УДК 351.746.1

ГРИГОР'ЄВ Володимир Ілліч

ТЕХНОЛОГІЇ СУЧАСНОЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ВІЙНИ

Постановка проблеми. Інформація, що передається каналами масової комунікації, може здійснювати безпосередній вплив як на життя суспільства в цілому, так і на соціально-психологічний і моральний стан кожного члена цієї спільноти. Водночас інформаційне суспільство, а саме глобалізація інформаційного простору несе у собі велику небезпеку яка перш за все пов'язана із кібертероризмом, інформаційними війнами, маніпулюванням масовою свідомістю.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій свідчить, що у війнах майбутнього перевага над противником досягатиметься за допомогою своєчасного інформаційного та психологічного впливу на важливі державні і військові об'єкти, а також населення й особовий склад військ противника при мінімально можливому ризику таких дій на свої сили і засоби. Питання використання технологій інформаційно-психологічного протиборства викладено у працях І. М. Панаріна, С. А. Зелінського, А. В. Манойло, А. І. Петренко, Д. Б. Фролова, Г. В. Грачова та інших авторів, але постає проблема узагальнення практики використання цих технологій в сучасних умовах.

Постановка завдання. Завданням статті є дослідження використання сучасних технологій в інформаційному просторі, способів інформаційно-психологічного впливу на свідомість населення і владно-суспільних відносин у національних державах. Стаття присвячена розгляду основних технологій інформаційно-психологічної війни.

Виклад основного матеріалу. Сьогодні соціально-політичні відносини формуються в складних умовах під впливом ідеології інформаційного суспільства, процесів геополітичної конкуренції, глобалізації, політичного й інформаційного протиборства. Ці процеси в сучасних умовах можуть приймати особливо небезпечні та агресивні форми, що отримали назву інформаційно-психологічних війн (ІПВ). Використання арсеналу сил, засобів і методів інформаційно-психологічної війни в політичних цілях в сучасному світі набуло широкого поширення. Терміни «інформаційні» і «психологічні» війни активно використовуються політиками та політологами. ІПВ

зараз розглядаються лідерами провідних країн світу як ефективний і універсальний засіб досягнення зовнішньополітичних цілей.

Відсутність норм міжнародних та внутрішньодержавних прав, що дають юридичну кваліфікацію особливо небезпечних агресивних акцій (заходів, операцій) інформаційно-психологічного впливу та перешкоджають розв'язанню такої агресії стосовно інших держав, дозволяє використовувати арсенал сил і засобів ІПВ як у воєнний, так і в мирний часи.

Так, на думку І. М. Панаріна, під час інформаційно-психологічного протиборства головними об'єктами впливу та захисту є психіка політичної еліти та населення протидіючих сторін, системи формування суспільної свідомості та прийняття рішень [1].

С. А. Зелінський у своєму дослідженні «Інформаційно-психологічний вплив на масову свідомість» вказує, що основний удар в результаті інформаційно-психологічних війн приймає на себе психічна свідомість мас. «Таким чином, відбувається певне формування громадської думки. Мета психологічної війни – це досягнення стійкого результату у формуванні громадської думки в заданому маніпуляторами ключі, закладання патернів поведінки, а саме стійких механізмів, при впливі на які станеться запланована реакція на підсвідомість людини» [2].

У своїй монографії А. В. Манойло визначає інформаційно-психологічний конфлікт як «зіткнення інтересів двох або декількох суб'єктів інформаційно-психологічних відносин з метою загострення або вирішення протиріч щодо влади й здійснення політичного керівництва в інформаційно-психологічному просторі. Відмінною рисою інформаційно-психологічних конфліктів є в першу чергу нові можливості усунення або загострення протиріч, які стали причиною виникнення конфлікту. Більш того, різноманітність засобів, методів і способів інформаційно-психологічного впливу визначає високу тактичну гнучкість поведінки суб'єктів соціальних відносин сучасного інформаційного суспільства в конфліктних ситуаціях» [3].

