Інтернет як нове середовище ведення інформаційних війн

У статті розкривається суть поняття «інформаційна війна», розглядаються її основні елементи, а також досліджується взаємозв'язок між інформаційними протистояннями та Інтернетом. У статті представлені основні переваги використання Інтернету.

Ключові слова: інформаційна війна, інформація, Інтернет, гроза, атака, небезпека.

В статті розкривається суть поняття «інформаційна війна», вважається її основним елементом, а також досліджується взаємозв'язок між інформаційними протистояннями та Інтернетом. В статті представлені основні переваги використання Інтернету.

Ключові слова: інформаційна війна, інформація, Інтернет, угроза, атака, опасність.

In this article the essence of concept «information warfare» is discovered, all its main components are considered. The interrelation between information contention and Internet is investigated. Fundamental advantages of Internet are presented in this paper.

Key words: information warfare, information, Internet, threat, attack, danger.

Із настанням XXI століття інформація посідає чи не найважливіше місце у житті людей. Звичайно, саме завдяки їй ми проходимо етап соціалізації, інтегруємося у суспільство. Завдяки інформації ми здобуваємо глибокі знання, отримуємо життєвий досвід, удосконалюємо власні здібності, покращуємо професійні навички, навчаємося чогось нового. Однак у зв'язку із науково-технічною революцією, розвитком новітніх технологій, прогресом засобів комунікації, впровадженням світових досягнень людства інформація розглядається абсолютно під іншим кутом зору. Тепер вона як ніколи не лише основним регулятором і каталізатором будь-яких відносин, але і надтою взаємною зброєю та засобом впливу. можна із впевненістю сказати, що сьогодні людство переживає глобальну інформатизацію, при чому залежність сучасного суспільства від якісної та релевантної інформації стрімко зростає.

Неодноразово висловлювалась думка про те, що із настанням третього тисячоліття людство у світі буде оцінюватися не стільки величиною економічного потенціалу, кількістю бойових військ чи об’ємом отриманих прибутків країни, скільки її вміння контролювати інформаційні процеси.

Сучасні досягнення у сфері інформаційних технологій все впевніше завойовують різні види діяльності суспільства. Останнім часом такий феномен досягнув настільки масштабних розмірів, що життєво-необхідні інтереси держав (особливо у сфері інформаційної безпеки) опинилися під загрозою. Сьогодні під прицілом опинилася перспективна сфера діяльності – професійний спорт. Тому державні системи захисту інформації перебувають у глибині кризовій ситуації.

Так як проблематика інформаційних війн є надзвичайно широю, підходи, погляди та різні аспекти надзвичайно активно вивчаються науковцями. На сьогодні представлено багато праць та статей, які присвячені саме специфіці і питанням інформаційних протистоянь із закрем. Серед науковців та дослідників, які вивчають цю проблему, а також розглядали її різні аспекти, слід відзначити таких вітчизняних та зарубіжних фахівців як А. Манойлов [6], В. Циганов, Г. Почепцов, І. Панаріна [7], М. Галамба, М. Лібікі, О. Цветков [9], П. Кузьмечен, Р. Првасеньський [10], С. Бухарін, С. Расторгуєв [8] та інших. Особливо варто привести увагу науковому досягненню І. Панаріна, який досліджував інформаційну війну у кількох суміжних аспектах: політика, геополітика та дипломатія [7]. Що ж стосується об’єкту статті, то Інтернет як нове явище в інформаційному суспільстві розглядалося багатьма дослідниками у різноманітних напрямках. Сьогодення вивчення
ні глобальної мережі зробили І. Стялова, І. Биков, Л. Іловайська, М. Хейг, які аналізували використання Інтернет-технологій у PR; А. Калимов, Дж. Гол. Л. Коханова, які розглядали особливості Інтернет у мас-медійному середовищі. Однак П. Ажед, Ф. Бредон, Р. Гордон, Г. Грезійон, К. Керделлан, К. Янг, О. Войсківський у порівнянні з іншими вже конкретніше досліджують Інтернет і розуміють його як чергову інновацію, створену людьми для поліпшення її урізноманітнення життя. Але зараз дуже важко ви- ділити вітчизняних чи зарубіжних дослідників, які б конкретно займалися питанням інформаційних війн та Інтернету. Тому за доцільне вважаємо продовжувати дослідження цієї тематики, адже вона є надзвичайно перспективною та актуальним у наш час.

