7. Заславська О. О. Політичні «паблік рілейшинз» і політична реклама як ефективні комунікативні технології впливу на електорат / О. О. Заславська. // Політологічний вісник : збірник наукових праць. – К. : ІНТАС, 2007. – Вип. 29. – 344 с.
8. Політологічний енциклопедичний словник / Упор. В. П. Горбатенко ; за ред. Ю.С. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка. – 2-ге вид., доп. і перероб. – К. : Ґенеза, 2004. – 736 с.
9. Вибори-2010: аналіз явки виборців. – Назва з екрану : http://polityka.in.ua/info /348.htm.
10. У рейтингу свободи слова Україна наздогнала Монголію й Сенегал. – Назва з екрану : http://tsn.ua/ukrayina.

Кавка Віктор Васильович,
кандидат історичних наук,
доцент кафедри політології і права
Вінницького Національного технічного університету

УДК 32.019

ІНТЕРНЕТ ЯК ЗАСІБ МЕРЕЖЕВОЇ ВІЙНИ

У статті розглядається проблема залученості Інтернет-ресурсів в процес мережевої війни. Аналізуються суть, структура і учасники мережевої війни як специфічного соціально-політичного явища. Виокремлюються основні проблеми контролю над Інтернетом з метою забезпечення безпеки суспільства, держави і особи.

Ключові слова: *мережева війна, ресурси, безпека, Інтернет, правове регулювання.*

В статье рассматривается проблема вовлеченности Интернет-ресурсов в процесс сетевой войны. Анализируются сущность, структура и участники сетевой войны как специфического социально-политического явления. Вычленяются основные проблемы контроля над Интернетом в целях обеспечения безопасности общества, государства и личности.

Ключевые слова: *сетевая война, ресурсы, безопасность, Интернет, правовое регулирование.*

The problem of Internet resources in the process of net war is considered in the article. The essence, the structure and participants of the net war as a specified social-political phenomenon is analysed. The main problems of Internet control with the aim of providing security of the society, the state and the person are separated.

Key words: *net war, resources, security, Internet, legal regulation.*

На сучасному етапі розвитку суспільства Internet як сукупність інфокомунікаційних технологій та техніки є глобальним засобом мас-медіа, що конструює принципово новий інформаційний простір суспільно-політичної сфери. Він є потужним джерелом впливу на громадян і надання їм інформації. Проте актуальним, на наш погляд, є вивчення його впливу на політичну сферу життя суспільства, питання контролю над інформацією, пошук балансу між свободою слова і певною загрозою у вигляді інформаційних атак.

У науковій літературі останнім часом виявляється значний інтерес до вивчення впливу Інтернету на настрої громадян, перебіг виборчих процесів тощо. Варто назвати таких науковців, як О. Бабкіна, В. Бебик, В. Бех, В. Горбатенко, А. Дугін, О. Заславська, Н. Комльова, В. Корнієнко та інші. Розробкою теоретичних та методологічних засад дослідження масової комунікації займалися як українські (Н. Костенко, С. Барматова, Ю. Сорока, С. Кащавцева, Л. Скокова та ін.), так і зарубіжні вчені (У. Ліпман, Г. Лассуелл, Т. Адорно, Е. Катц, П. Лазарсфельд, Б. Берельсон, Ж. Бодрійяр та ін.).Концепції постіндустріального (інформаційного) суспільства представлені в працях Д. Белла, О.

Тоффлера, К. Боулдінга, З. Бжезинського, А. Турена, Дж. Гелбрейта, Р. Арона, П. Серван-Шрайбера, М. Понятовського, М. Хоркхаймера, Ю. Хабермаса, Н. Лумана, М. Маклюена. Ці вчені розглядають високотехнологічні інформаційні мережі, що діють в глобальних масштабах, як основну умову формування інформаційного суспільства.