С. Некляєв стверджує, що «психологічна війна або інформаційно-психологічна війна (Psychological Warfare), пов'язана з впливом на психіку індивіда». До неї входить інформаційно-психологічний вплив на населення, політичне і військове керівництво протиборствуючої сторони, операції з модифікації культури [4].

Нині інформаційні війни виходять на авансцену можливих варіантів домінування в інформаційній сфері.

Фахівці виділяють особливості ІПВ, серед яких основними є:

– раптовість;

– скритність;

– ідеальність умов для маскування і приховування справжніх намірів, що створюються методами психологічного та інформаційно-технічного впливу;

– можливість діяти під чужим прапором і гаслами;

– відсутність матеріальних слідів агресії, що дозволяють зупинити істинного агресора і притягнути його до міжнародної відповідальності;

– відсутність необхідності фізичного вторгнення на територію противника та окупації цієї території для досягнення поставлених цілей;

– бездіяльність основного збройного потенціалу держави, яка стала жертвою агресії [4].

Інформаційно-психологічна війна – це комунікативна технологія, що має вплив на масову свідомість. В інформаційній війні можна виділити дві складові: технічну та соціально-психологічну.

Саме соціально-психологічна війна, на думку Г. В. Грачова, є «предметом досліджень психологів і соціологів і не піддається конкретному визначенню» [5]. Інформаційно-психологічна війна як один з різновидів інформаційної війни часто розглядається як інформаційно-психологічне протиборство.

За спрямованістю інформаційних впливів вчені виділяють два види інформаційного протиборства: інформаційно-психологічне та інформаційно-технічне.

У першому випадку об'єктом впливу стають індивідуальна та масова свідомість, у другому – комп'ютери та інформаційні системи.

Об'єктами інформаційного впливу першого виду є люди, другого – техніка.

Відповідно до цього вирізняються два типи інформаційних технологій: технології, які впливають на технічні засоби та технології, що позначаються на населенні.

Під час ведення психологічної війни на перше місце виходять процеси формування громадської думки. При цьому ефективно застосовуються такі заходи: зменшення (перебільшення) значущості тієї чи іншої події, недопущення появи певної події в інформаційний простір, використання в ході комунікативної кампанії «спіралі мовчання», тобто представлення думки меншості, як думки більшості населення та підміна, таким чином, смислових та ідеологічних акцентів.

До технічної складової відносяться комп'ютерні мережі та телекомунікації, електронні ЗМІ, несанкціонований доступ до даних супротивника [6].

Використання інструментарію інформаційно-психологічної війни дозволяє, з одного боку, зруйнувати наявну інформаційну систему, з іншого – провести зміну комунікативної установки в суспільстві і, таким чином, підпорядкувати його інтереси інтересам сторони-агресора.

Звідси виняткова небезпека засобів і методів інформаційно-психологічної війни як засобу вирішення політичних протиріч в міжнародній сфері.

Першим досвідом створення технологій, які здійснюють вплив на людей і масову свідомість, стало дослідження з «соціального кондиціювання», що проводилося перед Першою світовою війною для формування потрібної громадської думки. Його основи заклав військовий технік майор Джон Роулингс Ріїс, який пізніше, у 1921 році відкрив у Суссексі (Англія) Інститут

міжлюдських контактів (Тейвісток), котрий став спеціалізованим центром ведення психологічної війни.

У 1946 році Тейвістокським інститутом був утворений Стенфордський дослідний інститут. Сьогодні він являє собою величезний військовий мозковий центр, який залишив позаду себе Гудзонський інститут та Корпорацію Ренд. Саме в надрах Стенфордського центру в Лондоні була розроблена всеохоплююча техніка управління суспільством (автоматизація поведінки суспільства), яка вимагає взаємозв'язку величезного обсягу інформації. Для цього знадобилися високошвидкісні комп'ютерні системи, які розраховують напрямок руху суспільства і моменти часу найменшої активності чи готовності до капітуляції.

