Рижук О.М.

Інформаційні та гібридні війни в глобальному інформаційному суспільстві

Стаття наводить ряд визначень провідних науковців щодо поняття «інформаційна війна». Вказано, що на офіційному міжнародному рівні спостерігається відсутність єдиного підходу до цього явища, що веде до систематичного непорозуміння між представниками різних країн. Також акцент робиться на тому, що інформаційна війна є складовою частиною гібридної війни. Зазначено, що провідні країни світу мають дуже потужні види зброї, які роблять її використання небезпечним як для самого агресора, так і для усього світу. Для перемоги у гібридній війні не лише агресор повинен мати стійку державну владу, бути міцним економічно, морально і психологічно, але й в об'єкта агресії державна влада має бути нестійкою, існувати криза у суспільстві та проблеми в економіці. Така ситуація спостерігалася під час активної фази гібридної війни Росії проти України. Стаття аналізує поняття «гібридна війна» та вказує на характерні дії Росії проти України під час активної фази гібридного протистояння.

Ключові слова: *інформаційна війна, гібридна війна, глобалізація, інформаційне суспільство, інформаційна безпека.*

В статье рассмотрены определения ведущих ученых относительно понятия «информационная война». Указано, что на официальном международном уровне наблюдается отсутствие единого общепринятого подхода к этому определению, поэтому такая ситуация порождает состояние неопределенности между представителями разных стран. Также акцент делается на том, что информационная война является составной частью гибридной воны. Указано, что ведущие страны мира имеют такие виды оружия, использование которых может составлять опасность не только для самого агрессора, но и для всего мира. Для победы в гибридной войне не только агрессор должен иметь устойчивую государственную власть, быть стабильным экономически, морально и психологически, но и у объекта агрессии государственная власть должна быть нестабильной, существовать кризис в обществе и проблемы в экономике. Такая ситуация имела место во время активной фазы гибридной воны России против Украины. В данной статье также анализируются определения «гибридная война» и указываются характерные действия России против Украины во время активной фазы гибридного противостояния.

Ключевые слова: *информационная война, гибридная война, глобализация, информационная безопасность, информационное общество.*

The article gives a list of "information war" definitions by leading scientists and researchers. Emphasized is that single terminology is absent at the international level. It makes mutual understanding harder among representatives (investigators) from different countries. Attention is drawn to the fact that information war is a part of hybrid war. Stated that in the modern world there are powerful kinds of weapons (including weapons of mass destruction) which make classic wars very dangerous for both aggressor and the whole the world. To win a victory in a hybrid war, the aggressor must be stronger not only morally, psychologically and economically but also state power of the object of aggression must be weak. There should be a split in a society and problems in economy. That is the situation that took place during the active phase of Russia's hybrid war against Ukraine. Analysed in the article is the "hybrid war" concept. Pointed out are Russia's actions towards Ukraine during the active phase of hybrid conflict.

Key words: *information war, hybrid war, globalization, information society, information security.*

УДК 327.88:[323.266:316.658]](100)(045)

Рижук О.М.,
здобувач кафедри
суспільно-політичних наук,
глобалістики та соціальних комунікацій
Відкритого міжнародного університету
розвитку людини «Україна»

В індустріальному суспільстві конкурентоздатність держави, її військовий потенціал визначалися можливостями створювати важку зброю, транспортувати її та витримувати економічне навантаження. Інформаційне суспільство визначає військову конкурентоздатність держави її можливостями працювати з інформацією, а саме: обробляти та адаптувати до військових потреб інформаційні потоки, які впливають на майбутній перебіг бойових дій.

Військове протистояння між Російською Федерацією та Україною дедалі більше має формат інформаційного конфлікту. Нові цінності та можливості постіндустріального суспільства, яке формується і на пострадянську просторі, визначили особливості дій Росії з метою впливу на Україну.

У наш час тематика інформаційної та гібридної війни є надзвичайно актуальною. Вітчизняними дослідниками, які приділяють увагу інформаційним та гібридним війнам, є: П. Жарков, Р. Калюжний, Є. Магда, Г. Почепцов та інші.

