

УДК 316 (477)

ДЗЬОБАНЬ О.П., доктор філософських наук, професор, головний науковий співробітник ДНУ ІБП НАПрН України.

ORCID ID: <http://orcid.org/0000-0002-2075-7508>.

ПРУДНИКОВА О.В., доктор філософських наук, доцент, професор кафедри культурології Національного юридичного університету імені Ярослава Мудрого.

ORCID ID: <http://orcid.org/0000-0003-4610-908X>.

СУЧАСНА ВІЙНА: ТРАНСФОРМАЦІЯ ДО МЕРЕЖЕВИХ ФОРМ

Анотація. Зроблена спроба осмислення трансформації війни як соціокультурного феномена з акцентом на актуалізації нового виду зброї – інформаційної зброї. Обґрунтовується, що мережеві війни є специфічним видом інформаційних війн. Показано, що процеси розвитку інформаційної війни та її технологічного інструментарію пов'язані зі зміною типу наукової раціональності в ході історичного розвитку людини та суспільства. Акцентується увага, що мережева війна є фактором формування соціальних страхів і “екзистенційного вакууму”, оскільки інформаційний простір активно впливає на суспільні відносини і сферу безпеки. Обґрунтовується висновок, що у центрі війни, як і раніше, залишається людина, її воля, і мережево-центрична війна є людино-центричною, або такою, що в неї немає будь-якого центру взагалі.

Ключові слова: інформаційно-мережевий вплив, інформаційні технології, інформаційна зброя, інформаційна війна, мережева війна, мережево-центрична війна.

Summary. An attempt at epistemological knowledge is made with regard to the transformation of war as a socio-cultural phenomenon with an emphasis on the actualization of a new type of weapon – an information weapon. It is justified that network wars are a specific type of information wars. It is shown that the processes of the development of information warfare and its technological tools are connected with the change of the type of scientific rationality in the course of the historical development of man and society. It is emphasized that the network war is a factor in the formation of social fears and “existential vacuum”, since the information space actively affects social relations and the sphere of security. The conclusion is substantiated that at the center of war, as before, remains a person, their will, and network-centric war is human-centric, it does not have any center at all.

Keywords: information and network influence, information technologies, information weapons, information war, network war, network-centric war.

Постановка проблеми. Знайомлячись із змістом найбільших світових стародавніх пам'яток літератури, релігії та культури, можна переконатися у тому, що вони розповідають насамперед про конфлікти, протистояння, боротьбу, війни як найбільш значні події в історії людства. Складається враження, що за всіх часів люди тільки тим і займалися, що постійно воювали один з одним, а в період між війнами готувалися до нових зіткнень.

Протягом тисячоліть збройні конфлікти та війни виникали і велися з метою ненаситного, жадібного збагачення та встановлення необмеженої влади для невеликої кількості панівних еліт. Подібні претензії еліт існували в усі часи у всіх суспільно-економічних формаціях, але, як справедливо зазначає К. Долгов, “найбільшою мірою вони стали притаманні елітам того ладу, який одержав назву капіталізму і який існує досі” [1].

Боротьба держав в інформаційному просторі ведеться декілька тисячоліть за зони політичного і економічного впливу, джерела сировини, ринки збуту і території. Вона постійно ведеться і сьогодні на міжнародній арені та всередині кожної держави, в першу чергу за владу, власність та політичний вплив, за можливість маніпулювати настроями та поведінкою великих мас людей. У різні епохи інформаційні процеси відображали актуальні на той час технології. Це позначалося на особливостях проведення відповідних інформаційних протистоянь. Головні відмінності інформаційних процесів різних епох визначалися за такими параметрами, як-от: технології виробництва інформації, засоби накопичення та зберігання, носії інформації (матеріальні або нематеріальні) та виробники інформації.

Отже, уся історія людства – це історія війн і збройних конфліктів, яка сьогодні, в умовах інформаційного суспільства, є надто близькою до апокаліпсису. У зв'язку з цим уявляється цілком доцільним навести висловлювання видатного сучасного вченого, лінгвіста, філософа, громадського діяча Ноама Хомського, який, відповідаючи на запитання кореспондента “Євроньюс” у програмі “Глобальний діалог” про загальну картину сучасного світу – чи вселяє вона оптимізм чи песимізм, – дає образну, жахливу, апокаліптичну відповідь: “На глобальному рівні ми мчимо до прірви і сповнені рішучості у неї впасти, що різко знижує наші перспективи на гідне виживання” [2].

