УДК 327(4/9):004.738.5

П. С. Шпига
кандидат технічних наук, професор кафедри міжнародної інформації та інформатики Інституту міжнародних відносин КиМУ

Р. М. Рудник
студент 1-го курсу магістратури спеціальності «Міжнародна інформація» Київського міжнародного університету

ОСНОВНІ ТЕХНОЛОГІЇ ТА ЗАКОНОМІРНОСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ

У статті автори здійснили аналіз та узагальнили існуючі технології, дефініцій «інформаційної війни», та запропонували їх власне обґрунтоване авторське розуміння, визначили основні ознаки, закономірності та наслідки інформаційних воєн. Також у статті досліджено характер інформаційної війни та технології захисту населення від інформаційної зброї.

Ключові слова: *інформаційна війна, інформаційно-психологічний вплив, форми інформаційних воєн, ЗМІ, інформаційна зброя, наслідки інформаційної війни.*

Війна нині не ведеться лоб в лоб. Війна – поняття об'ємне і часом воїнам доводиться стояти, а атакувати журналістам, політикам, економістам.
О.Бригинець

Сучасні глобальні тенденції в галузі комунікації демонструють якісно нові результати, які були неможливими в минулому. Різко зріс обсяг інформації, яку

громадяни почали отримувати поза контролем своїх національних урядів. Інформація несе в собі як життєдайну, так і деструктивну силу. Але її вплив значно зріс. Тому надзвичайно актуальною стає проблема інформаційної війни. Це війна нового типу, об'єктом впливу якої є свідомість людей, їхнє світосприйняття. У її основі лежить можливість керування та маніпулювання масовою свідомістю, підкорення волі людини. Найнебезпечнішим є те, що це зовсім не сприймається свідомістю тих, хто підпадає під інформаційно-психологічний вплив. Головним завданням інформаційного агресора є формування в особистості вигідної для нього картини світу, неадекватного сприйняття реальності, що робить можливим підкорення такої особистості своїй волі, а згодом, через мільйони подібних підкорених особистостей – підпорядкування всієї держави. До того ж, інструментарій інформаційних воєн пропонує засоби, за допомогою яких користувачі інформаційної зброї зможуть упродовж тривалого часу втримувати у своїх руках владу таких держав. Головне – підтримка в населення необхідної, вигідної для себе картини світу, точніше – інформаційного образу світу, який, за наявності адекватних засобів захисту від інформаційної агресії, майже неможливо змінити. Тому для того, щоб захиститися від подібної загрози, яка в дійсності являє собою загрозу національній безпеці держави, необхідно осягти природу і технології інформаційної влади над людьми та чітко виділити можливі засоби захисту від інформаційно-психологічних впливів. Метою цієї статті є конкретизація основних правил і закономірностей інформаційних воєн на основі прикладів, які так чи інакше охоплюють майже весь проміжок часу існування людства – від часів Стародавнього світу до епохи постіндустріального суспільства. Об'єктом дослідження є самі інформаційні

війни. Предмет – технології та закономірності інформаційних воєн.

Поняття «інформаційна війна» з'явилось і почало широко застосовуватися від середини 80-х років минулого століття, хоча принципи ведення воєн такого типу були відомими ще в Стародавньому світі. Так, ще в Давньому Китаї, серед методів активного протистояння противнику підкреслювалася необхідність «розкладати все добре, що є в стані ворога», «розпалювати внутрішні чвари», «заважати всіма засобами» його цілеспрямованій діяльності.

Нині існує чотири підходи щодо визначення інформаційних воєн. Перший підхід трактує їх як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі. Так, один з представників цього напрямку, відомий російський фахівець у галузі інформаційних воєн Сергій Расторгуєв, визначає їх як відкриті та приховані цілеспрямовані інформаційні взаємодії інформаційних систем з метою отримання певного виграшу в матеріальній сфері. Під інформаційною системою автор розуміє систему, що здійснює отримання вхідних даних, обробку цих даних чи зміну свого внутрішнього стану та видачу результату або зміну свого зовнішнього стану. Під час протистояння інформаційні системипостійно використовують інформаційну зброю, яка має запустити програми самознищення ворожої інформаційної системи(для людини інформаційним впливом, що здатний привести до запуску таких програм, є активізація бажань, думок і провокування вчинків, скерованих на самознищення).

