одним з перших Т. Рона в аналітичному звіті для компанії Боїнг «Системи зброї і інформаційна війна» в 1976 р. [7]. З того моменту починається формуватися розуміння того, що інформація може бути зброєю. А з урахуванням того, що розвиток економік країн Європи і США засновано на прориві в інформаційно-телекомунікаційних технологіях, то цей сектор стає особливо вразливим як у воєнний, так і в мирний час. Виділяють два провідних напрямки впливу інформаційної зброї: вплив на інформаційні засоби і системи противника і вплив на свідомість людей. Перший напрямок отримало ще назву кібервійни, коли атакам піддається технічне обладнання і системи його програмного забезпечення. Другий напрямок – це старі способи пропаганди і агітації, контрпропаганди і контрагітації, але досягли небувалих по своє силі висот по витонченості і масовості впливу на уми людей.

Найбільш відомим визначенням інформаційних воєн стало таке: «... це вид конфлікту, при якому завданнями протиборчих сторін є захист власної інформації та інформаційних систем, маніпулювання інформацією противника або її спотворення, а також обмеження можливостей протиборчої сторони в доступі і обробці інформації» [8, с. 3].

На сучасному етапі стало очевидним фактом, що якщо ще недавно Інтернет мав переважно інформаційну складову, то тепер в ньому все більше набирає силу сектор агітаційний, пропагандистський, що відрізняється яскраво вираженою агресивністю. Традиційні ЗМІ все більше працюють з інтернет-ресурсами як джерелами інформації і засобом впливу на свідомість громадян. Інформація в Мережі стає все більш масово затребуваною, швидко розповсюджується і суспільно значимою. Метою інформаційної війни є управління процесом зміни свідомості людей, їх світогляду, ставлення до суспільства і держави; небезпекою для людей є втрата ними власної волі, а для держави – її суверенітету. Це завжди було метою будь-якого завойовника, але тепер того ж можна домогтися «м'яким» способом (навіть термін з'явився: «soft power» – м'яка сила, введений у вжиток американським політологом Дж. Найєм). Але «м'які» засоби в деяких випадках можуть бути небезпечніше «жорстких», тому що жертва м'якого примусу може і не усвідомлювати обману, може побачити результат тільки тоді, коли, як то кажуть, «поїзд уже пішов». При цьому така зброя має масовим характером ураження. Зі зрозумілих причин вільний і важко контрольоване поширення інформації в Інтернеті створює чимало проблем спецслужбам всіх держав. Лавиноподібний потік інформації (і дезінформації) здатний завдати шкоди будь-якій державі (аж до революційного вибуху і повалення влади).

Цікавою видається думка А. Дорошенко про те, що інформаційна війна на сучасному етапі постає у формі мережевоцентричної війни, завданням якої є ідентоцид, тобто знищення національної-державної-громадянської ідентичності країни-суперника до такого стану, коли про нього можна сказати одне – нелюдь і ворог. Ідентоцид полягає у переконанні більшості народу своєї країни, або навіть частини народу супротивника в злих намірах супротивника щодо своїх. Об'єктом такої війни є масова та індивідуальна свідомість. Слід зазначити, що інформаційний вплив може здійснюватися як на тлі інформаційного шуму, так і в умовах інформаційного вакууму [9].

До основних інструментів гібридної війни відносять наступні інформаційні заходи: засоби військово-політичної дезорієнтації противника; дезінформація щодо власних ресурсів; дії, спрямовані на поразку чи блокування каналів передання даних з метою дезорієнтації й дезорганізації, створення атмосфери напруженості

в українському суспільстві від постійного очікування ударів і масованого наступу по всій лінії фронту та вплив на масову свідомість українців з метою деморалізації та поширення паніки [10].

Постійне збільшення потоків інформації унеможливлює контроль за ними з боку будь-якої держави. Тому провідним завданням під час протистояння в інформаційній сфері є не контроль за потоками інформації, як вірно зазначає О. Дугін [11], контроль алгоритму руху інформації, що дасть змогу дешифрувати її та тим самим убезпечити суспільство та інститути управління ним.

В рамках аналізу сутності гібридної війни зустрічається термін «психологічна війна», який вперше використав британський історик Дж. Фуллер на початку XX ст. при аналізі Першої світової війни. Пізніше американські дослідники запозичили цей термін та стали вживати поняття «психологічна операція» або «інформаційна операція». Наразі під час навчання військовослужбовців в США офіцерів навчають тактиці та стратегії психологічних операцій, які найчастіше використовуються під час миротворчих операцій.

Інститут національно-стратегічних досліджень США та деякі західні експерти, аналізуючи складові елементи інформаційної війни, виокремлюють ведення психологічної війни, завдання якої полягає в маніпулюванні масами з метою: внесення в суспільну та індивідуальну свідомість ворожих шкідливих ідей та поглядів; дезорієнтація та дезінформація мас; послаблення певних переконань, устоїв; залякування свого народу образом ворога; залякування супротивника власною могутністю тощо [12, с. 138].

До основних методів ведення інформаційно-психологічної війни слід віднести пропаганду, поширення чуток, провокації, дезінформування, психологічний тиск, диверсифікацію суспільної свідомості тощо.