Результати аналізу наукових публікацій свідчать про те, що незважаючи на зростаючий інтерес до дослідження різноманітних проблем сучасного насильства, проблема комплексного розуміння феномена мережевих війн усе ще залишається недостатньо дослідженою. Оскільки на даний час поняття “мережева війна” у вітчизняній науковій лексиці ще залишається певною соціально-політичною, соціально-економічною та культурною новацією, неологізмом, то виникає необхідність його концептуалізації. Особливої й першочергової уваги потребує уточнення особливостей трансформації змісту і форм мережевих війн, їх місця й ролі у широкому комплексі сучасних проявів насильства.

Мета статті є уточнення ключових аспектів трансформації війн стосовно мережевих форм і змісту та окреслення їх основних цілей і спрямованості.

Виклад основного матеріалу. У сучасному розумінні війна – це “конфлікт між політичними утвореннями (державами, етносами, політичними угрупованнями тощо) що відбувається у формі збройного протиборства, воєнних (бойових) дій між їх збройними силами; регулюється законами та звичаями – сукупністю принципів і норм міжнародного права, які встановлюють обов’язки воюючих сторін (забезпечення захисту цивільного населення, регулювання ставлення до військовополонених, заборона на використання особливо нелюдських видів зброї)” [3, с. 146-148].

На початку ХХІ ст. фактори несилкових форм ведення боротьби, які відігравали раніше другорядну роль, вийшли на перший план у спектрі технологій, що застосовуються у сучасних збройних та незбройних конфліктах, управління якими перемістилось з поля бою у глибинний інформаційний простір. У цьому просторі сформувалися численні соціальні мережі, котрі не знаходяться під контролем держав. Це дозволило проводити тотальний моніторинг суспільних настроїв, здійснювати на них вплив і маніпулювати ними у реальному часі. Характерною рисою цього є те, що на відміну від попередніх методів впливу під зовнішній керований контроль беруться мотивації учасників суспільних процесів, а керівників держав і міжнародних організацій змушують робити поспішні та недалекоглядні кроки. Бойові операції, що супроводжуються наступами численних армій та окупацією території противника, хоча і залишаються формами збройної боротьби, однак втрачають свою актуальність. У

сучасних умовах вирішення задач може досягатися в іншому не силовому форматі, що характерно для сучасної політики великих держав. Як зазначає О. Дугін – “...метою мережевих війн є досягнення абсолютного контролю над усіма учасниками історичного процесу у світовому масштабі” [4, с. 159].

У кінці ХХ ст. розвиток збройних сил передових у технічному відношенні країн наблизився до певної точки біфуркації. Незважаючи на найсучасніше озброєння флот, авіація і наземні війська на полі бою стали зазнавати значних труднощів під час проведення спільних операцій. Певною відповіддю на виникнення цієї проблеми стала поява концепції мережево-центричної війни (*network-centric warfare*) [5]. За роки, що минули з моменту зародження цієї концепції, накопичилася ціла низка кардинальних технологічних змін. Як зазначають А. Скорик і С. Ярош – “...мережевий простір став звичним для людини. У цьому достатньо легко переконатися, просто діставши свій смартфон і усвідомивши, що проблеми мереж більше не існує. Вони доступні нам буквально на кінчиках пальців. Ще років двадцять тому вважалося, що світ захоплять складні алгоритми, які будуть хитро переробляти відносно прості дані. Але виявилось, що центр ваги зусиль проектувальників зміщується до роботи зі складними даними. Світ знов підійшов до чергової точки біфуркації – вибору подальшого шляху розвитку. З урахуванням цього, як один із перспективних шляхів розвитку озброєння та військової техніки може розглядатися створення дата-центричних систем, оптимізованих для ведення бойових дій в єдиному інформаційному просторі” [6, с. 26], що у технологічному плані й визначає появу та розвиток концепції мережево-центричної війни.