На думку з представників другого підходу, інформаційна війна – це найгостріша форма протистояння в інформаційному просторі. Акцент переноситься на характер протистояння опонентів. У даному випадку першочергового значення набувають такі якості інформаційної взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва. Для позначення агресивності сторін застосовується поняття інформаційної зброї.

При такому трактуванні інформаційної, коло учасників інформаційного протиборства значно розширюється. Ними вже є не лише дві сторони, але й всі ті, хто так чи інакше є присутнім в інформаційному просторі в даний проміжок часу, а саме: громадськість, особи, які відповідають за прийняття рішень, ЗМІ і т. п. За такої інтерпретації інформаційних воєн до них часто зараховують будь-які форми ідейного протистояння різних доктрин, релігій і навіть напрямків мистецтва. Ідейні суперечності, різниця в думках і навіть звичайні пристрасті визнаються формами інформаційного протистояння.

За третім підходом інформаційна війна інтерпретується як форма забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів, наприклад, цифрових випромінювачів, супутникових передавачів та інших аналогічних засобів, які застосовуються для виконання військових завдань.

Четвертий підхід ототожнює інформаційні війни з кібернетичними війнами. Під останніми розуміють протистояння між технічними системами.

Незважаючи на розбіжності в чотирьох вищезазначених підходах до розуміння інформаційної війни, їх об’єднує спільна думка про те, що основним засобом здійснення агресивних дій і нанесення ушкоджень

противнику є інформація. При цьому існує багато способів реалізації цих дій. Ще одна спільна риса вищезазначених концепцій – розгортання інформаційних баталій у сфері інформаційного простору.

Учасників інформаційних воєн можна розглядати в двох аспектах: широкому та вузькому. Увузькому розумінні – це інформаційні системи, тобто системи, що здатні здійснювати отримання вхідних даних, обробку цих даних або зміну свого внутрішнього стану(внутрішніх зв'язків і ставлень) і видачу результату або зміну свого зовнішнього стану (зовнішніх зв'язків і відношень). У широкому – це:

- індивід;
- група індивідів;
- суспільна система;
- держава;
- група держав;
- технічна система.

Форми інформаційних воєн залежать від характеру протистояння їх учасників.

Це може бути[1, с. 258]:

- конфлікт між державами або групами держав у дусі холодної війни;
- конфлікт між державою та недержавними організаціями(наприклад, війна з тероризмом);
- боротьба всередині держави між окремими політичними одиницями під час виборчих кампаній і виборів у державні органи влади;
- війна держави проти власного населення з метою його перепрограмування;
- війна проти політики конкретних держав у сфері захисту прав людини, свободи слова та віросповідання тощо.

Інформаційна зброя.Варто підкреслити, що інформаційна зброя не є винаходом середини – кінця XX століття. Просто так сталося, що її потенціал повністю розкрився після початку нової епохи в історії розвитку людства – епохи інформаційного суспільства, основною прикметою якого є надзвичайно високий розвиток і поширення інформаційних технологій. Як результат, людство отримало якісно новий вид зброї – інформаційну зброю. Що ж являє собою цей тип зброї? Наведемо декілька визначень науковців – фахівців у галузі інформаційних воєн:

1. Як вже згадувалося вище, це інформація, яка використовується для здійснення ворожих дій і нанесення пошкоджень противнику [1, с. 258].

2.Цезасоби, які дозволяють здійснювати задумані діїразом з повідомленнями(даними), що передаються, обробляються, створюються, знищуються та сприймаються [2, с. 115].

3.Це зброя, яка відрізняється такими якостями:

- асиметрія – якість,яка може зробити окремий елемент системи сильнішим за всю систему;
- мімікрія – якість, за якої інформаційна зброя повторює формою типовий елемент даної системи, але має при цьому зовсім інше значення;
- адаптація – якість, що дозволяє змінювати середовище згідно з вимогами змісту, що вводиться[5, с. 395].

