Запорожець О.Ю.*

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО У ЗОВНІШНІЙ ПОЛІТИЦІ США

Стаття присвячена американській концепції інформаційної війни. Розкрито основні терміни, охарактеризовано компоненти інформаційних операцій, визначено етапи планування психологічних операцій як ключового компоненту інформаційної війни.

Ключові слова: інформаційна війна, компоненти інформаційної операції, психологічна операція, США.

Статья посвящена американской концепции информационной войны. Раскрыта суть основных терминов, дана характеристика компонентов информационных операций, определены этапы планирования психологических операций как ключевого компонента информационной войны.

Ключевые слова: информационная война, компоненты информационной операции, психологическая операция, США.

The article focuses on the American approach to information warfare. This article contains definitions of key terms, description of information operations capabilities and planning process of psychological operations as a principal component of information warfare.

Keywords: information warfare, USA, information operation capabilities, psychological operations.

В сучасному світі інформація перетворилася на стратегічний державний ресурс, який дає змогу не лише впливати на міжнародні процеси, а й породжувати ті чи інші події та явища на національному, регіональному та міжнародному рівнях, й скеровувати думки, емоції та поведінку громадськості у бажаному напрямі.

Сучасна боротьба між суб'єктами міжнародних відносин за позиції на міжнародній арені, сфери впливу та досягнення пріоритетних національних цілей відбувається значною мірою в інформаційному просторі.

За цих умов актуальним є питання розробки і ведення інформаційної війни. Характерними рисами інформаційної війни є гнучкість і непередбачуваність арсеналу інформаційного впливу, поетапність і вибірковість його здійснення, можливість багаторазового охоплення тієї ж самої аудиторії, відсутність видимих руйнувань, множинність впливу з високим рівнем координації у часі і просторі; відсутність необхідності фізичного вторгнення на територію супротивника, складність виявлення джерела інформаційної атаки, визначення рівня небезпеки, істинних масштабів та цілей агресії тощо.

* кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Розвинені країни світу значну увагу приділяють дослідженню і розробці концепції інформаційного протиборства. Серед західних країн провідна роль в цьому питанні належить Сполученим Штатам Америки.

Метою даної роботи є висвітлення американської концепції інформаційної війни.

Вперше термін «інформаційна війна» було використано Томасом Роной у звіті «Системи зброї та інформаційна війна», підготовленому у 1976 році для компанії «Боїнг». У звіті відмічалося, що інформаційна інфраструктура стає ключовим компонентом американської економіки, і водночас перетворюється на уразливу ціль як у воєнний, так і в мирний час. Звіт Т.Рони зацікавив американських спеціалістів, відповідальних за «секретні матеріали», а також військове командування.

В офіційних документах Міністерства оборони США термін «інформаційна війна» з'явився після операції «Буря у пустелі» 1991 року, в якій вперше були використані новітні інформаційні технології як засіб ведення військових дій. У 1998 році Міністерством оборони США було затверджено Об'єднану доктрину інформаційних операцій, в якій інформаційна війна визначається як комплексний вплив (сукупність інформаційних операцій) на систему державного та військового управління супротивника, на його військово-політичне керівництво, що вже у мирний час сприяв би прийняттю бажаних для сторони-ініціатора інформаційного впливу рішень, а під час конфлікту повністю паралізував функціонування структури управління супротивника [1].

За американською концепцією, інформаційна війна реалізується на двох рівнях: державному та військовому.

На державному рівні мета інформаційного протиборства полягає у послабленні позицій конкуруючих держав, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери суспільного життя, здійснення психологічних операцій, підривних та інших пропагандистських акцій.

На військовому рівні інформаційна війна є складовою військових кампаній і спрямована на досягнення інформаційної переваги шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації, інформаційних систем та інфраструктури.

Інформаційна перевага визначається як здатність збирати, обробляти та розподіляти безперервний потік інформації про ситуацію, перешкоджаючи супротивнику робити те ж саме, а також як здатність визначати і підтримувати такий темп проведення операції, який перевершує темп супротивника, постійно домінуючи і залишаючись непередбачуваним, і діяти, випереджаючи супротивника у реагуванні.