У сфері впливу на індивідуальну і масову свідомість використовується приблизно однаковий «технологічний набір» засобів боротьби з об'єктом впливу:

– прагнення дезорганізації суспільства;

– здійснення контролю над освітою та інформацією;

– руйнування незалежності церкви;

– забезпечення низького рівня викладання математики і логіки, повна неувага до технічних наук;

– постійна пропаганда сексу, насильства та війн по телебаченню та в пресі;

– переписування історії та виховання нового покоління, байдужого до історичного минулого;

– створення системи розваг для людей на рівні розваг дитини дошкільного віку;

– досягнення максимальної зайнятості суспільства, тобто залучення громадян під все і вся і, як результат – повна відсутність часу для роздумів;

– використання практики керованих криз;

– прагнення переорієнтувати окремі держави на нові геополітичні центри тяжіння;

– підтримка сепаратизму, що прикривається кампанією із захисту прав людини;

– перехід від політики переважної взаємодії з центральною владою до «співробітництва» з регіонами і автономіями [7].

Як правило, психологічний вплив здійснюється через засоби масової інформації.

До засобів масової комунікації, крім ЗМІ (телебачення, преса, радіо, Інтернет і т. д.), відносяться також кінематограф, театр, всі видовищні заходи та література, відеофільми, комп'ютер, різні види реклами, відео і звукозапис тощо, за допомогою чого можна впливати на масову аудиторію.

Засоби масової інформації включають в себе розширений арсенал способів впливу на психіку індивіда і мас з метою впровадження в підсвідомість психологічних установок і формування стереотипів поведінки.

Технології впливу на психіку особи розрізняють залежно від цілей їх застосування в психологічній війні. До таких цілей можна віднести:

– спотворення існуючої інформації і нав'язування помилкової або беззмістовної інформації, яка позбавляє особу можливості правильно сприймати події або поточну обстановку та приймати вірні рішення;

– здійснення психологічної обробки населення;

– здійснення ідеологічної диверсії та проведення дезінформації;

– підтримання сприятливої громадської думки;

– організація масових демонстрацій під хибними гаслами;

– пропаганда та поширення неправдивих чуток;

– зміна та управління індивідуальною і колективною поведінкою.

Поряд з використанням традиційних засобів (друковані та електронні засоби масової інформації) йде активна розробка і апробація спеціальних засобів впливу на людину через комп'ютерні мережі: засоби інформаційно-психологічного (психофізичного) впливу (в тому числі в рамках програм МК-Ультра – ультрамозковий контроль, МК-Дельта – дистанційна зміна поведінки людини, Блю-берд, Артишок).

У числі таких розробок, які вже отримали застосування, називають голографічні зображення в просторі, вірус № 666 (видає на екрані ЕОМ особливу колірну комбінацію, викликає зміни стану психіки людини, аж до блокування судин головного мозку у оператора ЕОМ) [8].

На рубежі XX–XXI ст. у промислово розвинених державах склалися наукові, технологічні, економічні та кадрові передумови виникнення нового типу інформаційного впливу – кібернетичного: повністю сформувалася наука інформатика; комп'ютеризація охопила всі сфери життєдіяльності людини. Досягла високих темпів розвитку індустрія засобів інформатизації, телекомунікації та зв'язку. Виникли програмно-технічні засоби деструктивного впливу на комп'ютерні системи. У той же час об'єкти управління і зв'язку, енергетика і транспорт, банківська система стали дуже уразливими щодо інформаційно-технічного впливу. У результаті державні структури технологічно розвинених країн почали досліджувати можливості створення засобів і способів завдання шкоди об'єктам, функціонуючим на основі комп'ютерних систем. Військові відомства стали організовувати цілеспрямовану розробку кібернетичної зброї у воєнних цілях. Водночас віруси, програми зламу були взяті на озброєння міжнародними та національними кримінальними угрупованнями, поодинокими хакерами, а потім і терористами.

Таким чином, зараз існує низка типів і видів інформаційної зброї, розробкою та застосуванням яких займаються різні спеціалізовані структури. На це вказують американські й інші західні аналітики, а також українські та російські фахівці.

