Конотопенко О.П. *доцент*
кафедри правових наук
та філософії
ВДПУ ім. М. Коцюбинського,
кандидат філософських наук

ЗАСОБИ І МЕТОДИ ІНФОРМАЦІЙНОЇ ВІЙНИ В УКРАЇНСЬКОМУ ПРОСТОРІ

У статті розглянуто засоби і методи ведення інформаційної війни. На прикладах показано маніпулятивні технології та прийоми, їх вплив на психіку, свідомість та поведінку людини. Обґрунтовано важливість результатів дослідження та впровадження для розуміння дискурсу, інструментів та методів ведення сучасних інформаційних воєн, а також для здійснення ефективної державної політики протидії інформаційним агресіям.

Ключові слова: інформаційна війна, інформаційний простір, інформаційна зброя, пропаганда, інформаційна безпека, маніпуляція, інформаційне протиборство.

Сьогодні процес інформатизації суспільства, його державних та суспільних інститутів, розвивається стрімко і як правило непередбачено і некеровано. Суспільство, на наш погляд, з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки. Широке використання в процесі інформатизації персональних комп'ютерів уже сьогодні дозволило створити в технологічно розвинутих державах світовий інформаційний простір, в якому створюється, накопичується, розподіляється, передається, приймається, перетворюється та знищується інформація. Безсумнівним є те, що використання нових прогресивних інформаційних технологій в суспільному житті, в виробництві та управлінні, можливості швидкого обміну науково-технічною, економічною, навчальною та іншою інформацією, є неабияким добром. Але подібно тому як досягнення

ядерної фізики породили загрозу ядерних війн, таке створення єдиного інформаційного простору стало джерелом практично нерозв'язних або важко розв'язних проблем. Безсумнівно, що технологічно розвинуті держави, в крайньому випадку деякі, будуть намагатися збільшити політичну, економічну та військову перевагу за рахунок досягнення переваг в рівні інформатизації. І як наслідок – встановлення та ведення глобального інформаційного контролю над менш розвинутими державами, проведення в загальному інформаційному просторі ідеологічної та культурної експансії. Протиріччя, які виникають внаслідок зазначеного, можуть і будуть приводити до війн, інформаційних війн, тільки на перший погляд менш жахливих, ніж звичайні. Ці війни можуть вестись із використанням інформаційної зброї, ступінь же захищеності інформаційного простору держави характеризується її інформаційною безпекою.

Війна інформації на сьогодні стала одним з найнебезпечніших видів зброї. Користуватися компроматами, виливанням бруду, підкиданням неправдивої інформації, намагання за допомогою інформації ввести в оману стало для багатьох сенсом життя. Інформація має вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети: знищити опонента, прибрати з дороги конкурентів чи розпалити війну, як це було не раз у світі. На тлі останніх подій, які відбуваються в Україні можна зрозуміти, що основна боротьба між політичними опонентами відбувається за допомогою інформації, тобто Україна є полем інформаційної війни.

Зважаючи на роль інформації у сучасному світі, американський дослідник М.Маклюєн (ще 30 років тому) виводить цікаву думку про те, що економічні зв'язки та відносини все більше набувають форми обміну знаннями, а не товарами і тому істинно тотальна війна – це війна за допомогою інформації. На думку Г.Почепцова, інформаційна цивілізація

виражає себе не скільки у фізичному просторі, скільки в інформаційному, віртуальному просторі [1].

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та психологічній галузях.

Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою.

Уперше термін «інформаційна війна» було згадано в 1985 р. у Китаї. В основу теоретичних підходів китайських спеціалістів у сфері інформаційної боротьби покладено погляди давньокитайського воєнного діяча Сунь-Цзи, який узагальнив досвід інформаційного впливу на противника. В трактаті «Мистецтво війни» Сунь-Цзи писав: «У будь-якій війні, як правило, політика зводиться до захоплення держави в цілому... Здобути сотні перемог у бою – це не межа мистецтва. Підкорити супротивника без бою – ось це вершина мистецтва» [2].

У книзі Прокоф’єва "Інформаційна війна і інформаційна злочинність" інформаційна війна визначається як дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах[3].