Як зазначалося нами раніше, поняття *мережевої війни* – це новий якісний рівень розуміння цілей і завдань сучасної війни, збройних конфліктів. У сутнісному плані мережева війна зводиться до особливої форми ведення конфліктів, коли їх учасники застосовують мережеві форми організації, доктрини, стратегії та технології, максимально пристосовані до умов сучасного етапу розвитку інформаційного суспільства.

У концепції мережевих війн основним поняттям є термін “мережа” – новий інформаційний простір, у якому і розгортаються основні стратегічні операції (війни) як розвідувального, так і воєнного характеру, а також відбувається їхнє медійне, дипломатичне, економічне, технічне та інше забезпечення.

Мережева війна, на відміну від мережецентричної, заповнює весь соціокультурний простір, пронизує соціально-політичні, соціально-економічні, культурні та ідеологічні процеси і метою мережевих війн є досягнення абсолютного контролю над усіма учасниками історичного процесу у світовому масштабі.

Мережева війна здійснює тотальне руйнування базових характеристик певної нації у всіх типах геополітичних просторів і здійснюється, як правило, у прихованій формі.

У рамках теорії *мереже-центричних війн* військова могутність країни, суспільна думка, дипломатія, соціальні процеси, розвідка й контррозвідка тощо є елементами єдиної мережі, між якими здійснюється постійний інформаційний обмін. У зв’язку з цим, зміст військової реформи в рамках теорії мережецентричних війн полягає у створенні потужної й всеосяжної глобальної мережі, яка здатна концептуально замінити собою колишні моделі й концепції військової стратегії, інтегрувати їх у єдину систему. У таких умовах війна стає мережевим явищем, а військові дії – різновидом мережевих процесів [7].

На початку ХХІ ст. інформаційна боротьба та інформаційні мережні операції остаточно перестали вважатися вельми теоретичною проблемою та перейшли до практичної площини. Концепція мережних воєн, яка була свого часу розроблена Пентагоном, на сучасному етапі реалізується на державному та військовому рівнях. Для

держави мета інформаційного протиборства в широкому сенсі слова міститься в послабленні позицій конкуруючих держав, підриві їх національно-державних підвалин, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери існування суспільства, проведенні психологічних операцій, підривних атак та інших деморалізуючих пропагандистських акцій [8 – 10].

Сила концепції інформаційно-мережевого впливу, як справедливо стверджують А. Шумка і П. Черник, полягає в інтеграції зусиль з чотирьох напрямів: фізичного, інформаційного, інтелектуального та соціального. Це досягається формуванням механізмів управління поведінки великих мас людей, які забезпечують перемогу супротивнику несилowym шляхом – не за рахунок знищення збройних сил супротивника, а за рахунок впливу на його морально-психологічний стан [9, с. 245].

Зіштовхуючись з безліччю викликів і загроз складного, динамічного середовища безпеки ХХІ століття, суспільства й держави змушені адаптуватися, ініціюючи процес трансформації своїх ключових сфер, частиною якої стають революційні зміни у політичному й воєнному мисленні на організаційному й доктринальному рівнях, що відображається, зокрема, у рефлексивності від мережевих до мережево-центричних війн.

Сучасне суспільство поступово стає все більш інформаційним, не тільки через те, що воно насичується інформацією та інформаційними технологіями, а й тому, що його соціальний і економічний розвиток залежать від володіння адекватною інформацією та від уміння правильно користуватися нею. Головну роль у такому суспільстві відіграє інформація, причому точна, доступна і своєчасна. На цій підставі інформація перетворюється в третій вид ресурсів, поряд з речовиною і енергією. Усе це веде до того, що в усьому світі відбувається поступова інформатизація суспільства. Поява мікроелектроніки, котра відкрила можливості для масової комунікації, у поєднанні з інформаційно-комп'ютерними технологіями (далі – ІК-технології) породили мережеві інформаційні структури, а разом з ними і концепцію інформаційно-мережевих війн.