Мета статті полягає в тому, щоб дослідити інформаційні війни, які набувають дедалі більшого поширення в сучасному інформаційному світі; відобразити зв'язок між інформаційними та гібридними війнами; проаналізувати причини виникнення такого явища, як «гібридна війна», та пояснити її надзвичайну популярність за сучасних умов серед певних країн, які хочуть досягнути своїх політичних цілей за рахунок інших країн.

Сучасні та майбутні війни характеризуються такими формами та способами ведення збройного протистояння [2, с. 20]:

1) через забезпечення армій новітніми засобами боротьби, які дають змогу вести неконтактні (дистанційні) бойові дії, зростає значення неядерного стримування супротивника;

2) широке використання сил швидкого реагування, аеромобільних військ та військ спеціального призначення дає змогу пришвидшити рівень динамічності військових та підвищити їх маневреність;

3) збільшення масштабів збройного протистояння, розширення території бойових дій із землі до води та повітря, заглиблення під воду та підняття до космічного протру;

4) можливості електронного та вогневого ураження передових військових, тилової інфраструктури, економіки та допоміжних комунікацій одночасно на усій території супротивника;

5) використання новітніх інформаційних технологій у протиборстві з супротивником;

6) проведення заходів по боротьбі з міжнародним тероризмом, де необхідно створювати спеціальні сили для проведення антитерористичних на миротворчих заходів.

Цей перелік має умовний характер, але разом із тим вказує на важливість цих тенденцій. Ці характеристики залежні від конкретних особливостей держав [2, с. 20].

Значний складник щодо переваги в інформаційній війні полягає у контролі над інформаційними потоками, а також діяльності з використання інформації у вигляді зброї, тобто для ведення бойових дій. Для сучасної держави інформація, інформаційна інфраструктура та інформаційні технології, що разом становлять інформаційний простір, перетворюються на головний стратегічний ресурс країни.

Як свідчать історичні факти, інформаційні конфлікти між країнами відбувалися постійно, але відрізнялися різним ступенем конфліктності та їх системністю. Якщо проникнення до інформаційного простору іншої держави спланова но та організовано на державному рівні, це носить назву інформаційної війни.

Поведінка основних суб'єктів всередині країни може змінюватися навіть від звичайного спостереження за інформаційним простором іншої держави. Таким прикладом слугує Росія, яка розгорнула ряд інформаційних війн із пострадянським країнами. Об'єктами інформаційної агресії Росії були Латвія, Естонія, Грузія, Молдова та Україна.

Взагалі пострадянський простір став ареною своєрідної «холодної війни». Це виникло з тієї причини, що кожна країна має власні економічні, політичні та військові погляди на свій розвиток, але разом із тим вони створюють конкуренцію іншим країнам.

Розглядаючи пострадянський простір як територію своїх інтересів, Росія намагається вийти на етап реалізації власної глобальної мети. Як доводять різні дослідники, Росія не може існувати без глобальної мети.

Україна ж протягом останніх років виявилася неспроможною побудувати власну модель реальності, сформувати власну точу зору, а через це держава постійно перебувала між прозахідними та проросійськими інтересами. З метою ефективного аналізу явища «інформаційна війна» необхідно зрозуміти, що воно саме собою являє, тобто зрозуміти його визначення.

Американські спецслужби були першими, хто увів своє визначення терміна «інформаційна війна». Інформаційною війною вони вважали війну в інформаційному просторі [8].

У «Дослідженні по інформаційним операціям» [6] під інформаційною війною розуміються інформаційні операції, де уточнюється, що це є конфліктом, в якому критично та стратегічно важливим ресурсом є інформація, яку необхідно освоювати або знищувати. Термін «інформаційні операції» дає змогу дослідити роль і місце інформаційного протиборства більше, аніж термін «інформаційна війна».

Офіційні та неофіційні джерела давали різні визначення терміну «інформаційна війна». Є. Денінг у своїй роботі «Інформаційна війна та безпека» [5] вважає, що під інформаційною війною розуміється сукупність операцій, які мають на меті експлуатацію інформаційних ресурсів або вже перейшли до неї.