Найбільш поширеним методом є пропаганда, яка передбачає поширення в масах і роз'яснення яких-небудь переконань, ідей, вчення, знань.

Вперше роль пропаганди була проаналізована в працях Г. Лассауелла, який визначав її як особливий вид зброї, що впливає на моральний (тобто психічний) стан ворога. Серед основних цілей пропаганди автор визначає: збудження ненависті до ворога; підтримка дружніх відносин із союзниками; збереження добрих відносин із нейтральними країнами і, якщо можливо, намагання співпрацювати з ними; деморалізація супротивника [13].

Цікавим є трактування французького соціолога Ж. Еллюля, який запропонував розрізняти вертикальну (класичний варіант пропаганди, як ми всі собі її уявляємо, інформаційний потік згори до низу з пасивним реагуванням аудиторії) та горизонтальну (вона реалізується в певній соціальній групі, а не йде згори; у цій ситуації всі учасники є рівними, серед них немає лідера, а тому інформація сприймається з максимальною довірою) пропаганду. Автор також розрізняє два різновиди горизонтальної пропаганди: китайська (від членів групи не вимагається висловлювання власної думки) та американська (передбачає активність та виявлення індивідами власної позиції), спричинені особливостями групової динаміки [Цит. за: 14].

До основних прийомів пропаганди можна віднести: формування у масовій свідомості образа жертви з фігуранта, що насправді є злочинцев, перекладання відповідальності та приписування власних злочинів супернику, ігнорування фактів та таврування всіх, хто не згоден з пропагандою.

Означені прийоми використовуються РФ під час гібридної війни з Україною. Так, В. Ткач визначає методи, що використовувались під час проведення акцій спецпропаганди в Україні: «встановлення довірливих відносин із цільовою аудиторією (у спосіб використання поширених і усталених висловлювань, посилань на авторитети, цитат тощо); створення ілюзії самостійності розумової роботи (підготовка і подача матеріалів таким чином, щоб у аудиторії виникло відчуття, що до пропонованих висновків вона начебто дійшла абсолютно самостійно, понад те, зробила для прийняття цього рішення серйозну розумову роботу); використання образу енциклопедичності автора, який оперує величезним обсягом матеріалу і заливає супротивника інформацією (при використанні повномасштабних текстів архівних матеріалів, міжвідомчого листування, економічних таблиць і викладок та інших дуже нелегких для читання речей, щодо справжності яких практично неможливо визначитися); «утоплення в документах» (маніпулювання з документальними матеріалами, результатами досліджень, цілеспрямований відбір тільки тих джерел, які «вписуються» в задум, фальсифікація документів, унеможливлення їх перевірки тощо); свідоме і цілеспрямоване надання інформації інтенсивно емоційного забарвлення з метою пригнічення процесів раціонального мислення тієї аудиторії, яка піддається

інформаційній атаці; конструювання і описування подій у ЗМК і літературі задовго до того, як щось подібне сталося в реальності, інтерпретація та упереджене коментування замість детального інформування про факти» [15, с. 104].

Дезінформування та маніпулювання інформацією, на думку В. Петрика, досягається через: тенденційне викладення фактів (інформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних; як правило, за допомогою цього методу спеціально сформована інформація подається дозовано, до постійно зростаючого напруження); дезінформування «від зворотного» (відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві; в результаті виникає ситуація, коли об'єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу); термінологічне «мінування» (полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру); «сіре» дезінформування (передбачає використання синтезу правдивої інформації з дезінформацією); «чорне» дезінформування (використання переважно неправдивої інформації) [16].

Диверсифікація громадської думки має на меті розпорошення уваги правлячої еліти держави на різні штучно акцентовані проблеми і тим самим відволікання її від вирішення першочергових завдань суспільно-політичного та економічного розвитку з метою забезпечення нормального функціонування суспільства і держави. Її формами є: дестабілізація обстановки в державі чи її окремих регіонах; активізація кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів різними міжнародними установами; ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин [12, с. 139].

Психологічний тиск є також поширеним методом впливу на свідомість людей. Його застосування передбачає шантаж, погрози переслідувань, репресій, вбивств та ін., доведення до об'єкта відомостей про реальні чи надумані загрози та небезпеки, здійснення терористичних актів та диверсій. У вітчизняній практиці

найбільшого поширення отримав телефонний тероризм, тобто дзвінки з інформацією про нібито замінування громадських місць, вокзалів і т.п. До основних технологій тиску відносять: шахрайство, блеф, політичні ігри і містифікації, маніпулятивні дії, провокації, психологічні і таємні операції, політичні ігри і рекламні кампанії, дезінформація, чутки тощо.

Провокація є одним із часто вживаних методів ведення війни на сучасному етапі, що дозволяє спонукати противника здійснити невигідні для нього дії.

Поширення чуток є особливою технологією інформаційної війни. Г. Почепцов відзначає, що відсутність інформації моментально компенсується чутками. Він навіть вказує на вірогідність існування певного закону про можливості вакууму інформації: коли її не дають офіційні джерела, вона тут же з'являється в неофіційних каналах [17, с. 211-216].