У сучасних умовах тотального впровадження ІК-технологій перевагу одержує не той, хто в стані застосовувати інформаційні й мережні технології, що стає буденністю, а той, хто зробить це найбільш ефективним чином, буде більш рухливим й адаптивним. У нових умовах критичним стає фактор часу і здатність скорочувати цикли часу у всіх процесах управління військовою організацією й державою [11 – 12].

Сучасні темпи розвитку ІК-технології перевершили всі очікування і спростували навіть найсміливіші прогнози. Можливості апаратури зростають зараз набагато швидше, аніж очікувалося в численних прогнозах десятирічної давності. У результаті відповідна інфраструктура, яка будувалася на основі вчорашніх прогнозів, сьогодні виявляється неспроможною перед обличчям інформаційного вибуху [10].

У військовій справі пріоритети інформаційного розвитку пов'язані з військово-технічною революцією, яка відбулася в 80 – 90-х роках ХХ ст., і спрямовані насамперед на розробку ефективних засобів управління та зв'язку, інтелектуалізованих систем озброєння (високоточна зброя) тощо. Поряд із цим відбувається диференціація картини можливих війн у бік неklasичних типів її ведення, у яких значну роль завойовує концепція інформаційної війни. Виходячи з цього, інформаційна війна трансформується в інструмент політичного тиску, що має децентралізований, розосереджений, квазірізномний, мережевий характер; вона постає як цілеспрямований комплекс потайних, “м'яких” і деструктивних технологій впливу на масову суспільну свідомість, основне ядро яких складає соціогуманітарний компонент.

Новацією війн інформаційної епохи є не лише стирання кордону між війною та мирними формами протиборства, але й перенесення центру ваги протиборства в інформаційну площину. Неочікуваний успіх поєднання технологій руйнування основ державності з ІК-технологіями у соціальних мережах неодноразово показав на практиці можливості та ефективність такого поєднання.

Актуалізується новий вид зброї – інформаційна зброя, потенціал якої отримує глобальне визнання і чіткішу класифікацію. В авторитетних наукових публікаціях щодо інформаційної зброї вживають термін “зброя масових руйнувань” (*weapon of mass disruption*) на противагу традиційному “зброя масового знищення” (*weapon of mass destruction*). Відповідно, як зазначає О. Сенченко, інформаційна зброя отримує ранг найвищого пріоритету [13, с. 36].

Мережеві війни є специфічним видом інформаційних війн. Використання Інтернету в інтересах війни може як спричиняти позитивні, нешкідливі наслідки, так і руйнувати та завдавати тяжких збитків ІК-технологіям, системам та людям, країнам. Використання хакерських технологій та прийомів підривного характеру задля завдання тяжкої (іноді навіть матеріальної) шкоди несе той негативний відбиток мережної війни, з яким намагається боротися кожна країна окремо та світова спільнота в цілому. Мережеві війни поступово витісняють традиційні війни, адже подальший розвиток комунікаційних технологій, мережевих практик та технічного прогресу загалом лише сприяє переходу від затратної та чисельної за жертвами війни до мережної війни, яка є набагато вигіднішою та легшою [14, с. 283].

Процеси розвитку інформаційної війни та її технологічного інструментарію пов'язані зі зміною типу наукової раціональності в ході історичного розвитку людини та суспільства. Зміни у розвитку уявлень про інформаційну війну можна представити у вигляді наступного ланцюжка етапів:

- а) сприйняття інформаційної війни як безсистемного, стихійного впливу на супротивника шляхом обману (докласичний етап);
- б) лінійно-механістичне сприйняття (класичний етап);
- в) системна форма ідеологічного впливу на супротивника (некласичний етап);
- г) децентрований, мережевий характер сприйняття за допомогою формування (появи) соціогуманітарних технологій та їх використання (постнекласичний етап).

Аналіз концепції “мережево-центричної війни” дозволяє зробити висновок, що це не новий специфічний спосіб або форма ведення війни, а лише *спосіб інтеграції технічних засобів розвідки, автоматизації управління і вогневого ураження за допомогою інформаційно-телекомунікаційних мереж зв'язку та передачі даних з метою підвищення ефективності ведення бойових дій шляхом узгодження та координації дій наявних сил і засобів на основі єдиного інформаційного простору і прискорення, внаслідок цього, темпів операцій й ефективності ураження супротивника* [15]. Причому, як справедливо зазначає М. Куц, інформація для такої війни може бути як метою, так і зброєю [14, с. 283].

