М. БАГЛІКОВА (Донецьк)

ІНФОРМАЦІЙНІ ВІЙНИ І УКРАЇНА

Бурхливий розвиток інформаційних технологій, комунікаційних мереж, засобів зв'язку та доступу до різноманітної інформації, свідчить про те, що людство вступило в епоху інформаційної цивілізації, характерною ознакою якої є створення глобального інформаційного простору. Сьогодні навряд чи можна назвати хоч одну державу вилучену із загального інформаційно-комунікативного простору і незалежну від інформаційних потоків, які швидко створюють нову реальність, впливаючи на політичну, економічну, соціокультурну, оборонну та інші складові процесів розвитку суспільства. Усвідомлення значущості та цінності інформації сформували якісно новий тип протиборства між державами в інформаційній сфері, яке з кожним роком набуває панівного характеру, стає домінантою світового розвитку. Найвищою та найнебезпечнішою формою цієї боротьби є інформаційна війна, яка не завдає видимих фізичних та матеріальних руйнувань, а натомість ефективно змінює цілі, погляди, настрої соціуму, вводять його в оману, десинхронізує управлінські процеси, тобто вражає суспільство в усіх сферах його життєдіяльності. Інформаційна експансія щодо України та висока ймовірність її втягнення в майбутні інформаційні війни диктує необхідність вивчення цієї проблеми та вироблення певних засад інформаційної боротьби, які повинні стати фундаментом формування і реалізації політики забезпечення національних інтересів на інформаційному рівні, та створення національної системи інформаційної безпеки України.

Незважаючи, на об'єктивно наявні процеси та чималу кількість наукових робіт як закордонних (В. Плэтта, Д. Деннінга, М. Лібікі, І. Панаріна, С. Расторгуєва, І. Завадського, В. Цигічко, Д. Черешкіна, Г. Смоляна), так і вітчизняних науковців (Г. Почепцова, Д. Прокоф'єва, В. Абакумова, В. Бутраньця, О.Литвиненко, В. Бондаренко, Б. Кормича, М. Требіна) [1], в політичній науці й досі відсутня чітка дефініція поняття інформаційна війна, що обумовлено низкою причин. По-перше, традиційним сприйняттям концепту „війна" та відносною короткочасністю періоду визнання інформаційно-бойових дій, що відповідно ускладнює формування понятійного апарату у сфері інформаційних відносин, таких як: інформаційні операції, атаки, інформаційна зброя тощо. По-друге, диспутом серед дослідників щодо розрізнення понять «інформаційна війна», «інформаційно-психологічна війна» і «психологічна війна», визначенням пріоритетності чи то інформаційного, чи то психологічного компонентів у згаданому феномені. Відтак, з'ясуванню сутності інформаційних війн, їх впливу на Україну, і відповідно, визначенню методів запобігання та протистояння різним видам інформаційної агресії і буде присвячена дана стаття.

Загалом слід зазначити, що існує чимала кількість доктринальних підходів з боку військово-політичного керівництва ЄС, національних урядів США, Німеччини, Великобританії, Франції, Китаю, Росії та інших держав на ведення інформаційних воєн (як в агресивних цілях, так і з метою захисту), які найбільш повно відбивають існуючу реальність. Однак, на нашу думку, найбільший практичний інтерес представляють для нас погляди військово-політичного керівництва США, оскільки саме вони

значно підсилили свою політичну, економічну і військову перевагу за рахунок лідерства в інформатизації і в принципі намагаються здійснювати глобальний інформаційний контроль, а фактично нав'язують свої правила гри в реальному житті, накшталт подій в Іраці, в Афганістані, в Югославії, Ірану, Сирії, Північної Кореї тощо.