Основні методи інформаційної війни – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника.

Інформаційна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активну протидію в інформаційному

просторі. Інформаційна війна – це атака інформаційної функції, незалежно від засобів, які застосовуються.

У веденні стратегічних інформаційних війн застосовується специфічна зброя. Ця зброя не наносить фізичної шкоди, але може призвести до справжньої війни.

Інформаційна зброя – сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій або служб інформаційної інфраструктури в цілому або окремих її елементів.

Інформаційна війна виникає з нових підходів до застосування інформації, визначення її ролі та місця. Можна виділити два трактування поняття інформаційної війни: гуманітарну і технічну.

Наприклад, М.Павлютенкова зазначає, що у гуманітарному сенсі інформаційна війна становить собою активні методи трансформації інформаційного простору, що знаходить свій вираз у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на структури породження інформації – процеси міркувань. У той же час технічне трактування даного поняття полягає у тому, що за допомогою спеціальних програм руйнується обладнання, програмне забезпечення тощо.

Безперечним є той факт, що формування інформаційного суспільства стає не лише фактом, а все більше починає впливати на формування державної політики інформаційної безпеки. Досягнення тих чи інших цілей виявилося можливим із застосуванням лише інформаційних технологій, які б чинили вплив на суспільну свідомість. Одним з проявів застосування даного методу є сильний часовий пресинг на суб'єктів державного управління, який не залишає їм часу на прийняття виваженого, такого, що відповідає національним інтересам рішення. Відтак, досягнення певних геополітичних та інших важливих цілей уможливлюється за допомогою невійськових методів.

Сумний досвід неприділення належної уваги даним питанням спричинив до розпаду СРСР, могутньої держави, яка до 1991 року разом із США утворювали біполярну систему світу.

Зазначимо, що четверта влада – ЗМІ – відіграла значну роль в укоріненні у свідомості пересічного громадянина терміну "інформаційна війна". При чому під останнім, ЗМІ, як правило, розуміють використання компромату через засоби масової інформації, здебільшого електронні. Ідеальним засобом для цього є Інтернет, який дає можливість розповсюджувати будь-яку інформацію без будь-яких обмежень.

Що стосується іншого розуміння – технічного – то тут обов'язковою умовою є те, що ведення інформаційної війни є результатом узгодженої діяльності з використання інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності. При цьому інформаційна війна включає наступні дії:

- здійснення впливу на інфраструктуру систем життєзабезпечення - телекомунікації, транспортні мережі, електростанції тощо;

- промисловий шпіонаж – порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;

- хакінг – злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Коли йдеться про інформаційну війну, то слід говорити про існування рішучої і небезпечної діяльності, пов'язаної із реальними бойовими діями. Більш того, за даного випадку постає необхідність у виокремленні декількох підвидів інформаційних війн: кібернетична війна, електронна війна, психотронна війна, психотропна війна, штабна війна, психологічна, енергоінформаційна війна.

Таке розуміння інформаційної війни надає можливість погодитись із визначенням поняття інформаційної війни, яке міститься у керівних документах збройних сил США.

Згідно з Доктриною проведення інформаційних операцій інформаційна війна – дії, що вчиняються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи супротивника при одночасному забезпеченні безпеки власної інформації і інформаційних систем. Одним з прикладів є існування спеціальної програми запису всіх телефонних дзвінків, що виходять за кордон США на спеціальну апаратуру. За допомогою даної програми всі телефонні дзвінки, що виходять за межі країни, записуються, а потім пропускаються через спеціальний пристрій, який за допомогою пошукових систем за ключовими словами здійснює виявлення та ідентифікацію важливої інформації.

Відтак, існування розвиненої системи інформаційної безпеки закладе фундамент для стійкого функціонування системи національної безпеки. На думку деяких дослідників, стрімкий розвиток інформаційних технологій спричинить у майбутньому появу нових за змістом видів війн, які відбуватимуться без жодного пострілу. Особливо наголосимо, що сучасні інформаційні війни спрямовані здебільшого на дезорієнтацію людини, зміну її світогляду, підміну цінностей і перетворення на інформаційного споживача, тобто інформаційного раба.