Акцентуємо увагу на основних характерних особливостях мережевих війн, до яких відносяться [7]:

- інформаційна сфера (така ж сфера бойових дій, як повітряно-космічний, морський і наземний простір);
- асиметричний характер, тобто держава, що має невеликі збройні сили, може завдати серйозної шкоди державі, яка значно перевершує її за кількістю збройних сил;
- ведення мережевих війн безпосередньо або побічно впливає на події в реальному світі;

- мережеві війни суттєво впливають на когнітивні й емоційні процеси людей, на їх сприйнятливність і оцінку подій, на рішення, що приймаються;
- неясність і невизначеність правил застосування, відсутність повноцінних даних про можливості, швидкість та ефективність реакції радіоелектронних засобів і окремих елементів різних комп'ютерних систем;
- наявність труднощів у розпізнаванні навмисних і ненавмисних (випадкових) дій і процесів у кіберпросторі;
- необхідність одночасного використання сил і засобів операцій як для впливу на противника, так і для захисту своїх збройних сил і сил союзників;
- відстань до цілі впливу не має значення;
- противник може наносити атаки анонімно і приховано;
- метою мережевих війн є забезпечення ефективності бойових дій в умовах мережевого управління військами тощо;
- успіх мережевих війн ґрунтується на методології використання інтегрованих можливостей усіх сил інформаційних операцій, сил їх забезпечення або пов'язаних з їх застосуванням.

Ще раз наголосимо, що мережево-центрична війна має принципові відмінності від мережевої війни, оскільки, у широкому сенсі мережева війна – це війна мережі проти ієрархії, що ведеться мережевими структурами проти ієрархічних структур з використанням мережевої стратегії і мережевих методів. Мережева війна йде на більш тонких рівнях, з використанням інформаційних технологій, дипломатичних мереж, неурядових організацій, з підключенням журналістів, ЗМІ, блогерів і всього іншого арсеналу інформаційного суспільства, що лежить в парадигмі постмодерну. У зв'язку з цим, мережеву війну можна визначити як соціально-політичну, соціально-економічну та культурну інновацію на основі інформаційно-комунікативних технологій, що застосовується інститутами управління, певними групами для досягнення цілей управління й контролю. Мережеві агресивні дії в умовах мережевих війн провокують людину на прийняття ризикованих дій, що в свою чергу створює більш нестабільну соціокультурну ситуацію, що, в результаті, сприяє досягненню цілей мережевих війн [15 – 16].

Зазначимо, що мережева війна має два аспекти: технологічний і соціальний. Мережева війна у технологічному аспекті – це війна, в якій використовуються ІК-технології і нові можливості мережевої комунікації. Мережа тут використовується як механізм. У цьому аспекті слід виділити найбільш поширені у сучасних мережевих комунікаціях військові атаки – кібератаки. Суттєвими визнаються результативні кібератаки на державні установи, оборонні та високотехнологічні компанії, а також економічні кіберзлочини з фінансовим збитком. Наприклад, до таких кібератак можна віднести оприлюднення компанією Google у 2010 р. факту проведення висококваліфікованої кібератаки, результатом якої став злом її мереж поряд з мережами ще 30 інших американських компаній. Метою атаки був збір технологій і забезпечення доступу до системи управління паролями.

Існує піраміда кіберзагроз: в основі знаходяться загрози, які використовуються в атаках на рядових користувачів з боку традиційних кіберзлочинців, що спонукається виключно міркуваннями власної фінансової вигоди. На середньому рівні – загрози, що використовуються в цільових атаках корпоративного кібершпіонажу, а також так звані поліцейські програми-шпигуни, що застосовуються державами для шпигунства за своїми громадянами й компаніями. Верхівка піраміди – кіберзагрози, створювані

державами для проведення кібератак на інші держави, що є структурним елементом мережевої війни.