Основним завданням статті є розкриття суті поняття «інформаційна війна» та розгляд його основних складових елементів. Однак вперше чергу потрібно оцінити взаємозв’язок між інформаційними використанням та Інтернетом, а також дослідити влив нового явища на суспільство. Інформаційною війною є сукупність методів та способів ціле- спрямованого впливу суб’єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні і інформаційно-технічні системи, системи формування масової невідомості та психічної окремої людини, з використанням усіх властивостей інформації, інформаційних ресурсів та нових інформаційно-телекомунікаційних технологій з метою штучного створення факторів гальмування розвитку людино- суспільства та держави, встановлення контролю над інформаційними ресурсами потенційного супротивника задля отримання переваг у приоритетних сферах суспільного життя [1, с. 6]. Інформаційна війна має два аспекти: технологічний та ідеологічний [8, с. 222-226]. З точки зору першого, мова йде про те, що у визначений час приводиться в дію програмні віруси, логічні бомби, закладені у пам’яті інформаційних комп’ютерних мереж. Вони здатні зруйнувати і знищити програми управління, бази даних, вивести з ладу важливі об’єкти (наприклад, пошкодження роботи з рахунками у зарубіжних банках, заглушення теле- і радіо- омовлення у певному регіоні, припинення діяльності армійських
відміну від бомби або іншої небезпечної зброї, яка знищує всіх, інформаційна війна діє вибірково, охваючи лише цільову групу, яка має значними усиллями змоделювати конкретний план: атакувати та змінювати аудиторію впливу залежно від ситуації.

При веденні інформаційної війни можливе багаторазове захоплення одиних і тих ж людей, що виражається в атаки різних тематичних зон свідомості. А отже, це збільшує шанси ефективної маніпуляції над масами. Тому інформаційна війна представляє більшу загрозу у порівнянні із звичайною.

Людина не в змозі реагувати на невидиму дію (наприклад, радіацію). Більш того, така дія може приймати і доброзичливу форму, на яку біологічно людина ніколи не готова відповідати, навіть агресивно. Тому головна небезпека інформаційної війни – відсутність вимірних руйнувань, що характерні для звичайних вій. Суспільство навіть не підозрює, що воно піддається впливу. Як результат – люди не використовують навіть у їх розпорядженні захищені механізми. Загалом, інформаційна війна виглядає як «мирна», оскільки може вестися на фона благополуччя та миру [7, с. 93].

На відміну від війн минулого, простір та відстань не є перешкодою для інформаційних війн, особливо коли їхнім середовищем є Інтернет. Саме він є тим катализатором, який сприяє та пришвидшує рух процесів, які відбуваються у суспільстві, політиці, економіці та інших сферах життєдіяльності, та дозволяє дистанційно контролювати інформаційні війни.

В інформаційній війні змінюється роль впливу: від сухого фізичного (знищення об’єкта, завдання шкоди), до комунікативного. Основним завданням тепер постає зміна комунікативного оточення об’єкта. Війни, що були направлені на завоювання простору, змінилися війнями, які борються за знання. «Інформаційні технології дозволяють забезпечити розширення геополітичних криз, не зробивши жодного пострілу» [6, с. 58-59, 62].

Основними цілями інформаційної війни є бажання контролювати інформаційний простір, при чому зазнаючи власний від негативного впливу ворожих дій (контрінформація); контроль за інформацією для ведення інформаційних атак на ворога, підвищення ефективності сил спротиву за допомогою всебічного використання основних функцій інформації [3]. В принципі це є загальні та найбільш поширені завдання війни, проте слід пам’ятати, що вони можуть відрізнятися і залежати від певної специфіки тактики чи стратегії протисторбства. Наприклад, якщо інформаційна війна ведеться проти конкретної держави, основними цілями буде ініціювання страйків, масових заворушень, інших акцій протесту і неподорожні сходження з іншими державами; маніпулювання політичною орієнтацією населення для створення політичної напруту та стану, близького до хаосу; зниження рівня інформаційного забезпечення органів влади та управління; введення на- селення в оману щодо роботи державних органів влади, підтримку інформації, дискредитація їх дій, тощо.

За Бережною М. С. поле дії інформаційних воєн є досить широким і охоплює наступні області:

– всесвітня мережа Інтернет;
– системи управління та прийняття рішень (цивільні, військові, соціальні, культурні);
– інфраструктура систем життєзабезпечення держави (системи телекомунікації, енергетики, фінансів, промисловості, транспортних мереж);
– військова інформаційна інфраструктура (системи контролю, управління і з’єднання, розв’єдківкі);
– система особистих даних (закони та використання паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації);
– система охорони та захисту від шпигунства (розкриття та розкритівка інформації, сповіщення або знищення особливо важливих даних, послуг); збір інформації оновлення характеру про конкурентів) [2, с. 7-10].

Порівнюючи всі ці області ведення інформаційної війни, на перспективних та найактуальніших сьогодення, звичайно, залишається Інтернет. Але він володіє низьком переваг, яким не можна похвалитися інші види війн.

Найчастіше інформаційні війни ведуться у політичній, дипломатичній, фінансово-економічній та військових сферах. Хоча
останнім часом можна стосередити нову тенденцію — ведення інформаційних атак у сфері професійного спорту. Однак потрібно розрізнити два види таких протиріб: інформаційно-психологічне та інформаційно-технічне. Вони дуже схожі пов’язані із двома аспектами інформаційних вій — ідеологічним та технологічним відповідно. Найважливішими об’єктами впливу і захисту першого є психіка політичної еліті та населення, системи формування масової свідомості та думки, прийняття рішень. І це що стосується інформаційно-технічного, тоби системи передачі даних та системи захисту інформації.