Історія запровадження цього терміна починається з 70-х років XX століття, коли в світ вийшла книга А. Далласа під назвою „Таємна капітуляція" (1967 р.), де дане словосполучення вживалось в якості особливого виду спецопераций розвідки [2, с. 221]. У 1976 р. Томас Рона застосував термін інформаційна війна у звіті „Системи зброї та інформаційна війна", підготовленим для компанії Boeing [2, с. 222], в якому наголосив, що інформаційна інфраструктура робиться ключовим компонентом американської економіки, проте стає все більш уразливою мішенню навіть за мирних часів. Зазначена публікація каталізувала відповідну кампанію в засобах масової інформації, які почали активне обговорення проблеми та зацікавила військових, які зрозуміли, що інформація може бути не лише ціллю, але й зброєю. Активно він почав використовувались після проведення у 1991 р. операції „Буря в пустелі", в якій інформаційні технології вперше були використані як засіб бойових дій: інформація дозувалась та корегувалась, забезпечувалась підтримка з боку ЗМІ за межами безпосереднього контролю, а самі вторгнення здійснювалися як рекламно-пропагандистські шоу, із заздалегідь розписаним сценарієм і дійовими особами [3]. А вже 1992 р. директивою міністра оборони США DODD 3600 від 21 грудня, цей термін був офіційно введений до документів Міністерства Оборони. Починаючи з 1994 р. в США проводяться наукові конференції, командно - штабні військові ігри (КШВІ) за участю представників воєнно-політичного керівництва країни та силових структур з метою розробки концепції інформаційної війни. У липні 1995 р. Національний університет оборони у Вашингтоні здійснив випуск першої групи спеціалістів з інформаційних війн. Вже тоді в США був створений центр інформаційної стратегії і політики, завданням якого стало вивчення можливостей використання інформаційних технологій у військових конфліктах XXI сторіччя [2, с. 222].

В жовтні 1998 р. Міністерство Оборони США вводить в дію „Об'єднану доктрину інформаційних операцій", яка узагальнює досвід щодо створення концепції інформаційної війни та безпеки, уточнює ключові категорії з метою розробки однакових підходів та координації зусиль командування збройних сил усіх рівнів. Зокрема, під інформаційною операцією розуміються дії спрямовані на ускладнення збору, обробки та зберігання інформації інформаційними системами противника з одночасним захистом власної інформації та інформаційних систем, а інформаційна війна - це комплексний вплив (сукупність інформаційних операцій) на систему державного та військового управління противника, на її військово-політичне керівництво, який в мирний час змушував приймати сприятливі рішення для сторони – ініціатора інформаційного впливу, а в ході конфлікту повністю паралізував функціонування інфраструктури управління противника [4]. В переліку першочергових інформаційних операцій були зазначені: операції проти волі нації; проти командування суперника та ворожих військ; проти національних культур [5]. Основними елементами інформаційних операцій, згідно доктрини були визначені:

- дублювання розвідувальної інформації;
- дезінформація;
- психологічні операції;
- фізичне руйнування інформаційних ресурсів противника;
- напади (фізичні, електронні) на його інформаційну структуру;
- зараження комп'ютерними вірусами обчислювальних мереж, проникнення в інформаційні мережі [6].

Національний інститут оборони США ще у 1995 р. публікує працю М. Лібікі „Що таке інформаційна війна?", в якій були зазначені її форми:

- командно-управлінська;
- розвідувальна;
- психологічна;
- хакерська;
- економічна;
- електронна;
- кібервійна [2, с. 223]

Останніми роками США продовжують удосконалювати концепцію інформаційної війни. Зокрема, у „Стратегії інформаційних операцій" (2003 р.) основна увага приділяється розширенню сфери застосування та засобам ведення війни. В документі наголошувалось про безперервність та всеосяжність інформаційного впливу з поширенням на всю „аудиторію" включаючи як населення своєї країни за певних умов, так і населення країн – союзників чи суперників.

Пріоритетність віддається наступним формам ведення інформаційних операцій: публічна дипломатія, зв'язки з громадськістю та психологічні операції. На стратегічному та тактичному рівнях робота із зв'язками з громадськістю передбачає: оперативний доступ до ЗМІ; підготовку глобальних комунікацій до можливої зміни фокусу уваги в розширеному конвенті (так зване „щеплення" ЗМІ - поступова підготовка до сприйняття основної події); оперативне коментування подій; формування так званих „команд правди" з метою доведення „правдивої" інформації до аудиторії; розробку та запровадження різних видів вбудованого медіа-контенту (так звані „домашні заготовки"); підготовку передач новин; підготовку прес-конференцій та брифінгів; презентацію гуманітарних програм (відновлення у післявоєнний час, допомога біженцям) тощо.

