УДК 659.3:32.019.5(477)
DOI: 10.33663/1563-3349-2020-87-285

В. П. ТАРКІН

ІНФОРМАЦІЙНІ ВІЙНИ: ТЕОРЕТИЧНИЙ АСПЕКТ

Дається визначення дефініції інформаційних війн з різних наукових точок зору. На підставі поліпарадигмального підходу, який видається автору найбільш вдалим, виділяються два види – інформаційно-технічна та інформаційно-психологічна війна. Проведено паралель між інформаційною війною та війною в традиційному сенсі. З метою сприйняття інформаційних війн як процесу практичного виміру ілюструються конкретні приклади інформаційних війн, їх методи, форми та цілі.

Ключові слова: *інформаційна війна, інформаційно-технічна війна, інформаційно-психологічна війна, інформаційна зброя, кібервійна.*

Tarkin Vasiliy. **Information warfare: theoretical aspect**

The article contains a definition of information warfare from a variety of perspectives. On the basis of multisystem approach, which is the most suitable from Author's point of view, two kinds of information warfare have been identified: information technology warfare and information psychology warfare. The Author carries out a comparison between an information and traditional warfares. With a view of understanding of information warfares as a practilcal process, the article provides with illustration of specific examples of information warfares, their types, methodology and goals.

Key words: *information warfare, information technology warfare, information psychology warfare, information weapons, cyberwar.*

Цифрова революція і уміння бути її повноцінним учасником у нашому модерному світі – уже частина антропології: вчити, інформувати, отримувати задоволення і спілкуватися відмовившись від відстані й кордонів... Соціально-економічні, політичні й культурні перетворення нерозривно пов'язані із процесом інформатизації, однак, новий спосіб функціонування суспільства й перехід інформації у розряд цінних ресурсів – це нові виклики, один з яких – інформаційна війна, феномен якої викликає і науковий інтерес.

© *ТАРКІН Василь Павлович* – аспірант кафедри політичних теорій Національного університету «Одеська юридична академія»; ORCID: 0000-0002-1754-9046; e-mail: Twonderchilddd@gmail.com

Метою статті є теоретичний аналіз інформаційних війн, яка досягається шляхом розгляду наукових підходів до визначення терміна «інформаційна війна»; розкриття особливостей інформаційно-технічної й інформаційно-психологічної війни; конкретних прикладів інформаційних війн; виявлення співвідношення війн та інформаційних війн.

Інформаційні війни досліджували вітчизняні науковці О. Вишняков, О. Волович, Я. Жарков, Л. Бєсєдіна, Д. Зеркалов, Г. Почепцов, В. Горбулін, О. Курбан, О. Саєнко та зарубіжні вчені – В. Веприцев, А. Манойло, Д. Фролов, І. Власенко, Н. Волковський, В. Щекотихін, М. Лібікі та ін.

Для дослідження теми у статті використані такі методи: аналіз, синтез, системний, порівняльний, структурно-функціональний, дескриптивно-описовий.

Термін «інформаційна війна» з'явився приблизно у середині 70 х років XX ст., і хоча дефініція відносно нова, саме явище існувало так само давно, як і війна у традиційному сенсі. Троянський кінь у «Іліаді» Гомера – класичний приклад інформаційної війни у літературі, а життєвими прикладами інформаційних війн може бути вчення китайського воєнного теоретика і філософа Сунь Цзи, який говорив, що «будь-яка війна – це обман». До появи сучасних комунікаційних технологій інформаційна війна й інформаційно-психологічна війна були тотожними поняттями, адже зміст інформаційної війни розкривався через таку форму, як пропаганда. Винайдення радіо відкрило можливості радіоелектронної боротьби, оскільки противники намагалися обманути чи контролювати воєнні зусилля ворога за допомогою цього винаходу, а згодом, із розвитком комп'ютерних технологій, кібервійни набули нових масштабів.

На Заході «батьком» інформаційних війн називають ученого-фізика Томаса Рона, який 1976 р., у розпал «холодної війни», у звіті «Системи зброї й інформаційна війна» назвав інформацію найслабшою ланкою збройних сил і оборони [1; 2]. Офіційно цей термін вперше був ужитий у директиві міністра оборони США №3600 від 21 грудня 1992 р. У жовтні 1998 р. Міністерство оборони США ввело в дію «Об'єднану доктрину інформаційних операцій», в якій інформаційна війна визначалася як «комплексний вплив (сукупність інформаційних операцій) на систему

державного і військового управління супротивної сторони, її військово-політичне керівництво, який вже в мирний час призводив би до прийняття сприятливих рішень для сторони-ініціатора інформаційного впливу, а протягом конфлікту повністю паралізував би функціонування інфраструктури управління противника» [1; 3]. У науковий обіг дефініцію «інформаційна війна» ввів американський дослідник М. Маклюен, який проголосив тезу: «Справжня тотальна війна – це війна за допомогою інформації».