Так, в документах Центру стратегічних досліджень США наголошується, що «інформаційну зброю не можна розглядати як єдине ціле». На думку західних експертів, кожен тип і вид інформаційної зброї передбачає наявність самостійної концепції [9].

Особливу небезпеку становить використання сучасних технологій як інформаційної зброї для комп'ютерних систем органів державної влади, управління військами, фінансами і банками та економікою країни в цілому.

Інформаційна зброя може бути використана для ініціювання великих техногенних катастроф внаслідок порушення штатного керування об'єктами з великою кількістю небезпечних речовин, і які володіють високими концентраціями енергії. За своєю результативністю інформаційна зброя може порівнюватися зі зброєю масового ураження. З початком кібернетичної війни в першу чергу будуть зроблені кібернетичні атаки на комп'ютерні системи і сервери державного управління, установ, фінансових і ділових центрів. Ці атаки будуть підкріплені активацією комп'ютерних вірусів, закладених в ЕОМ ще в мирний час. Також передбачається використовувати спеціальні пристрої, які під час вибуху створюють потужний електромагнітний імпульс, або біологічні засоби, здатні знищувати електронні схеми та ізолюючі матеріали в комп'ютерах [10].

Засоби програмно-математичного впливу поділяються на: комп'ютерні віруси, засоби несанкціонованого доступу та програмні закладки.

До технологій, що впливають на технічні засоби, О. Г. Караяні визначає такі:

– комп'ютерні віруси, що відрізняються високою здатністю проникнення різними каналами в програми, закріплення, розмноження та виведення їх з ладу;

– «логічні бомби», «програми-перевертні», «програми-вбивці інформації» заздалегідь впроваджувані в інформаційно-керуючі центри військової та цивільної інфраструктури, які за сигналом або у встановлений час спотворюють або знищують інформацію чи дезорганізують роботу програмно-технічних засобів;

– програми несанкціонованого доступу до інформаційних ресурсів противника з метою розкрадання розвідувальної інформації;

– засоби придушення інформаційних систем противника, входження в них з метою підміни інформації або відкритого пропагандистського втручання;

– біотехнологічні засоби, створені на основі клітинної інженерії, що виводять з ладу комп'ютерні плати [11].

Вперше термін «комп'ютерний вірус» застосував співробітник Лехайського університету (США) Ф. Коен в 1984 році на 7-й конференції з безпеки інформації. Комп'ютерні віруси здатні розмножуватися, впроваджуватися в програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи управління. За своєю суттю – ця програма здатна до прихованого

розмноження в середовищі операційної системи шляхом включення у виконувані програми або зберігає свої копії з метою подальшого розмноження [9].

До засобів несанкціонованого доступу відносяться комп'ютерні програми з потенційно небезпечними наслідками, що виконують функції руйнування коду програм в оперативній пам'яті.

До класу програм з потенційно небезпечними наслідками відносяться програмні закладки, що виконують функції спотворення довільним чином, блокування і підміни масиву інформації, нейтралізації роботи тестових програм і систем захисту інформаційних ресурсів. Відмітна ознака між засобами несанкціонованого доступу і програмними закладками – наявність для перших і відсутність для других функції подолання захисту.

Розрізняють декілька видів програмних закладок: троянська програма, логічна бомба, логічний люк, програмна пастка, програмний черв'як. Троянська програма має законний доступ до системи, але виконує і приховані функції. Логічна бомба – програма, що здійснює злочинні дії при виконанні низки певних логічних умов. Як приклад логічних бомб можна назвати програмні закладні пристрої, заздалегідь впроваджувані в інформаційно-керуючі центри військової інфраструктури, щоб за сигналом або у встановлений час привести їх у дію. Логічний люк – механізм всередині операційної системи (програмного забезпечення), що дозволяє програмі зловмисника отримати привілейовану функцію або режим роботи, які йому не були дозволені. Логічними люками можуть бути різного роду помилки, які свідомо вводяться зловмисниками в програмне забезпечення об'єкта. Програмна пастка – програма, що використовує помилки або неоднозначності в програмному забезпеченні. Програмний черв'як – програма, що маскується під системні засоби пошуку вільних обчислювальних ресурсів у мережі. Мережевим черв'яком називається комп'ютерний вірус, що володіє властивістю самостійного розповсюдження в системі і заражає її елементи, функціональні сегменти або систему цілком.