Цілі інформаційної війни є дещо іншими, ніж війни у звичному розумінні. Якщо за умов ведення звичайної війни, головною метою є фізичне знищення противника та ліквідація його збройних сил, то за умови ведення інформаційної війни відбувається широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, зміни світоглядних настанов, зародження сумніву в необхідності та доцільності існування в рамках самостійної, суверенної держави.

На сьогодні термін "інформаційна війна" використовується у двох площинах:

- у широкому розумінні – для визначення протиборства в інформаційній сфері в засобах масової інформації для досягнення різних політичних цілей;

- у вузькому розумінні – для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою (в операції, битві).

У вітчизняній практиці в широкому розумінні частіше використовують термін "інформаційне протиборство", у вузькому розумінні - "інформаційні воєнні дії".

Інформаційне протиборство – це форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів, для впливу на інформаційне поле супротивника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей.

Враховуючи зазначене визначення, можна стверджувати, що інформаційне протиборство включає три незмінні складові: вплив, аналіз, безпосереднє протиборство.

Основним елементом, від якого залежить ефективність компанії, є аналіз, мета якого полягає в оцінці, стратегічному прогнозуванні та плануванні в аспектах внутрішньополітичного та зовнішньополітичного становища. Що ж стосується "інформаційної війни" то, як всеохоплююча, цілісна стратегія, вона обумовлена все зростаючою значимістю та цінністю інформації у питаннях командування, управління та політики. Також можна послуговуватись визначенням "інформаційної війни" як "комунікативної технології по впливу на масову свідомість з короткочасними та довготривалими цілями".

Інформаційна війна має наступальні та оборонні складові, але, починаючи з цільового проектування та розробки своєї архітектури командування, управління, комунікації, комп'ютерів та розвідки, яка

забезпечує особам, які приймають рішення, відчутну інформаційну перевагу у різноманітних конфліктах. Інформаційна війна може бути спрямована проти трьох елементів: комп'ютер, програмне забезпечення, людина.

Однією з головних цілей інформаційної війни є придушення в людині морального творчого початку.

На міжнародній арені інформаційні війни ведуться: між державами та блоками держав; між міжнародними корпораціями, транснаціональними корпораціями та міжнародними фінансовими групами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами з державами; між терористичними організаціями та державами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами; між злочинними організаціями; між злочинними організаціями та державами.

Технології інформаційної ери певним чином зрівняли індустріальні, постіндустріальні та доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже, є як суб'єктами, так і об'єктами інформаційної війни, а отже і забезпечення інформаційної безпеки.

Мета інформаційної війни – послабити моральні та матеріальні сили супротивника або конкурента і зміцнити власні. Вона передбачає вжиття заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється даху над головою. І це породжує легковажне ставлення до них. Тим часом руйнування, яких завдають інформаційні війни в суспільній психології, психології особи, за масштабами і за значенням цілком сумірні зі збройними війнами, а часом і перевищують їх наслідки.

Головне завдання психологічної війни полягає в маніпулюванні масами. Метою такої маніпуляції є:

• внесення в суспільну та індивідуальну свідомість ворожих шкідливих ідей та поглядів;

• дезорієнтація та дезінформація мас;

• послаблення певних переконань, устоїв;

• залякування свого народу образом ворога;

• залякування супротивника власною могутністю.

Одним із головних методів ведення інформаційно-психологічної війни є пропаганда, тобто поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою впровадження їх у громадську думку та активізації і тим самим використання цих ідей у масовій практичній діяльності населення. Водночас до пропаганди належать повідомлення, які поширюються для справляння вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення до певної ситуації або поводження певної групи людей, безпосередньо чи опосередковано вигідного організаторам. Яскравим прикладом ведення пропагандистських кампаній є діяльність ідеолога та пропагандиста фашизму Йозефа Геббельса, який проголосив такі принципи пропаганди:

• пропаганда має бути спланована і вестися з однієї інстанції;

• тільки авторитет може визначити, має бути результат пропаганди істинним чи фальшивим;

• чорна пропаганда використовується, коли біла неможлива або вона не має належного ефекту;

• пропаганда має характеризувати події та людей відмінними фразами чи гаслами;

• для кращого сприйняття пропаганда повинна викликати інтерес в аудиторії і передаватися через привабливе увазі середовище комунікацій [4].