Дж. Стайн у своїй роботі визначав інформаційну війну як заходи із застосування інформації, яку держава використовує для досягнення своєї реальної мети [9].

Американський теоретик М. Лібіцні у роботі «Що таке інформаційна війна» у 1995 р. навів 7 різновидів інформаційних війн [4]:

1) захоплення командно-контрольних пунктів внаслідок військового протистояння;

2) боротьба розвідки та контррозвідки;

3) боротьба в електронній сфері;

4) проведення операцій психологічного змісту;

5) організація систематичних та стихійних хакерських атак на інформаційні засоби;

6) проведення інформаційно-економічних війн із метою оволодіння інформацією та отримання контролю над торгівлею інформаційними продуктами – ці дані необхідні для отримання переваги над конкурентами;

7) проведення кібернетичних війн у віртуальному просторі.

У сучасному світі під інформаційною війною розуміється інтенсивне використання комп'ютерної техніки, електронних засобів комунікацій, психологічних методів, які, впливаючи на людську свідомість, можуть змінити хід думок, допомогти змінити рішення супротивника, одночасно захищаючи свою власну територію [4].

Оскільки на міжнародному рівні відсутній єдиний термінологічний апарат щодо вказаної про-

блематики, це ускладнює взаєморозуміння між представниками різних країн та веде до термінологічної плутанини в описі різних явищ чи подій [3].

Заради досягнення власних цілей провідні держави світу намагаються розробляти та застосовувати нові форми і методи боротьби. Про це говорить уся вищезазначена інформація. Класичні методи ведення боротьби в сучасному світі змінюються, а їм на зміну приходять так звані «гібридні війни», які тісно пов'язані з інформаційними засобами. Коло об'єктів, яких можуть охопити гібридні конфлікти, надзвичайно широке. Одні можуть спостерігатися у політиці, економіці, соціальній та інформаційній сферах та мати прихований характер. Армія за такої ситуації залучається в невеликій кількості та переважно з використанням спеціально-підготовлених військ, які розуміються на цьому напрямі боротьби. Такий підхід має на меті не фізичне знищення супротивника в межах масштабної війни, а проведення заходів, які можуть дезінформувати супротивника, призвести до зміни його керівництва, включити до сфери свого впливу.

Найхарактернішими ознаками «гібридних війн» є:

– боротьба в інформаційному полі;

– проведення заходів політичного та економічного тиску при юридичному збереженні відносин між обома країнами;

– проведення пропагандистських заходів із використанням «брудних» інформаційних технологій;

– початок агресивних дій без офіційного оголошення війни;

– використання мирного населення як прикриття під час проведення операцій;

– відмова від участі у конфлікті на офіційному рівні.

З метою врахування усіх основних аспектів воєнного конфлікту військова теорія використовує цілу низку критеріїв за якими можна визначити типи воєнних конфліктів. Якщо поділити конфлікти на типи, критеріями будуть ступінь охоплення дійсності, сфера їх дії, типи сторін, які є учасниками конфлікту, їх соціально-політичний устрій, соціально-політичні відносини, структура їх організації та рівень експлуатації тощо. Оскільки у воєнному конфлікті присутні різні його елементи, це говорить про велике різноманіття форм їх існування. В їх основі лежить комбінація трьох моделей війн – формальних, неформальних та війн «сірої зони». Формальним військовим протистоянням вважається військове зіткнення збройних сил двох і більше держав. Воно, як правило, оголошується офіційним (формальним) актом оголошення війни. До неформальних війн належать збройні протистояння, де учасниками конфлікту є недержавні утворення. Явище «сіра зона» виникло у зв'язку з новими загрозами, які стали актуальними після холодної війни. Сірою зоною прийнято вважати комбінацію війни та військових дій у поєднанні з організованою злочинністю. Прикладами можуть бути війна у Чечні на території Російської Федерації, війна у Сирії з угрупуваннями ІДІЛ тощо. Формальні війни характеризуються традиційними і нетрадиційними формами. Традиційними формами війни вважаються воєнні дії однієї держави, що здійснюються за допомогою регулярних збройних сил. Це контактні війни, які розробляють та впроваджують нові способи і засоби збройної боротьби. Новітні інформаційні технології дають змогу із традиційних війн виокремлювати мережеві та мережевоцентричні форми війн [2, с. 20].