Публічна дипломатія в залежності від рівня керівництва містить в собі: підготовку контенту публікацій для міжрегіонального розповсюдження; відкрите просування політики уряду США шляхом створення відповідних суспільно-політичних організацій та проведення ідеологічних заходів, на кшталт створення форуму Азіатсько-Тихоокеанського співробітництва; спостереження за діяльністю регіональних інформаційних центрів.

Психологічні операції загалом передбачають розробку спеціальних матеріалів для радіо, телебачення, друкованих та Інтернет – ЗМІ з метою безпосередньої зміни поведінки цільової аудиторії. При цьому дозволяється використовувати „жорсткі" методи впливу на аудиторію, а саме: шантаж, технічні та хімічні засоби. Цікавим є той факт, що ця концепції вже

неодноразово була апробована. Зокрема, це стратегічні операції під назвою „Боротьба з міжнародним тероризмом" та „Боротьба із зброєю масового знищення в Іраці", в результаті яких США закріпились на Близькому Сході та створили умови для реалізації власного плану перебудови регіону під назвою „Стратегія формування Близького Сходу" [7].

Виходячи з вищевказаного, бачимо, що термін інформаційна війна зобов'язаний своїм походженням військовим і позначає жорстоку та небезпечну діяльність, зв'язану з реальними і руйнівними сутичками в інформаційному просторі, тобто війну за знання, а саме за те, кому відомі відповіді на питання: що?, коли?, де?, чому? і наскільки надійними вважає окремо взяте суспільство свої знання про себе та своїх супротивників. "Ми наближаємося до такої ступені розвитку, коли вже ніхто не є солдатом, але усі є учасниками бойових дій... відтепер головна мета полягає не в знищенні живої сили, але в підриві цілей, поглядів і світогляду населення, у руйнуванні соціуму" [8]. Таким чином, бачимо, що інформаційна війна акумулює і інформаційні, і інформаційно-психологічні і психологічні компоненти в залежності від цілей сторони – ініціатора інформаційного впливу.

Подібні дії можуть бути початі геополітичними або економічними супротивниками, терористичними групами, фізичними та юридичними особами, тобто будь-ким. Однак, реальність свідчить про те, що найбільшими можливостями для організації і проведення інформаційних операцій володіє саме держава в особі системи органів влади і державного управління. Інформаційні війни є наступальними, спланованими та цілеспрямованими: їх ведення ніколи не буває випадковим або відособленим (і може, навіть, не порушувати закону), а має на меті погоджену діяльність по використанню інформації як зброї для ведення бойових дій - будь то на реальному полі брані, або у військовій, економічній, політичній, соціальній чи інших сферах. Така війна має наступальні й оборонні складові, але починається з цільового проектування і розробки своєї архітектури командування, керування, комунікацій, комп'ютерів та розвідки, що забезпечує особам, які приймають рішення, відчутну інформаційну перевагу [9, с. 36].

Театр інформаційних бойових дій всеосяжний: від службового приміщення до домашнього персонального комп'ютеру. Засобами ведення такої війни є будь-які засоби передачі інформації, які дозволяють цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, нейтралізувати системи захисту, обмежувати доступ, дезінформувати, порушувати функціонування носіїв інформації, дезорганізувати роботу технічних засобів, комп'ютерних систем і інформаційно-обчислювальних мереж супротивника. Методи впливу визначають особливості сфер, в яких ведеться інформаційна боротьба. Відтак ризик дезорганізації суспільства через штучно створений інформаційно-організований керований хаос, через надлишок чи дефіцит інформації, дезінформацію, і, як наслідок, загальну керованість великих соціальних груп є справою цілком досяжною.