Попри те, що розглядаються різні аспекти функціонування Інтернету як засобу ЗМІ, відсутнє його дослідження як ресурсу ведення саме мережевої війни. Тим часом кібернетичний простір активно використовується для проведення інформаційних атак, як прихованих, так і відкритих. Виходячи з цього, метою даної статті є визначення специфіки мережевої війни і місця Інтернет-ресурсів в її здійсненні. Почнемо із визначення місця Інтернету в межах суспільно-політичного дискурсу. Наразі прийнято виокремлювати його три основні підсистеми: технічну – засоби комунікації та комп'ютери; соціальну – соціальна взаємодія, що виникає завдяки Інтернету та комунікативне поле, що конструюється користувачами в процесі трансмісії інформації та визначається як віртуальна інформаційна реальність. Така структура є теоретико-методологічним підґрунтям двох базисних підходів до визначення предмету соціологічного аналізу Інтернету. Відповідно до першого підходу, Інтернет – це сукупність мережних відносин, соціальних інститутів, технологій та технічних засобів, що пов'язані за допомогою комп'ютерно-опосередкованих ліній та характеризуються єдиним часом та простором. Виходячи з іншого підходу, Інтернет – це складна мозаїчна соціотехнічна система, що здійснює процес створення, розповсюдження та обміну інформацією за допомогою інтерсуб'єктивної масової комунікації в глобальних комп'ютерних мережах та створює віртуальну інформаційну реальність.

Розглядаючи роль Інтернет-ресурсів у мережевій війні, визначимо сутність поняття «війна». Так, війна є виразом антагоністичного протистояння, що має за мету знищення супротивника, тобто кардинальна зміна його базових характеристик для підпорядкування тотальному контролю з боку ініціатора війни. Залежно від природи акторів, зацікавлених у веденні війни і типу простору, в якому вона здійснюється, розрізняються війни економічні, інформаційні (що ведуться як в кібернетичному, так і в ідеологічному просторі) і війни традиційні — з метою захоплення географічного простору [1].

У будь-якому випадку ініціатор війни прагне отримати ресурси розвитку, такі як: сировина; народонаселення; доступ до промислового або фінансового сектора супротивника; комп'ютерні мережі та інші системи зв'язку (інформаційний ресурс); символічний капітал, що забезпечує, згідно із М. Вебером, «престиж могутності» [2]. Чим важливіший ресурс і чим більший його потенційний обсяг, тим в більшому ступені розгортаються бойові дії.

Для отримання ресурсів суспільства, що є об'єктом атаки, необхідно перенести агресію з географічного простору в економічний і інформаційний простір і, перш за все, зробити операцію із зміни «настроїв» ментального поля цього суспільства. Це означає зміну його традиційних цінностей з тим, щоб фактична атака ззовні сприймалася цим суспільством як заохочення до подальшого розвитку.

В ході так званої «холодної війни» у другій половині XX ст. були значною мірою відпрацьовані технології мережевої війни як форми тотального руйнування геополітичного супротивника. «Холодна війна» — тип геополітичного протистояння держав, основним змістом якого є боротьба за стратегічне домінування в економічному та інформаційно-ідеологічному просторі [3]. Цей тип війни в силу специфіки просторів, в яких вона ведеться, не вимагає використання збройних сил. «Холодна війна» між наддержавами набуває глобального рівня і зазвичай супроводжується локальними «гарячими» війнами.

З розвитком інформаційного суспільства на рубежі XX–XXI ст. з'являються численні технології прихованої руйнівної дії, що мають комплексний характер і війни, що в сукупності утворюють новий тип — мережеву війну [3]. На наш погляд, мережева війна — це тотальне руйнування базових характеристик певної нації у всіх типах геополітичних просторів одночасно, що здійснюється переважно в прихованій формі.

Щодо мети мережевої війни, то вона полягає у значному закріпленні всієї сукупності ресурсів суспільства-супротивника за геополітичним агресором, причому «передача» цих

ресурсів агресору здійснюється досить часто добровільно, оскільки сприймається як додатковий імпульс до розвитку. Тому мережева війна є набагато складнішою в здійсненні, ніж традиційна, але є і найефективнішою. Щодо результатів, то мережеві війни можуть існувати століттями до того моменту, поки не зміняться самі актори-агресори і їх потреби.