Новітньою розробкою комп'ютерних вірусів є так звані інформаційні організми. Під інформаційним організмом (пакет вкладення) розуміється відносно короткий набір команд (до 30 команд), яким передається керування комп'ютером, в результаті чого здійснюється захоплення інформаційно-обчислювальних ресурсів автоматизованої системи (оперативної пам'яті, простору на носіях інформації, процесорного часу тощо).

Впровадження таких засобів здійснюється під час поставок на експорт ЕОМ з апаратними закладками в їх периферійному обладнанні, які маскуються під звичайні пристрої мікроелектроніки. Апаратні закладання застосовуються для збору, обробки і передачі конфіденційної інформації. Основні результати застосування такої інформаційної зброї: дезорганізація функціонування автоматизованих систем і зниження доступності інформації, пошук слабких місць у системі захисту інформації автоматизованих систем різного призначення [12].

Засоби ураження комп'ютерних систем експерти класифікують за такими критеріями:

– керованість (можливість або неможливість дистанційного або безпосереднього управління);

– походження (самостійні, спеціально створені чи модифіковані програмні засоби);

– об'єкт впливу (вражають системні або прикладні програми, дезорганізують роботу засобів управління та ін.);

– час дії (разової або тривалої дії);

– спосіб введення в дію (негайної або відкладеної дії);

– здатність до самовідтворення;

– цільове призначення (для ураження об'єктів інформаційного впливу або для перерозподілу даних) [12].

Життєдіяльність багатьох установ, підприємств та індивідуальних користувачів залежить від мережі Інтернет. У середньому за місяць веб-портали, що належать Google і Yahoo, відвідують понад 380 млн осіб.

Фахівці виділяють наступні види атак в Інтернеті:

– збір інформації (злам приватних сторінок або серверів для збору секретної інформації або її заміни на фальшиву, корисну іншій державі);

– відмова сервісу (атаки з різних комп'ютерів для запобігання функціонування сайтів або комп'ютерних систем);

– вандалізм (використання хакерами Інтернету для псування інтернет-сторінок, заміни змісту образливими або пропагандистськими картинками);

– пропаганда (розсилка звернень пропагандистського характеру або вставка пропаганди у зміст інших інтернет-сторінок).

У 2013 році директор ФБР США Дж. Коні передбачив, що кібернетичні атаки скоро стануть більшою загрозою для національної безпеки, ніж міжнародний тероризм. Найбільшими можливостями володіють держави, але найбільш ймовірними організаторами катастрофічного кібернетичного нападу є недержавні суб'єкти. «Кибер + 9 сентября» є більш ймовірним, ніж часто згадуваний «кібер Перл-Харбор». Ефективність хакерських атак продемонстрував американський студент Р. Морріс в 1988 році, що запустив вірус, який на три дні вивів з ладу фактично всю комп'ютерну мережу США. Були паралізовані комп'ютери Агентства національної безпеки, Стратегічного командування ВПС США, локальні мережі всіх великих університетів і дослідницьких центрів. Лише в останній момент вдалося врятувати систему управління польотом космічних кораблів Шаттл. Збиток оцінювався у понад 100 млн доларів [9].

Висновки. Останніми роками значення інформаційно-психологічних війн неухильно зростає, при цьому їх головними особливостями можна вважати поступове, непомітне впровадження в усі сфери суспільно-політичного життя.

В умовах глобалізації – це особливий вид відносин між державами, при якому для вирішення міждержавних протиріч використовуються методи, засоби і технології впливу на інформаційну сферу цих держав.

Роль інформаційного ресурсу в розвитку соціуму настільки велика, а зброя інформаційного простору настільки значна, що інформація сьогодні є ключем до сучасної війни – в стратегічному, оперативному, тактичному й технічному відношеннях.