У наукових працях термін «інформаційна війна» має дискусійний характер. У рамках психологічної парадигми вона визначається як латентний вплив інформації на індивідуальну, групову, масову свідомість за допомогою методів пропаганди, дезінформації, маніпулювання з метою формування нових поглядів на соціально-політичну організацію суспільства через зміну ціннісних орієнтацій й базових установок особистості [4]. Так, В. Брижко вважає, що «інформаційна війна – це відкриті та закриті цілеспрямовані невідомі інформаційні дії щодо нав'язування противнику небажаної інформації для зміни його поведінки через зміну мислення або для самознищення з метою отримання виграшу в матеріальній сфері» [5, с. 142].

Сучасна наукова література виділяє й іншу точку зору, що базується на соціально-комунікативній концепції інформаційних війн. Згідно із даним підходом у центрі предметного поля не свідомість людей, а сама інформація. Так, М. Радіонов та В. Пірумов вбачають в інформаційній війні форму боротьби сторін із використанням спеціальних засобів і методів впливу на чужі інформаційні ресурси при захисті власного інформаційного капіталу [6]. За визначенням Я. Малика «інформаційна війна – форма ведення інформаційного протистояння між різними суб'єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу заходів із нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери» [7].

У словниковій літературі інформаційна війна тлумачиться як широкомасштабна інформаційна боротьба із застосуванням способів і засобів інформаційного впливу на противника в інтересах досягнення цілей сторони, що впливає [8]. Таке визначення

відображає поліпарадигмальний підхід, дуалізм інформаційних війн, що полягає в їх розподілі на інформаційно-психологічну й інформаційно-технічну як окремі види. Ці види інформаційних війн нагадують її кінетичну версію із полем бою, миротворчими операціями й мирним договором. Тут виграє той, хто влучно оперує засобами пропаганди, хто доручив функції шпигування й саботажу цифровим пристроям. Тепер вони – на відстані й часто анонімні.

Інформаційно-технічна війна будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є порушення нормального функціонування інформаційної інфраструктури (дезорганізація роботи технічних засобів, долання системи захисту, обмеження доступу законних користувачів) з можливістю подальшого несанкціонованого збору, копіювання, блокування, видалення інформації. Синонімом даної дефініції може бути «кібервійна» [9]. Ознаками інформаційно-технічної війни є: 1) економія ресурсів і фінансів – на відміну від розробок збройних технологій інформаційні технології не вимагають значних фінансових ресурсів. Комп'ютер, доступ до Інтернету, експертиза інформаційних систем і доступ до важливих мереж можуть бути єдиним озброєнням; 2) проблема тактичного попередження й оцінки атак; 3) розмиті кордони – значення географічних меж нівелюється під впливом зростання ролі інформаційної інфраструктури, протиборство відбувається у віртуальному просторі. Тепер бої ведуться не лише на суходолі, морі чи повітрі, а й на віртуальному полі битви. Будь-хто може стати учасником війни, не лише воюючи, а й передаючи інформацію, гроші чи технології через он-лайн інфраструктуру.

Інформаційна війна супроводжується низкою інформаційних атак – спробами несанкціонованого впливу на інформаційний простір противника з метою його модифікації у свої інтересах [8]. Виділяють різні форми інформаційних атак: асинхронну, контрольовану, пасивну, активну. Так, внаслідок активної атаки фактично змінюються чи знищуються дані, що зберігаються чи обробляються, чи інші елементи ресурсу, пасивна атака передбачає зняття обмеження на доступ до даних чи зміну порядку контролю доступу до даних.

Мета інформаційно-технічної війни – завдати збитків країнам, закладам, установам, організаціям чи суспільству в цілому в електронному режимі та зруйнувати важливу інфраструктуру; порушити роботу інформаційних мереж таким чином, щоб важливі функції зв'язку, фінансової системи, водопостачання, енергопостачання не працювали, що супроводжується великою збитковістю.