Інформаційна війна реалізується у формі інформаційних операцій (ІО).

Інформаційна операція визначається як комплекс заходів, що спрямовані на здійснення впливу на інформацію та системи управління супротивника при одночасному захисті своєї інформації та інформаційних систем [2].

В «Стратегії інформаційних операцій» 2003 року просувається ідея «повноспектрових інформаційних операцій». Це означає, що інформаційні операції мають проводитися безперервно (і в мирний час, і при загостренні конфлікту) і спрямовуватися, як на населення і особовий склад збройних сил своєї країни, так і на громадян і збройні сили країн-союзників і країн-супротивників США у потенційному конфлікті.

Структурно інформаційні операції включають основні, підтримуючі і допоміжні компоненти [3].

Основними компонентами інформаційної операції є радіоелектронна боротьба, комп'ютерні мережеві операції, психологічні операції, операції з оперативного маскування та операції безпеки.

Радіоелектронна боротьба (РЕБ) – це військові дії, що передбачають здійснення впливу на обладнання супротивника за допомогою спрямованих електромагнітних хвиль.

Широкомасштабне застосування РЕБ було продемонстровано Сполученими Штатами ще у 1991 році під час війни в Перській затоці («Буря в пустелі»). За декілька днів до начала операції завдяки РЕБ на території Іраку були виведені з ладу системи державного і військового управління, системи протиповітряної оборони та зв'язку.

В 2011 році під час військової операції в Лівії американські військові використали новий літак радіоелектронної боротьби EA-18G Growler. Літак укомплектовано підвісними контейнерами з модернізованою системою ICAP III (Improved Capability III), за допомогою якої здійснювалися радіорозвідка та придушення систем радіозв'язку і радіолокації супротивника. EA-18G Growler здатен розвивати швидкість 2150 кілометрів на годину і діяти в радіусі 740 кілометрів на висоті до 15240 метрів.

Комп'ютерні мережеві операції включають комп'ютерні мережеві атаки, мережевий захист та використання комп'ютерних мереж супротивника у своїх цілях. Комп'ютерні мережеві атаки – це дії із застосуванням апаратно-програмних засобів, спрямованих на використання, перекручування, підміну або знищення інформації в комп'ютерах та комп'ютерних мережах супротивника або ж виведення з ладу самих комп'ютерів. Під мережевим захистом розуміються заходи, що передбачають моніторинг та аналіз мережевих атак на комп'ютерні об'єкти Міністерства оборони США та захист від них.

Психологічні операції (ПсО) - це заходи з поширення спеціально підготовленої інформації для впливу на емоції, прийняття рішень та поведінку цільових аудиторій у сприятливому для суб'єкта впливу напрямку.

В Польовому Статуті Армії США психологічні операції визначаються як планова пропагандистська і психологічна діяльність у мирний і воєнний час, спрямована на іноземні ворожі, дружні чи нейтральні аудиторії з тим, щоб вплинути на їхнє ставлення і поведінку у сприятливому напрямку для досягнення політичних та військових національних цілей США [4]. Психологічні акції передбачають використання ЗМІ та допоміжної діяльності (демонстрація сили, громадянська непокора, мітинги, демонстрації, програми в сфері освіти, медицини тощо) з метою підриву престижу та впливу супротивника у ворожих, нейтральних і союзних країнах.

Психологічні операції поділяються на стратегічні, оперативні та тактичні.

Стратегічні психологічні операції здійснюються в інтересах досягнення довгострокових цілей, покликаних створити сприятливу психологічну ситуацію для ведення воєнних дій. Об'єктами впливу виступають іноземні уряди, збройні сили, а також цивільне населення. На даному рівні психологічні операції можуть проводитись у формі пропаганди певних політичних або дипломатичних позицій, офіційних заяв або повідомлень керівників держави.

Оперативні психологічні операції здійснюються в інтересах досягнення середньострокових цілей, на підтримку військових кампаній. Об'єктом таких операцій зазвичай є населення певного регіону. На цьому рівні використовуються листівки, радіо- і телемовлення, засоби гучномовного зв'язку для поширення повідомлень, що містять заклики до масового саботажу, дезертирства, втечі або капітуляції.