Спробуємо дати єдине визначення інформаційної зброї на основі вищезазначеного:інформаційна зброя – це інформація(дані), які є засобом ведення інформаційних воєн і призначення яких полягає в зміні системних якостей об’єкта інформаційного впливу за допомогою прихованих

установок на здійснення задуманих користувачем інформаційної зброї дій.

Напрями і приклади використання інформаційної зброї:

- порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище яке їх оточує;
- здійснення впливу на суспільну думку та позицію політичної еліти;
- завдання шкоди протилежній стороні дипломатичними засобами;
- пропагандистські, психологічні та підривні акції у сфері культури й політики;
- дезінформація;
- чутки, які створені навмисно;
- упровадження у ЗМІ своїх прибічників для проведення підривних акцій;
- проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта;
- інформаційна підтримка дисидентських та опозиційних рухів.

Далі виникає цілком закономірне запитання: які ж переваги має інформаційна зброя над традиційною? Науковці мають спільну позицію з цього приводу:основною, найістотнішою перевагою інформаційної зброї є її порівняно низька собівартість відповідно до інших видів озброєння. За критеріями ефективності/вартість вона значно виграє в інших видів озброєння. Чому? А тому, що вона не вимагає вкладення зовнішніх системдля знищення ворога, бо він апріорі володіє всіма необхідними засобами для власного

знищення. Завданням використання інформаційної зброї є «допомогти» противнику скерувати всі засоби, що є в його арсеналі (серед них і технічні), проти самого себе [6, с. 105].

До того ж дуже важливе значення має здебільшого прихований характер інформаційної зброї. Багато жертв даного виду зброї, навіть володіючи теорією та відповідною матеріально – технічної базою, усвідомили себе жертвами тільки тоді, коли було вже занадто пізно(наприклад, СРСР).

Звідси випливає необхідність знаходження ефективних засобів своєчасного швидкого розпізнавання інформаційної загрози та її оперативної ліквідації, що можна трактувати як основну проблему інформаційної безпеки.

ЗМІ як основний інститут інформаційної війни.У вік інформаційних воєн, коли основним завданням будь-якого агресора є не фізичне знищення противника, а його перепрограмування, саме ЗМІ виступають якзброя масового ураження. Якими ж є її функції і характеристики ефективності?

До основних функцій ЗМІ належать такі [6, с. 397]:

- інформувати глядача(читача);
- розважати глядача(читача);
- нав'язувати глядачеві(читачеві) точку зору своїх власників або рекламодавців, що зрештою перепрограмовує поведінку споживачів у потрібному напрямку.

Основні характеристики ефективності ЗМІ такі [6, с. 398 – 399]:

- розмір аудиторії, яка охоплюється даним ЗМІ(для друкованих засобів характеристика визначається через тираж; для телевізійних – через кількість населення, яке має необхідні технічні засоби на території покриття);
- потенційні можливості, тобто інтелектуальний потенціал населення, яке є споживачем продукції ЗМІ;

• сила інформаційного впливу, яка є головним критерієм ефективності ЗМІ. Її можна визначити як величину, що характеризує зміну стану об'єкта інформаційного впливу під час цілеспрямованого інформаційного впливу порівняно з його початковим станом. Під «зміною стану об'єкта» ми розуміємо зміну хоча б одного складового елемента інформаційної системи – об'єкта, або хоча б одного зі зв'язків між елементами системи(наприклад, зміна точки зору після прочитання або перегляду певного матеріалу ЗМІ). Якщо під час інформаційного впливу початковий стан об'єкта не змінюється, то сила цього інформаційного впливу дорівнює нулю.

Останній показник у значній мірі залежить від рівня професійної підготовки працівників ЗМІ. Дія професійно підготовленої публікації не обмежується лише вузьким колом передплатників і випадкових покупців, вона поширюється майже на все населення завдяки накладу та гучних і водночас влучних назв, які мимоволі приковують до себе увагу та сприймаються на підсвідомому рівні. Будь-який несвідомо сприйнятий, незрозумілий нині текст залишається у підсвідомості і очікує свого виходу на поверхню.