Як ми зазначали, основний фронт мережевої війни розташовується в ментальному просторі, де метою супротивника є руйнування традиційних базових цінностей певної нації та імплантація власних. Факт ведення і структуру цього типу війни неможливо розпізнати на рівні масової свідомості. Якщо ж політична еліта суспільства, що стала об'єктом мережевої війни, не має достатньої кваліфікації для виявлення такої агресії і організації адекватної відповіді, то таке суспільство приречене на поразку. Для мережевих війн, як зазначалося, характерне поєднання агресивної дії на супротивника в різних геополітичних просторах, причому через це активні учасники бойових дій мають нетрадиційний характер. По суті справи, до процесу мережевої війни залучаються всі інститути суспільства. На рівні держави — це органи вищого державного керівництва і регулярні збройні сили. На рівні громадянського суспільства стають задіяними приватні військові контингенти, ЗМІ, релігійні організації, установи культури, правозахисні організації та інші елементи недержавної організації суспільства. Фахівці відзначають і таку особливість мережевих війн, як відсутність чіткої ієрархії в структурі-агресорі, що не дозволяє її відстежити.

Щодо специфіки мережевої війни, то її технологічна структура (сукупність технологій, що використовуються для боротьби з суспільством-супротивником) дуже складна. Технології мережевих війн включають складні комбінації, за якими часто не видно замовника [1]. Головне полягає в тому, що мережеві війни постіндустріальної інформаційної епохи характеризуються прагненням безкровного вирішення завдань перерозподілу просторів і ресурсів. Тут, на наш погляд, діє установка на підтримку іміджу «розвинених демократій», які і ведуть такі війни у всіх типах геополітичних просторів під гаслом дотримання прав людини. «Завдяки сучасним технологіям і накопиченому досвіду навіть геноцид можна вести без газових камер і масових розстрілів. Досить створити умови для скорочення народжуваності і збільшення смертності. Більшого успіху можна досягти, обдурюючи народ, міняючи його стереотипи і поведінкові норми з тим, щоб навіть силовий розвиток подій сприймався ними як належне» [2]. Розглянемо основні технології мережевих війн за сферами. Так, можна виокремити такі групи: *у географічному просторі*: контроль з боку великих держав; контроль територій за допомогою космічних апаратів; підтримка тероризму в різних його формах; «кольорові революції»; *в економічному просторі*: надання кредитів; економічні санкції різної інтенсивності дії; провокації; *в інформаційно-ідеологічному просторі:* використання спотвореної інформації; підміна понять; *в інформаційно-кібернетичному просторі*: хакерські атаки на кібернетичні системи супротивника; використання «вірусів» і «черв'яків», «логічних бомб» тощо [3].

Перераховані технології не вичерпують весь арсенал засобів боротьби з супротивником, що застосовується в мережевих війнах. Одним з елементів технологічної структури мережевої війни є інформаційна війна, що розуміється нами як цілеспрямоване руйнування ментального простору певної нації, тобто заміщення базових цінностей даного суспільства сукупністю цінностей, що формують психологічні установки, вигідні агресорові. Значну роль в цьому процесі відіграє такий кібернетичний ресурс, як Інтернет.

Поява Інтернету надала принципово нові можливості ведення інформаційної війни в кібернетичному просторі, поставила до порядку денного наступні питання: які межі свободи слова і як слід трактувати — в моральних і правових відносинах — прояви неприязні одних людей (організацій, політичних сил) по відношенню до інших? Відповівши на ці питання, світова спільнота могла б чітко визначити суть мережевої війни і представити ступінь відповідальності тих, хто бере участь в розв'язуванні такого роду конфліктів.