Ф. Хоффман, який є одним з авторів концепції «гібридної війни» та консультантом Міністерства ВМФ США вказує на певні специфічні форми війни, якими характеризується кожна епоха. Це несе за собою нові термінологічні підходи. У військовій сфері, як зазначає Ф. Хоффман, сучасному світу притаманні процеси гібридизації, тобто відбувається перетворення традиційних форм війни з організованою злочинністю, тероризмом та іррегулярними формуваннями [7, с. 34–39]. Саме тому сучасні військові конфлікти необхідно називати «гібридною війною». Це допоможе охарактеризувати їх реальність. Цей термін відображає усю суть змін, що відбуваються у сучасних війнах.

Через це необхідно провести аналіз безпосередніх причин виникнення явища «гібридна віна» та пояснити, чому саме гібридні воєнні конфлікти набувають великої популярності у наш час для досягнення політичних цілей окремими країнами.

Щодо явища «гібридна війна» немає однозначного трактування, оскільки дослідження по ній тривають, але ми можемо виділити найбільш поширені приклади визначення гібридної війни [1, с. 22–39]:

1) поєднання звичайної, малої та кібервійни в єдину стратегію;

2) атака, яка передбачає використання усього арсеналу ядерної, біологічної та хімічної зброї, а також інформаційних засобів, залежно від масштабів протистояння;

3) один із видів війни, що ґрунтується на сучасних технологічних засобах та методах мобілізації;

4) метод асиметричного протистояння, що взаємодіє з трьома факторами і населенням конфліктної зони, тиловим населенням та міжнародною спільнотою;

5) комбінація дій ворога, з використанням дозволеної зброї, партизанських методів, тероризму, для досягнення політичних цілей.

З огляду на вищевикладене, гібридну війну можна охарактеризувати як сукупність заздалегідь підготованих і реалізованих дій, які націлені на досягнення стратегічної мети однієї держави

стосовно іншої та мають економічний, військовий, дипломатичний та інформаційних характер. Складовими частинами гібридної війни вважаться традиційні і нестандартні загрози, терористичні дії, що мають підривний характер, новітні та нешаблонні технології, які забезпечують перевагу над супротивником у військовій силі.

Оскільки гібридна війна не є війною у класичному розумінні цього слова, окрім протистояння на полі бойових дій, вона включає в себе економічні, психологічні, духовні складники протистояння та партизанщину. Залежно від розвитку суспільства визначаються і всі відношення цих компонентів у конфлікті.

Новітні технології у гібридних війнах працюють на межі своїх можливостей, постійно вдосконалюючись, намагаючись обігнати конкурентів за перевагами. Саме ці технології надають перевагу гібридним збройним силам над традиційними. Гібридна війна стирає уявлення про традиційні війни.

Поняття «гібридна війна» може розглядатися у двох площинах: загальній та військовій. Загальна площина визначає гібридну війну як крайній ступінь конфліктів, які виникають лише між державами. Ці протиріччя можуть бути вирішені не лише воєнними методами, але й з використанням економічних та інформаційних підходів. Із розвитком демократії та вдосконаленням суспільних трансформацій, важливого значення набувають поняття справедливої та несправедливої війни. Усі держави, демократичні чи квазідемократичні, намагаються виставити себе учасниками справедливої війни перед своїми населенням та перед світовою спільнотою.