Загалом, створення конкретного матеріалу ЗМІ чимось нагадує проектування засобу масового ураження. Кількість уламків від кожного слова, від кожного сюжету намагаються зробити якомога більшим, а радіус враження – якомога ширшим. Це означає, що дія цих повідомлень має зачепити якомога більшу кількість елементів і зв'язків між ними у інформаційній системі, якаперебуває під впливом ЗМІ. Але на шляху повідомлень, що розлітаються в усі боки, є істотна перешкода: сприйняття повідомлення вимагає наявності спільних понять і категорій, що містяться в

повідомленні, та отримувача цього повідомлення. Інакше випадку повідомлення не дійде свого адресата. Тому завданням персоналу ЗМІ є виготовлення таких повідомлень, які найбільше враховують рівень своєї цільової аудиторії [6, с. 405 – 406].

Історія інформаційних воєн нині включає до себе такі війни, які завершувалисязазвичай або революцією, або переворотом [4, с. 31]:

- холодна війна між країнами соцтабору на чолі з СРСР і західним блоком, очолюваним США;
- «оксамитові революції» в країнах Східної Європи наприкінці 80х років;
- «революція троянд» у Грузії (2003);
- «помаранчева революція» в Україні (2004);
- спроба «джинсової» революції в Білорусі (2006);
- російсько-грузинська війна (2008);
- український «Євромайдан» (2013) іросійська окупація Криму (2014).

Безумовно, найважливішою з вищезазначених інформаційних воєн є холодна війна, яка, на думку деяких авторів, являла собою, по суті, третю світову війну, інформаційно-психологічну за своїм характером. Саме її можна вважати першою повноцінною інформаційною війною, тому що інформаційний вплив з обох боків здійснювався усвідомлено, на базі наукових рекомендацій відповідних дисциплін. До того ж, надзвичайного рівня розвитку набули комп'ютерні системи, які зробили можливою побудову моделей інформаційного впливу.

Наслідки інформаційної війни.Якщо виходити з того, що інформаційна війна нічим не відрізняється від звичайної війни, за винятком типу зброї, що використовується, то ознаки поразки мають бути такими ж. Для такої системи, як

держава, поразка у традиційній війні характеризується такими наслідками [2, с. 155]:

- загибель та еміграція частини населення;
- руйнація промисловості та сплата контрибуції;
- втрата частини території;
- політична залежність від переможця;
- різке скорочення збройних сил;
- вивіз наукомістких технологій.

Провівши узагальнення, можна сказати, що для інформаційних систем поразка має такі ознаки [2 с. 155 – 156]:

- скорочення структури інформаційної системи, загибель її елементів і підструктур; таке спрощення системи робить її безпечною для агресора;
- виконання завдань у площині інтересів переможця. Система обробляє тільки ті дані, які отримує від переможця;
- переможена система вбудовується до алгоритму функціонування системи переможця, тобто поглинається її структурою.

Як бачимо, для переможеної сторони майже немає різниці, у якій війні вона програла – чи то у звичайній, чи в інформаційній. Різниця може бути тільки в тому, що інформаційна війна не має чітко окресленого завершення на відміну від звичайної, фінал якої, як звичано, визначається підписанням мирної угоди. До того ж, агресор навряд чи відмовиться від можливості подальшого контролювання завойованої системи, бо це дозволить йому протягом тривалого часу отримувати виграш у матеріальній сфері.

Отже, теорія інформаційних воєн пояснює термін «інформаційна війна», описує її принципи та закономірності; займається вивченням основних якостей і можливостей застосування інформаційної зброї; досліджує інститути інформаційної війни; встановлює можливі для

інформаційної системи наслідки поразки або перемоги в інформаційній війні та намагається передбачити сценарії інформаційних воєн у майбутньому.

Отже, зазначимо, що поняття інформаційної війни з'явилося лише у 80х роках XX століття, тоді як інформаційні війни у тому чи іншому вигляді пронизують майже всю історію людства. Але усвідомлено інформаційна зброя почала застосовуватися саме від 70х років XX ст., коли людство почало вступати до інформаційної ери, яка характеризується визнанням пріоритету за знанням, інформацією та інформаційними технологіями.