Однак ці питання так і не отримали чітких відповідей в міжнародному праві. Відповідно немає ясності і в практичній їх реалізації. У сучасній дослідницькій практиці утвердилось думка про те, що Інтернет кинув виклик традиційним ЗМІ, запропонувавши

принципово нові форми ведення інформаційної війни. Разом з тим складно заперечувати і те, що Інтернет, по суті, запозичував інструментарій емоційної дії, властивий традиційним ЗМІ. Проте, на відміну від будь-яких інших ЗМІ, що функціонують в умовах вже розробленої законодавчої бази, Інтернет, як і раніше в цьому відношенні залишається «темною конячкою». Правове оформлення поки не встигає за розвитком нових технологій. За справедливим твердженням Д. Маквейла, фахівця в галузі масових комунікацій, Інтернет сьогодні функціонує на напівлегальній основі [4].

Зауважимо, що Рада Європи і ОБСЄ поставили на обговорення питання, чи можливий контроль над рухом інформації в Інтернеті? В ході цього обговорення мова фактично зайшла про те, чи можна зберегти баланс між свободою слова і обмеженнями, спрямованими проти розповсюдження агресивної і неетичної інформації [5]. Забігаючи наперед, відзначимо, що питання й досі залишається відкритим. Зрозуміло, що практичний контроль над регулюванням Інтернету і припинення можливих мережевих війн залишаються складними. Насправді, Інтернет не підкорюється певному регулюючому органу, не має власників, не просуває жорстко сконструйовані політичні ідеї, не має територіальної «прописки». Унаслідок цього його інформаційна діяльність не отримала належного юридичного обґрунтування. Так, з одного боку, Інтернет залишається без власника і тому дає можливість для ініціації в кібернетичному просторі будь-яких сумнівних дій, а з іншого — є об'єктом постійної критики з боку окремих держав, політичних і суспільних груп з приводу протизаконних ідей, що вільно транслюються. Проте ця критика, судячи з усього, виявляється малоефективною.

Зазначені питання є актуальними для України з урахуванням зростаючого ступеня її комп'ютеризації. Не дивлячись на невизначеність юридичного статусу Інтернет-сайтів, українські офіційні особи бачать їх потенційну небезпеку в розповсюдженні різних форм загрози, «чорного піару» тощо. Для дослідження цієї проблеми В. Остроухов розділив всі сайти на чотири групи: сайти, що використовуються для відкритого розповсюдження ідей екстремізму, сепаратизму і тероризму; сайти, спрямовані на розповсюдження релігійних доктрин і сект; сайти, що поширюють ксенофобські ідеї на основі певної расової або національної належності; сайти, що спонукають чинити незаконні дії [3].

Досить переконливим був Ю. Чайка, який виступив з ініціативою закриття веб-сайтів, що містять екстремістську інформацію. За допомогою сучасних Інтернет-технологій, що діють в режимі он-лайн, новачки засвоюють терористичні прийоми [1]. Аль-Каїда, наприклад, ініціювала створення веб-сайту, що розповідає і показує, як використовувати на практиці різні види зброї, зарядні пристрої для виготовлення бомб, як організовувати викрадання людей [5].Відсутність чітких, зрозумілих для всіх країн правил регулювання Інтернету приводить до невизначеності і колізій, коли справа стосується реальних життєвих ситуацій. Існування веб-сайту www.kavkazcenter.com з очевидністю це ілюструє. Як відомо, через декілька тижнів після трагедії в Беслані тодішній Президент Росії В. Путін зробив офіційну заяву, закликавши держструктури, громадські організації і всіх громадян об'єднатися в боротьбі проти тероризму (http://president.kremlin.ru/eng, 2004). В. Путін поставив цю ідею в розряд найважливіших для Російської держави. З цієї причини вона відразу ж стала привабливою для ЗМІ, які висловлювали думки і будували прогнози з приводу небезпеки виникнення нових терористичних погроз.

Серед вогнищ цієї небезпеки інформагентство «Інтерфакс» неодноразово озвучувало офіційний сайт «Кавказ-центра» www.kavkazcenter.com, який веде підривну роботу проти Росії. На цю тему на прес-конференції, організованій «Інтерфаксом», виступив віце-прем'єр Чечні З. Сабсабі. За його словами, цей веб-сайт постійно дезінформує світову громадськість щодо подій в Чечні за допомогою розпалювання пристрастей з приводу одних подій і замовчання інших. Це спричиняє спотворення інформації західними ЗМІ, які є користувачами цього веб-сайту (www.interfax.ru).