Останнім часом словосполучення "інформаційна війна" та "інформаційна атака" надійно увійшло в лексикон українських політиків, державних діячів та науковців. Обговоренню цього питання були присвячені й декілька круглих столів на тему „Інформаційні війни в Україні: новітня історія чи майбутнє" за участю політологів, експертів та представників засобів масової інформації [10]. Проте, при цьому, усі констатують лише факт інформаційної експансії стосовно України та необхідність у цьому контексті "щось робити". Між тим інформаційна агресія щодо України триває. Це і „таємні в'язниці ЦРУ", „придністровське питання", „продаж зброї Іраку та Грузії" тощо [11]. Однією з найтриваліших війн, є так звана газова війна, яка активізується ледве не щороку. Сценарій майже завжди однаковий: російські засоби масової інформації звинувачують Україну в крадіжці російського газу, неплатоспроможності, в не здатності вести переговорний процес тощо. Як наслідок, Україна втрачає свій міжнародний імідж, і його складову, як країни - транзитеру блакитного палива. Не підлягає сумніву й те, що Росія готувалась до війни, бо її інформаційні атаки були масованими, нав'язливими та всеосяжними: заяви офіційних осіб, брифінги, інтерв'ю, створення аналітичних сайтів тощо. В результаті не лише українське суспільство, але й влада опинились у шоковому стані, особливо коли минулорічний конфлікт з площини України - Росії був перенесений до Європи. В той же час українські засоби масової інформації спромоглися лише ретранслювали російську позицію, не усвідомлюючи того, що "грають" на боці держави - "агресора": зокрема, висвітлення подій починались з представлення російської позиції з цього питання і лише згодом надавались невеликі коментарі з боку української влади. Наслідки цих інформаційних атак вражаючі: починаючи від втрати довіри до української влади з боку ЄС до прямих збитків в політичній, економічній та інших сферах. Саме після цих подій деякі європейські країни погодились з Росією, що й стало початком побуди альтернативних газотранспортних мереж в обхід України. Якщо проаналізувати наслідки всіх інформаційних атак, що останнім часом здійснювалися проти нашої держави, то можна зробити невтішний висновок: Україна, по-суті, втрачає контроль над власним інформаційним суверенітетом, а її інформаційний простір незахищений від впливу інформаційних потоків суміжних держав, з усіма наслідками, які з цього випливають.

Все це вимагає негайної розробки комплексу заходів щодо створення ефективної системи захисту та протидії інформаційній агресії. Насамперед, потрібно удосконалити законодавство в сфері забезпечення інформаційної безпеки держави з врахуванням сучасних тенденції розвитку глобального інформаційно - комунікативного простору. В контексті цього розбірливого формулювання потребує така дефініція як інформаційний простір, бо на сьогодні, на жаль, не існує чітко визначених і юридично закріплених кордонів і тому його порушення, згідно міжнародного права, не може розглядатись як втручання у внутрішні справи нашої країни. По-друге, потрібно сприяти розвиткові вітчизняної індустрії телекомунікаційних і інформаційних засобів, забезпечити їх пріоритетне в порівнянні з закордонними аналогами поширення на внутрішньому ринку, прискорити процеси модернізації матеріально-технічної бази та забезпечення захисту державних інформаційних ресурсів від несанкціонованого доступу, перекручування або знищення інформації з акцентом на збереженні якості інформації (своєчасності, точності, повноти і необхідної присутності). Можливо, з метою захисту національного і інформаційного простору доцільно розглянути питання щодо створення аналогічної „Інтернету" української локальної мережі „Укрнет", яка повинна бути надійно захищена від агресивного вторгнення ззовні завдяки розробці і впровадженню українських сервер-провайдерів необхідного функціонального призначення. У Росії, наприклад, для обслуговування усіх органів державної влади вже давно розпочато створення єдиного сервіс-провайдера, покликаного забезпечити її відповідний

захист і надійне функціонування з точки зору національної безпеки [12, с. 58]. По-третє, доцільним є створення спеціальних інститутів організаційно-управлінського та інформаційно-аналітичного спрямування з метою розробки і проведення стратегічних заходів задля попередження та нейтралізації негативних інформаційних впливів як на зовнішніх (глобальному, субрегіональному, регіональному), так і внутрішніх (державному, відомчому, місцевому) рівнях. Україна повинна проводити активну, або навіть агресивну, інформаційну політику з постійним пропагуванням здобутків та можливостей держави, створювати та підтримувати українські центри в різних країнах, просувати українські засоби масової інформації в світових мережах, проводити віщання на різних мовах, беручи приклад із США, Китаю та Росії. Лише за виконання цих умов, Україна захистить свій інформаційний простір від будь-яких інформаційних впливів та збереже свій інформаційний суверенітет, який є складовою національної безпеки країни та неодмінною рисою незалежної та сильної держави.