Можна виокремити такі основні методи інформаційної агресії проти України: 1) дезінформування та маніпулювання; 2) пропаганда; 3)

диверсифікація громадської думки; 4) психологічний та психотропний тиск; 5) поширення чуток. Дезінформування та маніпулювання інформацією – метод, який передбачає обман чи введення об'єкта спрямувань в оману щодо справжності намірів для спонукання його до запрограмованих суб'єктом дій. Найчастіше у світовій практиці застосовуються такі форми дезінформування та маніпулювання інформацією:

• тенденційне викладення фактів – форма дезінформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних;

• дезінформування «від зворотного», що відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві;

• термінологічне «мінування», яке полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру;

• «сіре» дезінформування, що передбачає використання синтезу правдивої інформації з дезінформацією;

• «чорне» дезінформування, яке передбачає використання переважно неправдивої інформації [5].

Метою методу диверсифікації громадської думки є розпорошення уваги правлячої еліти держави на різні штучно акцентовані проблеми і тим самим відволікання її від вирішення першочергових завдань суспільно-політичного та економічного розвитку з метою забезпечення нормального функціонування суспільства і держави.

Нині відсутня розроблена на концептуальному рівні концепція (система теоретико-методологічних засад, положень) забезпечення інформаційної безпеки. Більш того, аналіз сучасної геополітичної обстановки і безпекотрансформаційних процесів дозволяє зробити висновок, що проти України здійснюються широкомасштабні інформаційні

акції, спрямовані на дискредитацію, дезорганізацію, підрив іміджу, інформаційну кластеризацію і дестабілізацію нашої держави. І, передусім, цей вплив чиниться на систему державного управління [6]. Саме тому першочерговим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій є розробка термінових ефективних заходів щодо нейтралізації інформаційно–диверсійної діяльності Російської Федерації проти України та протидії її подальшому розгортанню. Крім того, виклики, що постали перед Україною, потребують вжиття негайних заходів щодо розробки нової Доктрини національної безпеки України, модернізації всієї системи інформаційної безпеки держави.

Список використаної літератури:

1. Почепцов Г. Росія і Україна у співставленні їх комунікативно-пропагандистських можливостей [Електронний ресурс] / Г. Почепцов. – Режим доступу : http://osvita.mediasapiens.ua/material/33291.
2. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції [Електронний ресурс] / В. Ліпкан, Ю. Максименко, В. Желіховський. – Режим доступу : http://mobile.pidruchniki.com/15800119/politologiya/ ponyattya_ zmist _zagroz _informatsiyniy _ bezpetsi.
3. Сливка В. Інформаційна війна проти України: міф чи реальність? [Електронний ресурс] / В. Сливка. – Режим доступу : http://intkonf.org/slivka-vv - informatsiyna-viyna-proti-ukrayini-mif-chi-realnist/.
4. Жуковская Д. Йозеф Геббельс – теоретик СМИ Третьего Рейха [Электронный ресурс] / Д. Жуковская.– Режимдоступа : http://www.historicus.ru/ joseph_ Gebbels_ teoretik_SMI_Tretyego_Reiha/.
5. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу : http://justinian.com.ua/ article.php?id=3222.
6. Горбань Ю.О.Інформаційна війна проти України та засоби її ведення Режим доступу: http://visnyk.academy.gov.ua/wp-content/uploads/2015/04/20.pdf.
7. Информационная война [Текст] :/ Расторгуев С.П.. - М. 1998г. - 143с.

Konotopenko Oleksandr

MEANS AND METHODS OF THE INFORMATION WARE IN THR UKRAINIAN SPACE

The article deals with the means and methods of the information ware. The examples show manipulative technologies and techniques, their influence on the mentality, consciousness and human behavior. The article illustrates the

importance of the results of the research and implementation for understanding the discourse, tools and methods of conducting modern information wars, as well as for effective state policy of counteracting information aggression.

Key words: information ware, propaganda, information space, information weapon, information security, manipulation, information confrontation.

----------***----------