Напевно невідомо, хто конкретно стоїть за сайтом www.kavkazcenter.com, що виник ще в 2003 р. і представляє інтереси прихильників Шаміля Басаєва. Проте оперативність

інформації і професійний рівень її обробки дозволяють говорити про серйозні фінансові вливання в цей сайт. Чеченська опозиція діє сьогодні не тільки через www.kavkazcenter.com., а й через інші сайти (www.chechenpress.com., www.kvestnik.org, www.daymokh.info). Зрозуміло, що Росію не влаштовувала ситуація безкарного Інтернет-віщання, націленого проти її інтересів. Проте добитися закриття сайту вона поки не в змозі внаслідок труднощів правового регулювання Інтернету в міжнародному масштабі. Отже, все це з очевидністю підтверджує, що сучасні комп'ютерні технології створюють реальну основу для підриву національної безпеки Росії, України і взагалі всіх країн світу, що інформаційна загроза виявляється надзвичайно небезпечною для них. Сьогодні необхідно розробити нові інформаційні стратегії, без яких неможливо країні відстояти свої інтереси.

На нашу думку, мережеві війни сьогодні стали реальним чинником, що формує глобальну конфліктність. Вони примушують засумніватися в тому, що технічний прогрес несе в собі тільки позитивний зміст. Проблемна ситуація, на наш погляд, визначається невирішеністю багатьох питань, пов'язаних з існуванням Інтернету як найбільш потужного і розгалуженого джерела передачі інформації. Розвиток Інтернету із самого початку базувався на ідеї вільної передачі інформації як необхідної умови існування істинно демократичного суспільства. Натомість реалії сучасного світу ставлять на порядок денний питання про те, наскільки безперешкодно, поза будь-якими обмеженнями може функціонувати у всесвітній мережі інформація, чи повинна існувати в цьому інформаційному просторі цензура і як конкретно вона повинна виглядати. Актуальність цих питань визначається тим, що традиційним правом будь-якого демократичного суспільства залишається право на отримання об'єктивної і оперативної інформації. Проте Інтернет-інформація, що долає будь-які територіальні межі, може створювати серйозні соціально-психологічні проблеми як для окремих держав, так і для всієї цивілізації.

В умовах реального ведення мережевих війн світовій спільноті необхідно прояснити цілий ряд принципових моментів, що стосуються законодавчої бази в області інформації. Важливо прийти до єдиного висновку, чи допустимо вважати Інтернет засобом масової інформації. І якщо так, то відповісти на питання, чи застосовувати до Інтернету правові норм законів про ЗМІ, прийняті в багатьох країнах. Як і раніше невизначеними залишаються можливості контролю над інформацією, яка часто носить провокаційний, конфліктний характер, підштовхуючи до здійснення екстремістських або навіть терористичних дій.

Очевидно, що для розв'язання цих питань потрібні зусилля різних міжнародних структур, а також органів державної влади, здатних запровадити в життя конкретні програми з подолання соціально-політичної конфліктності. Важливо надалі проводити дослідження в цьому напрямку і стратегії і тактики забезпечення інформаційної безпеки України.

Література:

1. Дугин А. Мир охвачен сетевыми войнами / А. Дугин. — Назва з екрану: http://www.kreml. org/media.
2. КомлёваН.А.Основы геополитики/Н.А.Комлёва.—Екатеринбург:Изд-во Урал.ун-та,2008.—324с.
3. Сетевая война и «бархатные революции». — 13.03. 2009. — Назва з екрану: http://www.pravda.ru/ print/politics/parties/other
4. McQuail D. McQuail's Mass Communication Theory / McQuail D. — 4th ed. London : Sage Publ., 2000. — P. 29.
5. Щербина В. Сітьова кіберкомунікація як соціальний феномен / В. Щербина // Соціологія: теорія, методи, маркетинг. – 2002. – № 1. – С. 109.