Сучасне міжнародне право створило ряд обмежень щодо методів, форм та порядку ведення сучасних війн. Для того щоб безболісно для власної держави застосовувати відкриту зброю проти іншої держави, потрібні потужні інформаційні переконання, які б виправдовували керівництво країни перед власним населенням, оскільки воєнні дії спричиняють великі людські жертви, тому перш, ніж почати воєнні дії, керівництво країни має заручитися підтримкою власних людей. Бажано знайти шляхи впливу і на населення супротивника, щоб заручитися і його підтримкою та мінімізувати опір. Це один із прикладів проведення гібридної війни, де агресивна політика держави підтримується власним населенням та забезпечується підтримка активного населення країни-жертви.

Винайдення потужних видів зброї, в тому числі і ядерної, перетворює класичні війни на небезпечні не лише для країни-жертви, але й для самого агресора. Традиційні воєнні дії призводять до руйнації інфраструктури, промислових об'єктів, значних людських жертв, появи біженців тощо. На країну-агресора можуть бути накладені міжнародні санкції, що похитне її положення на міжнародній арені та завдасть проблем економічним зв'язкам. Тому, за сучасних умов, країні-агресору ефективніше встановити свій контроль над об'єктом агресії шляхом інтеграційних, політичних, економічних та безпекових систем, не завдаючи великих збитків.

Ще однією з умов, яка необхідна країні для впевненого розв'язування гібридної війни, є наявність сильної та дієвої влади, яка може згуртувати громадян навколо національної ідеї незважаючи на існуючі проблеми

Разом із тим гібридна війна може мати успіх через слабкість влади в об'єкті агресії, розколу у суспільстві, кризи в економіці, зниження рівня обороноздатності силових структур. У такому стані була Україна під час відкритої агресії з боку Росії. На той час практично усі сфери суспільного життя в Україні перебували в стані кризи – економіка, політика, культура. Висока залежність зовнішніх ринків збуту від Росії та відсутність інших шляхів постачання ресурсів поставили під загрозу українську державність. Російська пропаганда нав'язувала проблему дискримінації російського населення в Україні.

Гібридні війни, що стали поширеними у XXI ст. вимагають свого теоретико-методологічного осмислення. Необхідний досвід усієї світової наукової думки з метою вироблення методів ефективного протистояння гібридним загрозам. Під час дослідження гібридних небезпек мають братися до уваги не лише військові методи боротьби, а й політичні, культурні, економічні і геополітичні підходи. Будучи міцною політично, економічно і духовно, держава не завжди може потрапити під інформаційну пропаганду іншої країни. Політичні кризи, які можуть виникнути через неефективність державної влади, непорядність державних керівників, нестабільність політичної системи полегшують зовнішній інформаційний вплив інших держав та можуть призвести до інформаційних протистоянь зовнішнього та внутрішнього характеру.

ЛІТЕРАТУРА:

1. Арзуманян Р.В. Определение войны 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегическпх исследований Армейского военного колледжа, 6–8 апреля 2010 г. / Р.В. Арзуманян. – Ереван, 2010. – С. 22–39.

2. Василенко О.В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому / О.В. Василенко // Наука і оборона. – 2009. – № 4. – С. 18–22.

3. Деркаченко Я. Эволющия понятия «Информационная война», 2006р. [Електронний ресурс]. – Режим доступу : http://www.psyfactor.org/psyops/infowar46.htm.

4. Information operation Roadmap [Електронний ресурс]. – Режим доступу : http://www.nsarchive.gwu.edu.

5. Information warfare and security by Dorothy E. // Denning Addison-Wesley. – 1998. – December.

6. Joint Publication 3-13 / Information operations/ November 1998 Incorporating change 120 November 140 [Електронний ресурс]. – Режим доступу : http://www.dtic.mil.

7. Hoffman Frank G. Hybrid warfire and chellenges / F. G. Hoffman // Joint Force Quarterly (JFQ). – 2009. – Issue 52, Forth Quarter. – P. 34–39.

8. Strategic information warfare: a new face of war / Roger C. Molander, Andrew S. Riddle, Peter A. Wilson [Електронний ресурс]. – Режим доступу : http://www.rang.org.

9. The future of Information Warfire / Defining [Електронний ресурс]. – Режим доступу : http://www.airpower.maxwell.of.milles.