Загалом, інформаційно-мережеве протиборство охоплює такі сфери [11, с. 17-19]:

- географічну – встановлення контролю над територією планети чи країною противника за допомогою глобальних інформаційних і розвідувальних систем, заохочення сепаратистських рухів і терористичної активності в різних формах на території противника для його ослаблення, залучення противника в конфлікти малої інтенсивності, а також організація заворушень і “кольорових” революцій;

- економічну – нав’язування противнику кабальних кредитів, введення ембарго та економічних санкцій, а також залучення до членства в різних неефективних міжнародних економічних організаціях;

- ідеологічну – використання брехні, спотворення інформації, підміни понять, внесення ментальних вірусів і міфологем у свідомість населення противника;

- мережеву – організація хакерських атак і внесення комп’ютерних вірусів різного роду в обчислювальні і комунікаційні системи та бази даних противника.

Сили, які залучаються для підготовки та реалізації мережевої війни є розгалуженою мережею добре поінформованих, але географічно розсіяних центрів, що мають при цьому постійний доступ до всієї необхідної інформації. Сенс мережевої війни якраз і полягає у формуванні суспільної думки та соціально-політичних процесів таким чином, щоб їх суб’єкти або не чинили опір трансформаціям, що відбуваються, або навіть несвідомо брали участь у цих трансформаціях. Мережева війна є “інструментом дій для найширших верств населення, у чому переконали численні події останніх років, хоча техніки та тактики мережевої війни можуть цілком застосовуватися і військовими, і політичними спільнотами” [20]. У ній неможливо однозначно визначити супротивника і лінії фронту, що розділяє території, підконтрольні сторонам, що воюють.

Основним засобом ведення усіх мережевих війн є проведення так званих “операцій базових ефектів” [20, с. 339], які визначаються як “сукупність дій, спрямованих на формування моделі поведінки друзів, нейтральних сил та ворогів у ситуації миру, кризи та війни” [21]. Операції базових ефектів припускають план прямого планетарного контролю нового типу, коли управлінню підлягають не суб’єкти, а їх мотивації, дії, наміри тощо. Однак для досягнення головної мети мережевої війни необхідне вирішення цілої низки окремих завдань [6 – 11, 20, 22, 23]:

- створення атмосфери аморальності та бездуховності, негативного ставлення до культурної спадщини населення країни-супротивника;

- маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення країни на користь створення обстановки політичної напруженості та хаосу;

- дестабілізація політичних відносин між партіями, об’єднаннями та рухами з метою провокації конфліктів, розпалювання атмосфери недовіри та підозрілості;

- загострення політичної боротьби, провокування репресій проти опозиції;

- зниження рівня інформаційного забезпечення органів влади та управління з метою ускладнення прийняття важливих рішень;

- дезінформація населення про роботу державних органів, піддрив їхнього авторитету, дискредитація органів управління;

- провокування соціальних, політичних, національних та релігійних зіткнень;

- ініціювання масових заворушень та інших акцій протесту;

- піддрив міжнародного авторитету держави, її співпраці з іншими країнами;

- заподіяння шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах;
- розв'язання у суспільстві громадянської війни.

Отже, у даний час активно формується нова глобальна соціальна реальність, яка діалектично поєднується з локальною мережевою соціальною реальністю. Світ на глобальному й на локальному рівнях стикається з ускладненням соціокультурної динаміки суспільства, небаченими раніше біфуркаціями, новими різновидами агресії й силового протистояння. В умовах глобалізації конкретні культури, піддаючись змінам, починають не тільки активно протидіяти, але й рефлексувати, прагнучи підтримувати свою ідентичність, нерідко залучаючи для цього різноманітні сучасні засоби й способи ведення війни.