1. Див. роботи: Плэтт В. Стратегическая разведка. Основные принципы/ В. Плэтт. - М.:Наука. - 1997. – 348 с.; Denning D.E. Information Warfare and Security. – Reading, Mass. etc., 1999. - 323 p.;
   Forno R., Baklarz R. The Art of Information Warfare. Insight into the Knowledge of Warrior Philosophy. – 1999; Панарин И. Н. Информационная война и геополитика / И. Н.Панарин. – М.: Поколение, 2006.- 560 с.; Расторгуев С.П. Информационная война/ С.П. Расторгуев. — М: Радио и связь, 1999. — 416 С.; Прокоф'єв Д. Інформаційна війна та інформаційна злочинність [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Prokop.htm. - Назва з титул. екрану; Черешкин Д.С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны/Д. Черешкин, Г. Смолян, В.Цыгичко //Конфидент. - № 4.-1996.- С.38-42.; Почепцов Г. Г. Информационные войны /Г. Г. Почепцов. – К. : Ваклер, 2000. – 576 с.; Абакумов В. М. Суб'єкти інформаційних війн: поняття та види / В. М. Абакумов Форум права. – 2009. – № 2. – С. 6–12 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09avmptv.pdf; Кормич Б. А. Правові засади політики інформаційної безпеки України: монографія /Б. А. Кормич. – Одеса : Юридична література, 2003. – 472 с.; Бутранец В. К. Информационное противоборство: понятие, субъекты, цели /В. К. Бутранец // Государственное управление и право. – 2008. – № 3 (28). – С. 104-109; Бондаренко В.О., Литвиненко О.В. Інформаційні впливи і операції/В. Бондаренко, О. Литвиненко//Стратегічна панорама.-1999.-№4.-С.134-140; Требін М. Інформаційне суспільство. Війни нової епохи/ М. Требін//Віче.-2002. - № 4 (121).- С. 64-68.
2. Панарин И. Н. Информационная война и геополитика / И. Н.Панарин. – М.: Поколение, 2006.- 560 с.
3. Бондар Ю. Поле битви – інформаційний простір [Електронний ресурс]/ Ю. Бондар. - Режим доступу: http://personal.in.ua/article.php?ida=215.- Назва з титул. екрану.
4. Гриняев С. Информационная война: история, день сегодняшний и перспектива / С. Гриняев [Электронный ресурс] – Режим доступу: http://infwar.ru/article.php?num=41. - Назва з титул. екрану;
5. Гуріна Н. Інформаційне протиборство – один з головних напрямків політики сучасних міжнародних відносин / Н. Гуріна [Електронний ресурс] – Режим доступа: http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=13657. - Назва з титул. екрану;
6. Кузьменко А. Інформаційно-психологічна війна епохи глобалізації/ А. Кузьменко [Електронний ресурс] – Режим доступу: http://www.justinian.com.ua/article.php?id=2662.- Назва з титул. екрану;
7. Гриняев С. О нових направлениях развития информационной войны в США/ С. Гриняев [Электронный ресурс] – Режим доступу: http://infwar.ru/article.php?num=39. – Назва з титул. екрану;
8. Перепелица Г. Информационные войны/Г. Перепелица [Электронный ресурс] – Режим доступа: http://www.zn.ua/1000/1550/21435/. - Название з титул. экрана;
9. Завадский И.И. «Информационная война — что это такое? /И. Завадский //Конфидент. - № 4.- 1996 .- С.34-37;
10. Информационные войны в Украине: игра втемную без прикупа или гадание на кофейной гуще? [Электронный ресурс] – Режим доступу: http://news07.join.com.ua/?p=15645. - Название з титул. экрана;
11. Як виграти інформаційну війну? [Електронний ресурс] – Режим доступу: http://www.ukrslovo.com.ua/work/archive/2006/21/02.html. - Назва з титул. екрану;
12. Сьомін С. Україна в третій світовій війні / С. Сьомін//Нова політика.- 2000. - № 4. - С. 53 – 58.

SUMMARY

Baglikova M. INFORMATION WARS AND UKRAINE

The article is clarifying the essence of information wars, their conceptual reasons, kinds and forms. The information expansion to Ukraine is considered, recommendations as for the methods of prevention and counteraction to information aggression from other states.