Методи інформаційно-технічної війни:

1) проникнення, видалення чи зміна інформації за допомогою шкідливих програм (віруси, черв'яки, трояни), обходу ненадійних паролів, фішингових атак, схем на кшталт «нори кролика» тощо;

2) дистанційне керування комп'ютерними системами;

3) впровадження скомпрометованого програмного чи апаратного забезпечення, яке працює некоректно; 4) зруйнування ключових сервісів і структури команд шляхом цілеспрямованих атак типу «відмова в обслуговуванні» (DoS-атака);

5) шпигунство – вторгнення у чужі комп'ютерні системи з метою збору інформації.

Так, у 2010 р. в Ірані на заводі із збагачення урану із ладу вийшло 1368 центрифуг, і хоча офіційно іранський уряд вину вірусу Stuxnet, про який говорили спеціалісти не визнав, однак на найвищому рівні атаки на об'єкт визнавалися. Час, потрібний вірусу від перших заражень комп'ютерів до цілих цехів, – один рік. А у 2017 р. уже Європа опинилася «у полоні» вірусу Petya-A, який не оминув і Україну. Вірусом були вражені комп'ютерні системи Укренерго, Київенерго, Епіцентр, Київстар, Vodafone, Lifecell, канал ATR, аеропорт «Бориспіль», мережа автозаправних станцій WOG, Укргазвидобування та ін. Під удар потрапив навіть сайт Кіберполіції України.

Із несподіваним входженням COVID-19 у щоденний словник кількість бажаючих скористатися пандемією зросло. Так, за повідомлення прес-центру СБУ, «з початку карантину хакерські угрупування, зокрема, масово направляють на поштові скриньки державних установ електронні листи на тему коронавірусу. До листів насправді долучені файли із вірусними програмами, які активізуються при відкриванні листа» [10]. Ось так парадоксально любителі «вірусів» користуються вірусом.

Інформаційно-технічна війна – високотехнологічна форма війни традиційної, кінетичної, але заснована на широкій комп'ютеризації та електронізації. Це теж збройний конфлікт, тільки зброя у ньому інформаційно-технічна й програмно-математична. Кібервійна може існувати як самостійне явище, так і супроводжувати звичайні військові дії, збільшуючи їх шанси на успіх. Нині комп'ютери й інформаційні технології присутні в розумних бомбах, а сучасні винищувачі несуть більше десятка комп'ютерів, більшість із яких, якщо не усі, не можуть літати без активованих комп'ютерних систем. Інформаційні технології не тільки включені в озброєння сучасної війни, а й сильно впливають на процес отримання і зберігання розвідувальних даних і стратегічного планування.

Інформаційно-психологічна війна – наміри, зусилля, планові психологічні операції, застосовані до певної аудиторії, з метою впливу на їх свідомість, волю, емоції, мотиви, об'єктивні судження [9]. Інформаційно-психологічна війна, по-перше, публічна, позаяк полягає у впливі на певну авдиторію; по-друге, застосовує різні методи з прихованими мотивами, покликані створити атмосферу, в якій загал найкраще підкориться впливу;по-третє, покликана керувати сприйняттям за допомогою двох ключових понять – «переконання» і «сугестивність».

І. Парфенюк розрізняє дві форми інформаційно-психологічної війни: стандартну інформаційну війну, в якій під час цілеспрямованого інформаційного впливу активно задіяний інформаційний простір, а також культурні цінності, ціннісні орієнтації, символи, світогляд та інші компоненти культурного простору, в якому знаходиться об'єкт впливу, й стратегічну інформаційну війну, під час якої здійснюється вплив на інформаційний та культурний простір об'єкта з метою їх трансформації, що призведе до змін у культурних цінностях, світобаченні та поведінці об'єкта інформаційної агресії [11].

Відкрита й прихована пропаганда – найчастіше вживаний метод інформаційно-психологічної війни, що характеризується комплексом дій – переконання, розповсюдження ідей, думок, доктрин, ідеології, чуток та іншої інформації (чи дезінформації), що впливають на цільову аудиторію з метою її примушування до певного способу поведінки й мислення. Деякі автори навіть

визначають одне поняття через інше. Наприклад, О. Копан та В. Мельник вважають, що «інформаційно-психологічна війна – це використання пропаганди проти ворога, зазвичай, вона спрямована проти певної держави, може бути причиною зміни державної політики чи розладу економічної системи, а в подальшому призвести до активізації дій громадянського суспільства проти власних урядів. Її мета полягає не лише у зміні поведінки противника, а і його мислення, свідомості та поведінки населення» [12]. Й справді, формами пропаганди є і маніпулювання, і поширення чуток, і провокації, однак поряд із нею до методів інформаційно-психологічної війни можна віднести диверсифікацію громадської думки й будь-яку форму створення політичного, культурного, економічного чи соціального тиску. Метод диверсифікації громадської думки полягає у розпорошенні уваги правлячої еліти держави на різні штучно акцентовані проблеми і тим самим відволікання її від вирішення першочергових завдань суспільно-політичного та економічного розвитку [13]. Політичний тиск може проявлятися шляхом протестів, мітингів, демонстрацій; культурний – переглядом або зміною цінностей; економічний – запровадженням санкцій; соціальний – примусом до дій, які окремий індивід не вчинив би, перебуваючи поза межами конкретного колективу.

До завдань інформаційно-психологічної війни належать: 1) ослаблення підтримки конкурента чи ворога з боку населення; 2) ліквідація політичної опозиції; 3) знищення або зменшення ролі організацій, які допомагають конкуренту чи ворогу.

Листівки, плакати, гасла, зображення замінюють бомби, ракети і вогнепальну зброю. Досить вдале формулювання кінцевої мети інформаційно-психологічної війни наводить американський дослідник Джон Стейн у книзі «Інформаційна війна»: «Метою такої війни є розум, особливо розум тих, хто приймає ключові рішення з приводу війни і миру, а з військової точки зору, розум тих, хто приймає ключові рішення стосовно того, коли і як використовувати наявні сили і можливості стратегічних структур» [14].

Інформаційно-психологічна війна застосовується щодо ворогів, союзників і навіть власного населення. Вона може здійснюватися як у мирний час, так і під час воєнних конфлік-

тів. Пропаганда і «ворожі образи» зазвичай супроводжують конфлікти у війні. Ці та інші заходи використовуються цілеспрямовано й комбіновано для дестабілізації суперника. Центральним елементом таких стратегій є часте маніпулятивне використання сучасних засобів масової інформації.

Отже, «інформаційна війна» – термін кінця XX ст., що означає комбінацію людських або технологічних дій, призначених для присвоєння, знищення чи зміни інформації або нав'язування певного бачення реальності. Уміння використовувати широкий спектр інструментів, проводити амбіційні кампанії пропаганди й влучні кібератаки – усе це характеризує інформаційні війни. Циркуляція світу в режимі реального часу вивела нову формулу: рівень техніки=рівень небезпеки. Використовуючи переваги цифрової революції, інформаційна інфраструктура розгортається у глобальному масштабі: технології уже давно попереду гучномовців і розповсюдження листівок повітрям, а психологія впливу на маси тепер вимагає не лише творчого й послідовного спрямування, а й високої адаптивності, імпровізації, психологічного опортунізму й технічних знань.

1. Погрібна В.Л., Герасіна Л.М. Інформаційна війна як каталізатор геополітичних змін. URL: http://dspace.nlu.edu.ua/bitstream/123456789/11320/1/Pogribna_Gerasina_72-75.pdf. **2.** Thomas P. Rona, «Weapon Systems and Information War». Boeing Aerospace Co, Seattle, WA. 1976. **3.** Joint Pub 3–13 «Information Operations», DOD US, December, 1998. URL: https://militera.lib.ru /science/suntszy/01.html. **4.** Кунакова Л.Н. Информационная война как объект научного анализа (понятие и основные характеристики информационной войны). *Альманах современной науки и образования*. Тамбов: Грамота, 2012. № 6 (61). С. 93-96. **5.** е-боротьба в інформаційних війнах та інформаційне право: монографія / В.М. Брижко [та ін.]; за ред. М. Швеця. Київ: НДЦПІ АПрН України, 2007. 234 с. **6.** Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах. *Военная мысль*. 1997. № 5. С. 44-47. **7.** Малик Я. Інформаційна війна і Україна. *Демократичне врядування*. 2015. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf. **8.** Информационная война и защита информации. Словарь основных терминов и определений. Москва, 2011. 68 с. **9.** Міщенко І. В., Басалюк Н.В., Таркін В.П. Інформаційні війни й кібертероризм: поняття, особливості. *Молодий вчений*. 2017. № 10. С. 698-703. **10.** Коронавирусный спам из России: СБУ остановила 103 кибератаки на госучереждения. URL: https://www.ukrinform.ru/rubric-society/3019915-hakery-rf-zabrasyvaut-gosucrezdenia-koronavirusnymi-pismami-sbu-

ostanovila-103-kiberataki.html. **11.** Парфенюк І. Стратегічні та стандартні інформаційні війни в Україні (на прикладі інформаційної агресії РФ). *Український інформаційний простір*. 2014. № 2. С. 298-305. **12.** Копан О.В., Мельник В.І. Інформаційно-психологічна війна як засіб маніпулювання людською свідомістю. Інформація і право. 2016. №2 (17). С. 92-98. **13.** Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. №1. С.136-141. **14.** George J. Stein. Information warfare / AWC. URL: http://www.airpower. maxwell.af.mil/airchronicles/apj/apj95/spr95_files/stein.htm.