Принцип великої популярності інформаційних вій у XXI столітті є безліч, але основним є наступний. Велика різниця у якості та кількості знань представників різних соціальних груп та бажання змагатися новими цікавими фактами. По-друге, існує неперевершено велика різниця в психологічних, соціальних і матеріальних силах їхніх конкурентів з однієї сторони, та посилень власні з іншої. По-третє, використовуються різні методики впливу (особливо пропагандистські) на свідомість людей. По-четверте, війна є однією з тих важливих складових ідеологічної боротьби, яка завжди є наперед спланована, узгоджена та цілеспрямована дією, яка має власну стратегію, цілій набор методів та засобів. Звичайно, її наслідки не обов’язково призводять до кровопролиття, руйнувань або численних жертв. Але така увага псевдобезпека лише маскує реальні наслідки інформаційної війни, адже вони за своїми масштабами куди серйозніші у порівнянні із звичайними. Як мінімум, це може викликати дискомфорт та стрес, також здійснюється величезний вплив на масову свідомість, руйнується загальна стабільність у багатьох сферах життя. Найгірше, чого варто очікувати, це зниження психології людини, суспільства, нації, ризика військових відбувається, узгоджених правил, стеретотипів та установок. Тому твердження, що інформаційна війна є спонтанним явищем або результатом випадкових подій, абсурдно помилкове.

Разом із стрімким розвитком новітніх технологій та більшою кількістю таких взаємодій з іншими групами (включаючи внутрішні) або державами, виникають нові та більш складні проблеми, які у подальшому можуть призвести до інформаційної ві-
реального часу. Крім того, вона підготовка та оформлення матеріалу в електронному вигляді займає небагато часу, що значно збільшує ефективність і швидкість ведення інформаційної війни.

Економічність. Для звичайної інформаційної атаки достатньо залучити як мінімум підготовленого користувача персонального комп'ютера (що включає можливість використання кількість комп'ютера та матеріальних засобів для вирішення поставлених завдань. У порівнянні з звичайною війною, засоби комп'ютерних технологій дають значно більший ефект та істотно менші витрати.

Дистанційний характер впливу на комп'ютерні системи у різних регіонах світу. Прикладом такого переваги може бути атака на комп'ютери системи одного з каліфорнійських операторів, який здійснювався навесні 2001 року на території однієї з провінцій Китаю через американські веб-сервери, що розташовані в трьох містах США. Цей кібер-напад виявив лише через 17 днів.

Масштабність можливих наслідків. Окрім впливу на формування громадської думки, деякі дії на позиції офіційних осіб, які приймаються найважливіші рішення, використання Інтернету може призвести до порушення балансу функціонування деяких елементів або тривалого виведення з ладу життєво необхідних об’єктів і систем в окремих районах, країнах або регіонах.

Комплексність інформації та її сприйняття. На веб-сайтах можна розміщувати як текстову, так і графічну інформацію, а її обсяг може у сотні разів перевищувати об’єм будь-якого друкованого видання, радіо- або телепередачі. Використання сучасних мультимедійних технологій дозволяє одночасно здійснювати вплив на декілька органів чуття, що має додатковий емоційний вплив.

Доступність інформації. За словами Хамадун Туре, генерального секретаря Міжнародного союзу електроніки (посвячена установа ООН), загальна кількість користувачів Інтернету на початку 2011 року становила дві мільярди. У лічені секунди будь-хто безперешкодно отримує доступ до інформації, яка належить різним країнам, нехтуючи при цьому прикордонними, цензурами та інші бар’єрами [4].

Можливість дезінформувати здійснюється шляхом розсилання електронних листів, розміщення постів на форумах, бло-

Отже, під інформаційною війною потрібно розуміти різносторонню і цілісну стратегію, яка спричинена підвищення значущіс- тю і цінністю інформації у сфері політики, економіки, оборони та безпеки держави. Дуже часто у ході такої боротьби використовуються переваги технологічних вдосконалень і досягнень сьогоден- ня, зокрема Інтернет. Основною зброєю такої боротьби вва- жаються повідомлення ЗМІ та нетрадиційних джерел інформації, які використовуються для широкомасштабного, целісноправодя- ного, швидкого та таємного впливу на цивільні, військові, еконо- мічні та державні загали інформаційні системи противника.

Найпоширенішою формою війни сьогодення вважається інформаційна війна, об’єкт якої бацькує на можливості підкорення волі людини, управлянні знаннями та маніпулювання суспільною свідо- містю. Основна небезпека такого протитворства полягає у різкому збільшенні масштабу бойових дій за рахунок глобальної мережі Інтернет, а також у тому, що такий вплив здійснюється ірраціонально та приховано, тому виявити інформаційно-психологічну дію вдається не одної і не завжди.

Література:


