Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Університет Ауреля Влайку (Румунія)
Центральна бібліотека Болгарської академії наук (Болгарія)
Коледж Санта-Фе (США)
Державний університет Сан-Паулу(Бразилія)
Університет Метрополітен Лондон (Великобританія)
Західноукраїнський національний університет (Тернопіль)
Державний архів Полтавської області
Центральна бібліотека Полтавської міської територіальної громади

Документно-інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи

МАТЕРІАЛИ
VIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

23 листопада 2023 року

Полтава

УДК 355.01+327.8

Руслан Гула
м. Харків

МЕРЕЖЕВА ВІЙНА В СУЧАСНИХ РЕАЛІЯХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

На початку XXI ст. чинники несилових форм ведення боротьби, які виконували раніше переважно допоміжну функцію, набули пріоритетного значення у спектрі комплексу технологій інформаційно-психологічного впливу, що застосовуються в сучасних конфліктах. Управління останніми змістилось у глобальний інформаційний простір, де сформувалися численні соціально-комунікативні мережі, що є практично неконтрольованими. Це дає можливість сторонам інформаційного протиборства проводити тотальний моніторинг суспільних настроїв, здійснювати на них вплив і маніпулювати ними у реальному часі.

Своєрідним «полігоном» апробації, кореляції та трансформації змісту інформаційних потоків є поняття мережі, оскільки «інформаційні війни в сучасних умовах ведуться не державами, а численними некомерційними, суспільними організаціями – фондами, центрами, інститутами, лігами, що формуються державою-агресором» [1]. Тому підготовка до конфлікту в глобалізованому світі потребує переходу до нових форм організації, особливо до універсальної, надійної, багатоканальної системи сукупності каналів і зв’язків.

Мережа є основою, необхідною інфраструктурою, головною передумовою існування мережевого суспільства. При цьому підході поняття **«мережі»** визначається як інтегрована *система* інформаційних

комунікацій ЗМІ, ЗМК та інтеграційний *процес* перетворення технічних засобів передачі інформації і мережевих структур (*засоби зв'язку, масмедіа, транснаціональні корпорації, релігійні організації, неурядові організації, соціальні інститути, політичні партії, спецслужби різних держав, мережі закладів швидкого харчування, молодіжних клубів, «розкрутки» брендів (мемів*)) на спільну, надзвичайно гнучку й мультифункціональну структуру для ведення підривної діяльності в усіх сферах життя суспільства та політичній системі держави-конкурента з метою руйнування її національної безпеки.

Структура мереж має чотири рівні: організаційний, доктринальний, технологічний і соціальний [2, с. 17–18].

Організаційний рівень визначає розмір актора або їх (акторів) комбінації, організованої в мережу, та дійову особу, яка призначена для ведення мережевої війни. Організаційна особливість мережі полягає ще в тому, що незначні збої не здатні вивести систему з ладу, вона спроможна до відтворення потрібного потенціалу та подальшої успішної діяльності. Також цей рівень визначає потенційну можливість з'ясування того, що утримує мережу від розпаду та дозволяє її членам діяти стратегічно й тактично без центрального командування або лідера.

Доктринальний рівень розкриває специфіку процесу об'єднання членів у мережу (доктрини, ідеології, інтереси та інші причини або мотивації для того, щоб вони використовували таку форму). Тобто визначальну роль у створенні та функціонуванні мереж відіграє не сила, а ідея, не воїни, а ідеологи, а також можливість та способи передачі інформації [3]. Оскільки за принципом мережевості чимало людей працюють з однією метою різними за чисельністю групами, діють узгоджено, керуючись ідеєю, то їх робота є ефективною.

Технологічний рівень розкриває специфіку технології, що підтримує мережу, здібності, щільність інформаційних і комунікаційних потоків.

Соціальний рівень відповідає рівню взаємозв'язку між членами мережі. Це класичний рівень аналізу соціальної мережі, де потужні персональні зв'язки, часто на основі спорідненості, етнічної та релігійної приналежності, дружби та спільного досвіду допомагають гарантувати більш високий рівень міжособистісної довіри, аніж в інших формах організацій, наприклад, ієрархічних.

Отже, «*мережа»* – новий інформаційний простір, у якому розгортаються основні стратегічні операції (війни) як розвідувального, так і воєнного характеру, а також відбувається їх медійне, дипломатичне, економічне, технічне та інше забезпечення [2, с. 13].

Мережевість як *характеристика* виявляється у підвищенні ролі інформації в житті суспільства, у можливостях її передавання, багатоканальності шляхів комунікації, зростанні чисельності віртуальних комунікацій, комп'ютеризації населення [3].

Метою мережевої війни є домінування інформаційного впливу, конструювання масової свідомості, формування моделі поведінки ворога, а також союзних і нейтральних сторін за допомогою використання інструментарію мережевих структур.

Головний *зміст* мережевої війни – це використання соціальних мереж, не лише Інтернет-спільнот, а й реального суспільства – соціальних ком'юніті (спільнот) індивідів, груп, рухів, організацій як середовища конструювання передумов для створення нової системи соціальних сенсів. Мотивацією ведення мережевої війни є ідеї про еталонні моделі світопорядку на основі ідеалізованих уявлень. Результатом мережевої війни є зміна панівних режимів, «кольорові революції», контроль над інформаційним простором, розміщення військових баз і контингентів, перекодування свідомості мас, вплив на прийняття стратегічних рішень політичного істеблішменту, конструювання результатів виборів та інших

електоральних дій. Існує думка, що мережева війна побудована за принципами рекламної кампанії [4, с.24].

У *сутнісному плані* мережева війна полягає в особливій формі ведення]доктрини, стратегії та технології, максимально пристосовані до умов сучасного етапу розвитку інформаційного суспільства [2, с. 13].

Мережева війна ведеться переважно глобальними інституціоналізованими структурами. Різні мережеві структури (масмедіа, транснаціональні корпорації, релігійні організації, політичні еліти, спецслужби) інтегруються в загальну, гнучку й різноманітну мережу [2, с. 18].

Особливості мережевої війни:

1. Одночасна різновекторність спрямовування дій у формі тривалого пульсування («принцип спагеті») та раптова концентрація сили вбачається як визначальний чинник її результативності [5].

2. Перманентний пошук об’єктів нападу робить стан війни нескінченним [6].

3. Деієрхарізація структури – відсутність чітко визначених єдиних центрів управління. Основними компонентами є ядро, периферія та вузли [7]. Учасники «мережі» здатні координувати свої дії без чітко визначеного центрального керівництва.

4. Прихованість і анонімність дій – наявність труднощів у розпізнаванні навмисних та ненавмисних (випадкових) дій і процесів у кіберпросторі, складнощі або неможливість виявлення джерела інформаційно-психологічної агресії та визначення ступеня загроз національній безпеці, справжніх масштабів та цілей військової операції.

5. Незрозумілість і невизначеність правил застосування суттєво збільшує ефективність використання можливостей мережі.

6. Асиметричний характер – перевага інформаційного складника над військовим. Американський професор Д. Арквілл, який власне і

запропонував термін «мережева війна», стверджував, що «в епоху глобального взаємозв'язку, насиченого передовими інформаційними технологіями, навіть малі команди бійців можуть завдати величезної шкоди» [Цит. по: 8].

7. Геополітичний масштаб – дії відбуваються в усіх типах геополітичних просторів, де відстань до цілі впливу не має значення. Ведення мережевих війн безпосередньо або побічно впливає на події в реальному світі.

8. Смислова спрямованість – фронт мережевої війни міститься в ментальному просторі, де метою противника є руйнування традиційних базових цінностей нації та імплантація їй власних світоглядних наративів.

Суб'єктами мережевої війни переважно є недержавні та позадержавні структури. *За масштабами* вони можуть бути субнаціональними і наднаціональними [9, с.19].

Соціальною ресурсною базою є три категорії діячів мережевої війни, кожній із яких притаманна конкретна бойова стратегія. Для першого типу – активізму – характерні збір інформації на певних сайтах та її оприлюднення в мережі, побудова конструктивного діалогу та обмін ідеями, координування дій і лобіювання. Активісти використовують Інтернет для підтримки певних вимог або справи. Хакерам, які представляють другий тип стратегії, властиві більш радикальні дії: віртуальне блокування сайтів та їх зламування, поширення електронно-поштових «бомб» і вірусів. Цей тип є певним союзом між хакерством та активізмом. Третій тип – кібертероризм – має за мету стратегію кібератаки або кібероборони. Ця категорія означає вихід тероризму в кіберпростір та завдає конкретних людських і матеріальних втрат [10, с. 282–283]. Важливо зазначити, що один і той самий суб'єкт може займатися усіма трьома видами діяльності. Кібертерорист може збирати інформацію про певний об'єкт в Інтернеті, публікувати пропагандистські матеріали,

координувати свої дії за допомогою електронної пошти та потім розпочати кібератаку [9], тобто бути послідовно чи ситуативно активістом, хакером та кібертерористом.

Поняття мережевої війни можна визначити як форму геополітичної протидії між глобальними інституціями за допомогою використання механізму залучення великої кількості індивідів у комплекс мереж соціально-політичного, духовно-інтелектуального, торговельно-економічного, сектантсько-терористичного характеру з метою уніфікації світоглядних основ мережевого суспільства епохи постмодерну в інтересах домінуючої групи глобальних інституцій.

Отже, **мережева війна** є формою інформаційно-комунікаційного протистояння мережевих структур у форматі офлайн (організації або тимчасові/ситуативні об'єднання індивідуумів на основі спільної діяльності чи інтересів) та онлайн [11] (інтернет-ресурси формату web 2.0 – віртуальні соціальні мережі та наступних – web 3.0. й web 4.0) з використанням спеціалізованих технологій для впливу на широкий спектр інформаційних, соціальних, психологічних, когнітивних, етнічних, релігійних та інших факторів.

Цей тип війни породжений наслідками глобалізації та феноменом інформаційної ери, парадигма якої вплинула на усі сфери життя суспільства. Як провідну тенденцію слід вважати подальшу перспективу розвитку власне мережевих війн, котрі поступово витіснятимуть традиційний класичний вид війн. Цьому сприятиме подальший розвиток комунікаційних технологій і технічного прогресу, що забезпечить перехід від затратної та чисельної за жертвами війни до мережевої війни, яка є набагато вигіднішою економічно.

Джерела та література

1. Сенченко М. Четверта світова. Інформаційно-психологічна війна. К.: ФОП Стебляк М. І., 2014. 384 с. URL: https://lib.rus.ec/b/241595/read

2. Данильян О. Г., Дзьобань О. П. Феномен мережевих війн: до проблеми філософського осмислення. *Вісник Національного юридичного університету імені Ярослава Мудрого*. 2021. № 3 (50). С.11–27.

3. Лазоренко О. А.Визначальні характеристики мережевої війни як нового виду боротьби. Scientific researches and their practical application.modern state and ways of development. 2014. URL: https://sworld.education/index.php/safety-314/national-security-314/23039-314-248

4. Дорошкевич А. С. Гібридна війна в інформаційному суспільстві. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого».* 2015. 2 (25). С. 21–28.

5. Arquilla John. The new rules of war. *Foreign policy*. 2010. April. URL: http://www.foreignpolicy.com/articles/2010/02/22/the_new_rules_of_war

6. Гула Р. В., Дзьобань О. П., Передерій І. Г., Чобіт І. Р. Інформаційне протиборство: роль та практика діяльності бібліотек, архівів і музеїв (за досвідом російсько-української війни). Монографія. Київ: Видавництво Ліра-К, 2023. 260 с.

7. «Мережева війна» як спосіб досягнення світового панування США. *Військова панорама*. URL: http://wartime.org.ua/206-merezheva-vyna-yak-sposb-dosyagnennya-svtovogo-panuvannya-ssha.html

8. Мишкало М. Нові правила війни. URL: http://zgroup.com.ua/article.php?articleid=3851

9. Мережі і мережні війни: майбутнє терору, злочинності та бойових дій / [за ред. Дж. Арквілла, Д. Ронфельдта; пер. з англ. А. Іщенка]. Київ: Вид. дім «Києво-Могилянська академія», 2005. 350 с.

10. Куц М. Ю. Мережні війни: сутність та основні характеристики. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого».* 2015. № 2 (25). С. 277–286.