Всі означені методи психологічної війни використовуються і під час інформаційної агресії проти України. Крім того, СБУ встановила, що російські ЗМІ застосовують і інші методи впливу на глядача: поширюють напівправду, показують деталізовані сцени вбивств і насильства, намагаючись сформувати образ ворога (в ролі якого виступає українська влада) в свідомості глядачів, використовують технологію «25-го кадру» тощо [18].

Таким чином, в даний час ще не розроблені кардинальні заходи з протидії інформаційним атакам. А це означає, що в інформаційних війнах успіх буде забезпечуватися за рахунок все більшого вдосконалення інформаційних технологій. Як показує практика, недостатня увага до питань парирування інформаційних загроз може завдати значної шкоди політичній системі будь-якої держави аж до руйнування самої держави. Отже, на нашу думку, виправданими є кроки, запроваджені керівництвом нашої держави щодо обмеження інформаційного впливу з Росії (вимкнення російських каналів, заборона частини російських фільмів тощо), а також створення спеціального інституційного механізму для боротьби з інформаційними впливами з боку Росії (кіберполіція).

Бібліографічний список:

1. Маклюен Г. М. Внешние расширения человека / Г. М. Маклюен ; пер. с англ. В. Николаева ; закл. ст. М. Вавилова. – М. ; Жуковский : КАНОН – пресс – Ц, Кучково поле, 2003. – 464 с.
2. Арзуманян Р.В. Определение войны в 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегических

исследований Армейского военного колледжа, 6-8 апреля 2010 / Р.В. Арзумян. – Ереван, 2011. – 60 с.
3. Hoffman F. G. Hybrid vs. compound war [Електронний ресурс] / F. G. Hoffman // Armed Forces Journal, Oct. 2009. – Режим доступу: http://armedforcesjournal.com/hybrid-vs-compound-war/
4. Hoffman F. G. Future Threats and Strategic Thinking [Електронний ресурс] / Hoffman F. G. // Infinity Journal, No Fall 2011. – Режим доступу: https://www.infinityjournal.com/article/34/Future_Threats_and_Strategic_Thinking/
5. Заявление по итогам встречи на высшем уровне в Уэльсе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического союза в Уэльсе – 4-5 сентября 2014 [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=ru
6. Смола Л.Є. Аспекти ведення інформаційної та гібридної війни в контексті застосування комунікаційних технологій / Л.Є. Смола // S.P.A.C.E. – 2016. – № 1. – С. 48-53.
7. Thomas P. Rona. Weapon Systems and Information War / Thomas P. Ro – Boeing Aerospace Co., Seattle, WA, 1976. – 72 p.
8. Бедрицкий А.В. Эволюция американской концепции информационной войны // Аналитические обзоры РИСИ. – 2003. – № 3. – 26 с.
9. Дорошенко А.С. Гібридна війна в інформаційному суспільстві / А.С. Дорошенко // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». – 2015. – № 2(25). – С.21-28.
10. Присяжнюк Д.М. Застосування маніпулятивних технологій з боку Росії в ЗМІ України (на прикладі Криму) / Д.М. Присяжнюк [Електронний ресурс]. – Режим доступу : http://vuzlib.com/content/view/1108/23
11. Дугин А. Г. Основы геополитики. Геополитическое будущее России. Мыслить Пространством / А. Г. Д угин. – М. : Арктогея-центр, 1999. – 928 с.
12. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення / Ю.О. Горбань // Вісник НАДУ. – 2015. – №1. – С. 136-141
13. Ласвель Г. Техника пропаганды в мировой войне: сокр. пер. с англ. в обработке Н. М. Потапова / Г. Ласвель. – Л.: Отдел военной литературы Госиздат, 1929. – 200 с.
14. Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни [Електронний ресурс] / Л.П. Макаренко. – Режим доступу: http://oaji.net/articles/2014/797-1402908125.pdf
15. Ткач В.Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України / В.Ф. Ткач // Стратегічні пріоритети. Серія «Політика». – 2016. – №1(38). – 99-109.

16. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://justinian.com.ua/article.php?id=3222
17. Почепцов Г. Г. Психологические войны / Г. Г. Почепцов – М., К.: Рефл-бук, Ваклер, 2000. – 528 с.
18. У СБУ заявили, що російські канали застосовують проти телеглядачів «25-й кадр» [Електронний ресурс].– Режим доступу : http://tsn.ua/politika/u-sbuzayavili-scho-rosiyski-kanali-zastosovuyut-protiteleglyadachiv-25-y-kadr-350517.html

Статья посвящена научному анализу содержания понятия «гибридная война» в современных социально-политических условиях. Рассмотрены составляющие гибридной войны и близкие по смыслу понятия, такие как: «информационная война», «политическое манипулирование» и другие. Выявлены основные методы ведения гибридной войны в современных реалиях.

The article is devoted to the scientific analysis of the content of the concept of «hybrid war» in modern socio-political conditions. The components of the hybrid war and related concepts are considered, such as: «information war», «political manipulation» and others. The main methods of conducting a hybrid war in modern realities are revealed.

Стаття надійшла до редколегії 30.11.2016