References

1. Pohribna V.L., Herasina L.M. Informatsiina viina yak katalizator heopolitichnykh zmin. URL: :http://dspace.nlu.edu.ua/bitstream/123456789/11320/1/Pogribna_Gerasina_72-75.pdf. **2.** Thomas P. Rona, «Weapon Systems and Information War». Boeing Aerospace Co, Seattle, WA. 1976. **3.** Joint Pub 3–13 «Information Operations», DOD US, December, 1998. URL: https://militera.lib.ru /science/suntszy/01.html. **4.** Kunakova L.N. Informatsionnaia voina kak obiekt nauchnoho analyza (poniatye y osnovne kharakterystyky informatsyonnoi voini). *Almanakh sovremennoi nauky i obrazovanyia*. Tambov: Hramota. 2012. № 6 (61). S. 93-96. **5.** e-borotba v informatsiinykh viinakh ta informatsiine pravo: monohrafiia / V.M. Bryzhko [ta in.] ; za red. d.e.n., prof., chlena-korespondenta APrN Ukrainy M. Shvetsia. Kyev: NDTsPI APrN Ukrainy, 2007. 234 s. **6.** Pyrumov V.S., Rodyonov M.A. Nekotorыe aspekti informatsyonnoi borbi v voennikh konflyktakh. *Voennaia mysl*. 1997. № 5. S. 44-47. **7.** Malyk Ya. Informatsiina viina i Ukraina. *Demokramychne vradyvanna*. 2015. Vyp. 15. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf. **8.** Informatsyonnaia voina i zashchyta informatsyy. Slovar osnovnikh termynov i operedelenyi. Moskva, 2011. 68 s. **9.** Mishchenko I. V. , Basaliuk N.V., Tarkin V.P. Informatsiini viiny y kiberteroryzm: poniattia, osoblyvosti. *Molodyi vchenyi*. 2017. № 10. S. 698-703. **10.** Koronavyrusnii spam iz Rossyy: SBU ostanovyla 103 kyberataky na gosucherezhdeniia. URL: https://www.ukrinform.ru/rubric-society/3019915-hakery-rf-zabrasyvaut-gosucrezdenia-koronavirusnymi-pismami-sbu-ostanovila-103-kiberataki.html. **11.** Parfeniuk I. Stratehichni ta standartni informatsiini viiny v Ukraini (na prykladi informatsiinoi ahresii RF). *Ukrainskyi informatsiinyi prostir*. Chyslo 2. 2014. S. 298-305. **12.** Kopan O.V., Melnyk V.I. Informatsiino-psykholohichna viina yak zasib manipuliuvannia liudskoiu svidomistiu. Informatsiia i pravo. 2016. №2 (17). S. 92-98. **13.** Horban Yu.O. Informatsiina viina proty Ukrainy ta zasoby yii vedennia. *Visnyk NADU*. 2015. №1. S.136-141. **14.** George J. Stein. Information warfare / AWC. URL: http://www.airpower. maxwell.af.mil/airchronicles/apj/apj95/spr95_files/stein.htm.

Tarkin Vasiliy. **Information warfare: theoretical aspect**

Information warfares have been originated as a kind of escalation of information conflicts, which is a humanity's global development product, generated in 20th century.

Global digitalization, which is ensured by an intensive informational exchange, has made the international community much more vulnerable; yet a short-term informational transfer delay may lead to a national or even international crysis. Modern scientific and technical revolutions spawned a new types of intensive, dangerous and widescale conflicts. The concept of agression has been also transofrmed to the information agression. The main component of information agression is an information warfare, which may be theoretically split into information technology and information psychology warfares.

The Author carries out a comparison between an information and traditional warfares. With a view of understanding of information warfares as a practilcal process, the article provides with illustration of specific examples of information warfares, their types, methodology and goals.

Nowadays the emphasis in the struggle for economic and politic speheres of influence is shifting from use of the force towards to a flexible and latent forms of agression, among which are information warfare and cyberterorism. The theoretical analysis makes possible to understand, that information warfare is a complex and multifaceted object. The existense of various well-argued concepts is owing to a different scientific schools and methodological frameworks of research area.

Key words: information warfare, information technology warfare, information psychology warfare, information weapons, cyberwar.