Можна з упевненістю стверджувати, що інформаційно-психологічні війни в сучасному світі є невід'ємною частиною політичного протиборства. Однак, на відміну від збройних дій, не підпадають під заборони та обмеження міжнародного права.

Нині відсутні міжнародні та національні правові норми, що дозволяють в мирний час юридично кваліфікувати дії іноземної держави, які супроводжуються заподіянням шкоди інформаційній, психологічній або іншій безпеці, як акції інформаційно-психологічної агресії (інформаційно-психологічної війни).

Саме тому проблема безпеки в інформаційно-психологічній сфері є настільки актуальною і затребуваною в сучасних умовах.

Список використаних джерел

1. Панарин И. Н. Информационная война и геополитика / И. Н. Панарин. – М. : Мир безопасности, 2006. ─ С. 54.

2. Зелинский С. А. Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды – как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс / С. А. Зелинский. – СПб. : Издательско-Торговый Дом «СКИФИЯ», 2008. – 280 с.

3. Манойло А. В. Государственная информационная политика в условиях информационно-психологических конфликтов высокой интенсивности и социальной опасности : курс лекций / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – М. : Изд-во МИФИ, 2003. – 390 с.

4. Некляев С. Информационно-психологическая война в условиях сетевой войны как новая форма угрозы национальной безопасности / С. Некляев // Вестник Московского университета. Сер. 10. Журналистика : науч. журн. – 2008. – № 5. – С. 35–51 [Электронный ресурс]. – Режим доступа : convergencelab.ru/files.

5. Грачев Г. В. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. В. Грачев, И. К. Мельник. – М. : Эксмо, 2003. – 153 с.

6. Саченко И. И. «Информационная война»: методы и практика манипулирования общественным мнением /

И. И. Саченко. – Минск, 2012 [Электронный ресурс]. – Режим доступа : ib2.znate.ru/docs/index-352351.html

7. Старостин В. И. Правовые аспекты информационно-психологической войны / В. И. Старостин ; Военный университет. – М., 2000 [Электронный ресурс]. – Режим доступа : mark5.ru/26/ 7229/ index1.1.html.

8. Якунин В. И. Новые технологии борьбы с российской государственностью. Центры влияния / В. И. Якунин, В. Э. Багдасарян, С. С. Сулакшин. – М. : Научный эксперт, 2009. – 263 с.

9. Тихонов М. Н. Кибернетические войны и информационная безопасность / М. Н. Тихонов, М. М. Богословский. – СПб. : ВМА им. С. М. Кирова, 2011 [Электронный ресурс]. – Режим доступа : //www.proatom.ru/modules.php?name= News&file=article&sid=6182.

10. Смолян Г. Оружие, которое может быть опаснее ядерного: Реалии информационной войны / Г. Смолян, В. Цыгичко, Д. Черешкин [Электронный ресурс]. – Режим доступа : http:// studopedia.ru/7_123916_zaklyuchenie.html.

11. Информационные войны как средство управления общественно-политическими процессами [Электронный ресурс]. – Режим доступа : http://www.psycho.ru/library/367.

12. Караяни А. Г. Информационно-психологическое противоборство в современной войне / А. Г. Караяни. – М. : ВУ, 1997. – 172 с.

Рецензенти:
кандидат педагогічних наук, доцент О. Гущин,
кандидат політичних наук В. Дереко

Аннотация: В статье раскрыты некоторые технологии и средства манипулирования сознанием, формы и методы проведения информационно-психологической войны. Рассмотрено современное состояние информационно-психологического противостояния, а также особенности использования информационного влияния. Проанализировано их влияние на общественные отношения на современном глобальном этапе развития цивилизации.

Ключевые слова: информационно-психологическая война, технологии влияния, информационное оружие, компьютерные вирусы, информационный ресурс.

Abstract: The article reveals some technology and means of manipulation, forms and methods of information and psychological warfare, the current state of information and psychological confrontation, and the specificity of information influence application. Their impact on social relations at the current stage of global civilization development is analyzed.

Key words: the information and psychological warfare, the impact of technology, information weapons, computer viruses, the information resource.