Сьогодні цілком зрозуміло, що контроль інформації й управління її потоками здійснює суттєвий вплив на суспільні процеси. У той же час, війна в традиційній формі за участю держав, що володіють ядерною та руйнівною високоточною зброєю, є надзвичайно небезпечна. Це може призвести до катастрофи, в результаті котрої будуть назавжди втрачені геополітичні ресурси всіх учасників конфлікту: територія, економіка, завдані збитки природним ресурсам та населенню. Тому, завданням ідеологів інформаційно-мережових війн є перенесення центру протистояння з матеріальної сфери в інформаційну. Для цього здійснюється прихована трансформація ментального поля населення тих країн, які є ціллю у інформаційно-мережовій війні. Для цього, в першу чергу, здійснюється переорієнтація, а потім знищення традиційних духовних і культурних цінностей народу. При цьому, як влучно зазначають А. Шумка і П. Черник, “здійснюється свого роду анестезія, психологічне знеболення, виконуване для того, щоб інформаційно-мережеве вторгнення сприймалось суспільством-жертвою як добровільне бажання слідувати шляхом загальнолюдського прогресу. У масовій свідомості народу противник намагається представити це у вигляді природної, дружньої та цивілізованої форми трансформації свого архаїчного, відсталого в розвитку суспільства з боку іншого, більш високорозвиненого суспільства, яке протягує йому руку допомоги” [9, с. 246].

Аналізуючи процес трансформації сучасних війн у бік мережових форм, варто згадати думку Г. Почепцова, який наголошує на тому, що сьогодні інформаційні війни, перш за все, ведуться за допомогою інтелектуального інструментарію, а безпосереднім середовищем для їх використання є, зокрема, соціальні мережі. Також він відзначає створення нового методу впливу на громадську думку, що отримав назву мікротаргетингу і полягає у публікації персоналізованих повідомлень на рівні окремої людини для привернення її уваги та завоювання прихильності [22].

Висновки.

Таким чином, мережева війна – це війна нового покоління, якісно новий рівень міждержавного протистояння та воєнного мистецтва, форма геополітичного насильства з залученням великої кількості суб'єктів у комплекс різноманітних мереж, передусім інформаційних. Як зазначалося у наших попередніх публікаціях, основною ідеєю мережових війн є інформаційний вплив на людину і суспільство з метою управління та регулювання суспільних процесів у глобальному масштабі. Тому, будь-яка мережева війна призводить до руйнування базових цінностей народу й держави, національної, конфесійної та культурної ідентичності, також, інформаційний та ідеологічний вакуум обмежує стратегічний вибір країни у глобалізованому світі й робить її частиною системи планетарного контролю. У зв'язку з цим, фронт мережевої війни розташовується у ментальному просторі, де метою супротивника є руйнування традиційних базових цінностей даної нації й імплантація власних [15; 16; 23; 24].

Мережева війна здійснює тотальне руйнування базових характеристик певної нації у всіх типах геополітичних просторів і здійснюється, як правило, у прихованій формі. У зв'язку з цим, загострюється проблема дослідження характерних особливостей і принципів мережевих війн і їх впливу на безпеку особистості, суспільства й держави.

Ефективність мережевої війни розкривається у процесі створення інформаційно-мережевого механізму, який забезпечує маніпулятивну й дестабілізуючу функції мережевих війн, здатних тотально і в глобальних масштабах впливати на процеси демократизації, життєдіяльності людини і сучасного суспільства у цілому.

Глобальні соціокультурні трансформації у сучасному суспільстві “тотального ризику” детермінують зміни адаптаційних механізмів людини й суспільства, деформують систему їх безпеки. Одна з цілей впливу мережевих війн на суспільство – це руйнування смислової єдності світу й людини, у зв'язку з чим руйнуються базові цінності народу й держави, національної, конфесійної та культурної ідентичності. Тому, мережева війна є фактором формування соціальних страхів і “екзистенційного вакууму”, оскільки інформаційний простір активно впливає на суспільні відносини і сферу безпеки. В центрі війни, як і раніше, залишається людина, її воля, і мережево-центрична війна є людино-центричною, або такою, що в неї немає будь-якого центру взагалі.