Існує багато підходів щодо визначення інформаційної війни. Усі наявні дефініції можна звести до такого загального визначення: інформаційна війна – це протистояння між інформаційними системами, які є учасниками інформаційних воєн, у сфері інформаційного простору з використанням інформаційної зброї за виграш у матеріальній сфері.

Інформаційна зброя є основним знаряддям конфронтуючих сторін для нанесення ушкоджень один одному. Її визначають як інформацію, призначення якої полягає в зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих у ній установок на здійснення задуманих користувачем інформаційної зброї дій. Основними перевагами інформаційної зброї є її над дешева порівняно з іншими видами озброєнь собівартість і здебільшого прихований характер.

Ведення інформаційної війни спирається на певні принципи. Найважливішими серед них є такі:

- намагання розширення інформаційного простору під власним контролем;

- скерування інформаційного впливу проти найуразливіших елементів інформаційної структури противника;
- жорсткий спротив інформаційним акціям ворога та зменшення сфери його впливу;
- використання комплексного підходу при формуванні стратегії інформаційної війни, тобто поєднання суто інформаційних методів впливу з економічними, військовими, політичними і т.д.

Необхідною умовою для проведення інформаційних операцій є залучення інститутів інформаційної війни, серед яких чи не найважливіше значення мають ЗМІ, що зумовлено особливостями інформаційної епохи.

Стратегія інформаційної війни є загальним планом ведення інформаційної війни. Розробка стратегії зводиться до чіткого окреслення низки елементів ворожої інформаційної структури, на яких буде спрямовуватись інформаційний вплив, їхніх властивостей і потенційних можливостей, засобів інформаційного впливу та заходів щодо забезпечення інформаційної безпеки власної інформаційної структури.

Наслідки від програшу в інформаційній війні є подібними до наслідків від поразки у війні з використанням традиційних видів озброєнь. Подібно до того, як переможена держава втрачає частину своєї території, населення, промислового потенціалу і підпадає під економічну та політичну залежність від переможця, інформаційна система позбавляється частини своєї структури, змушена виконувати завдання, які містять в площині інтересів переможця, і згодом поглинається його інформаційною структурою.

Література

1. Политические коммуникации: учебное пособие для студентов вузов/под ред. Соловьёва А.И. – М . : Аспект Пресс, 2004. – 332 с.
2. Расторгуев С.П. Философия информационной войны. – М . : Московский психолого-социальный институт, 2003. – 496 с.
3. ПочепцовГ.Г. Информационные войны. – К . : Ваклер, 2001. – 576 с.
4. РасторгуевС.П. Информационная война. Проблемы и модели. Экзистенциальная математика: учебное пособие [для студентов вузов, обучающихся по специальностям в области информационной безопасности]. – М . : Гелиос АРВ, 2006. – 240 с.
5. Кара-Мурза С.Г. Манипуляция сознанием. – М . : Эксмо-Пресс, 2004.– 368с.
6. Зиновьев А. Русскийэксперимент. – М . : Наш дом, 1995. – 284 с.
7. Кара-Мурза С.Г. Экспортреволюции. – М . : Алгоритм, 2005. – 462 с.
8. ПочепцовГ.Г. Психологические войны. – К . : Ваклер, 2002. – 528 с.

In the articte the author carried out analyze of existing technologies, definitions of the informational was and offered his own grounded definition, defined main features, appropriateness and outcomes of the informational war. Also character of the informational war was researched.

Key words: informational war, informational and psychological influence, forms of informational war, Mass-media, informational arm, outcomes of informational wars.

В статье автор осуществил анализ сущесствующих технологий, дефиниций «информационнойвойны» и

предложил свое обоснованно еавторское понимание, определил основне черты, закономерности и результатыинформационны хвоен. Также в статье было исследовано характер информационной войны.

Ключевые слова: информационная война, информационно-психологическое влияние, формы информационных воен, СМИ, информационное оружие, результаты информацинных воен.