Використана література

1. Долгов К. Современные войны и вооруженные конфликты: истоки, причины и пути решения. URL: <https://interaffairs.ru/news/show/14724> (дата звернення: 07.09.2022).
2. Хомский Н. Мир мчится к пропасти. URL: <https://ru.euronews.com/2015/04/17/chomsky-says-us-is-world-s-biggest-terrorist> (дата звернення: 09.09.2022).
3. Війна. Соціологія права: енциклопедичний словник / Герасіна Л.М., Панфілов О.Ю., Погрібна В.Л., Требін М.П.; за ред. М.П. Требіна. Харків: Право, 2020. С. 146-148.
4. Дугин А. Геополитика постмодерна. Санкт-Петербург: Амфора, 2007. 382 с.
5. Alberts D., Garstka J., Stein F. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, DC: CCRP Publication Series, 1999. 287 p.
6. Скорик А.Б., Ярош С.П. Еволюційний розвиток концепції мережево-центричних війн, системно-концептуальні основи теорії дата-центричних операцій. *Наукові праці Харківського національного університету Повітряних Сил*. 2020. № 4. С. 26-34.
7. Данильян О.Г., Дзьобань О.П. Феномен мережевих війн: до проблеми філософського осмислення. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2021. № 3 (50). С. 11-27.
8. Бережна М.С. Інформаційні та мережні війни у військових доктринах США. *Наукові праці Чорноморського державного університету імені Петра Могили. Сер. Історія*. 2010. Т. 129. Вип. 116. С. 77-80.
9. Шумка А.В., Черник П.П. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. *Військово-науковий вісник*. 2013. Вип. 19. С. 243-255.
10. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. 558 с.
11. Дзьобань О.П., Соснін О.В. Мережево-комунікативний простір управління. *Гуманітарний вісник Запорізької державної інженерної академії*. 2015. Вип. 63. С. 174-186.
12. Лаврінчук О.В., Валерко В.В., Цветков Є.В. Аналіз основних напрямків впровадження принципів мережецентричних війн у збройних силах провідних країн світу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2012. № 2. С. 87-93.
13. Сенченко О. Інформаційно-мережеві війни – стратегічні війни другого покоління. *Вісник Книжкової палати*. 2016. № 10. С. 36-40.

14. Куц М.Ю. Мережні війни: сутність та основні характеристики. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія.* 2015. № 2. С. 277-286.

15. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию. Москва: Евразийское движение, 2011. 130 с.

16. Данильян О., Дзьобань О. Мережеві війни як форма інформаційної експансії: матеріали Міжнародної науково-практичної конференції *Актуальні проблеми сучасних міжнародних відносин*, м. Дніпро, 5 – 6 лист. 2021 р. Дніпро: ПринтДім, 2021. С. 92-95.

17. Ковалевич Б.В. Соціальні мережі як новий інструмент ведення інформаційних війн у сучасному світі. *Грані.* 2014. № 4. С. 118-121.

18. Курбан О.В. Інтернет-технології та онлайнві соціальні мережі у сучасній гібридній війні. *Наукові записки Української академії друкарства.* 2017. № 1. С. 264-273.

19. Сенченко О. Мережевий інструментарій нових війн. *Вісник книжкової палати.* 2017. № 1. С. 37-41.

20. Ганнова О.С. Сетевая война: сущность и содержание. URL: <https://cyberleninka.ru/article/n/setevaya-voyna-suschnost-i-soderzhanie> (дата звернення: 09.09.2022).

21. Smith, Edward A., Jr. Effects Based Operations: Applying Network-centric Warfare in Peace, Crisis, and War. URL: <https://go.gale.com/ps/i.do?id=GALE%7CA118039873&sid=google Scholar&v=21&it=r&linkaccess=abs&issn=00281484&p=AONE&sw=w&userGroupName=anon%7E1650e512> (дата звернення: 08.09.2022).

22. Почепцов Г. Інформаційна війна як інтелектуальна війна. URL: <http://osvita.media.sapiens.ua/material/13303> (дата звернення: 10.09.2022).

23. Contextos Humanistas. Expresiones para el Siglo XXI. Cerdeña: Fondazione Giovannino Pinna, 2022. 90 p.

24. Getman A.P., Danilyan O.G., Dzeban A.P., Kalynovskyi Yu.Yu. Modern ontology: reflection on the continuity of cyberspace and virtual reality. *Revista de Filosofia.* 2022-3 (Sep-Dic). Vol. 39. № 102. P. 78-94.

~~~~~ \* \* \* ~~~~~