Тактичні психологічні операції здійснюються в інтересах досягнення короткострокових цілей, на підтримку командирів тактичної ланки. Об'єктом таких операцій є те чи інше

угруповання військ супротивника. На тактичному рівні використовується гучномовний зв'язок та інші засоби для нагнітання страху, розпалення розбіжностей і посилення непокори в рядах супротивника.

Останнім часом для здійснення психологічного впливу на супротивника активно використовується мережа Інтернет. Так, під час військової кампанії в Іраку на початку 2003 року Збройними Силами Сполучених Штатів була організована розсилка електронною поштою листів іракським генералам із закликами не виконувати накази С. Хусейна. Вищим офіцерам нав'язувалася думка про те, що іракці понесуть величезні втрати, якщо не приєднаються до боротьби проти Саддама Хусейна. В електронних повідомленнях, підготовлених американськими військовими психологами, також містилися звернення до громадян Іраку допомогти запобігти використанню зброї масового знищення та позначати місцезнаходження складів хімічної, біологічної і ядерної зброї «світловими сигналами» [5].

Як зазначають спеціалісти з психологічних операцій, мережа Інтернет може використовуватися Збройними Силами США для сприяння у вирішенні неконвенційних військових задач, ведення пропаганди і контрпропаганди, поширення дезінформації про супротивника, а також інформаційної роботи з нейтральними країнами.

Надзвичайно перспективним засобом ПсО є соціальні мережі. Ще у 2000 році в доповіді комітету військових наукових досліджень Міністерства оборони США про перспективи психологічних операцій йшлося про використання таких інтернет-технологій як чати і служби обміну повідомленнями для ініціювання керованих дискусій з метою здійснення впливу на громадян [5].

Операції з оперативного маскування (введення в оману) - це заходи, призначені для навмисного введення в оману військового керівництва супротивника щодо військових можливостей, намірів та операцій, аби спонукати супротивника до дій, які сприятимуть досягненню поставлених цілей. По суті це вплив на органи прийняття рішень супротивника через його системи збору, аналізу та розповсюдження інформації шляхом надання хибної інформації та приховування ознак реальних дій збройних сил [1].

ПсО та операції з оперативного маскування доповнюють одна одну. Метою операцій з оперативного маскування є підштовхнути супротивника до неправильного аналізу і змусити його дійти помилкових висновків. ПсО передбачають заперечення достовірної інформації та перешкоджання правильній оцінці супротивником реальних планів країни-ініціатора впливу [3].

Операції безпеки - це процес ідентифікації критичної інформації та подальшого аналізу дій, спрямованих на визначення даних, необхідних супротивнику для отримання точної інформації про сили і наміри союзників; заперечення критичної інформації супротивника про сили і наміри союзників; спонукання супротивника недооцінювати доречність відомої йому критичної інформації.

До *підтримуючих елементів ІО* відносяться безпека інформації (information assurance), фізична безпека, фізичні атаки та контррозвідка [3].

Безпека інформації (information assurance) – це заходи щодо захисту інформації та інформаційних систем шляхом забезпечення їхньої доступності, цілісності, автентичності, конфіденційності тощо.

Фізична безпека – це фізичні заходи, призначені для захисту персоналу, попередження неавторизованого доступу до обладнання, споруд, документів та захисту їх від шпіонажу, саботажу, пошкоджень та крадіжок. Забезпечення фізичної безпеки передбачає визначення уразливостей, застосування засобів стримування та контролю, а також реагування на зміни обстановки.

Фізичні атаки є складовою військових операцій і полягають у фізичному руйнуванні, пошкодженні або знищенні об'єктів супротивника. Такі атаки можуть використовуватися як засіб впливу на командно-управлінські системи супротивника, аби порушити його здатність впливати на цільові аудиторії. Крім того, на підтримку фізичної атаки можуть використовуватись психологічні операції, аби посилити вплив атаки на моральний стан супротивника.

Контррозвідка – це збір інформації та діяльність, спрямована на захист від шпіонажу, інших дій розвідки, саботажу або вбивств, замовлених або здійснених від імені іноземних урядів, іноземних організацій/особистостей або міжнародних терористичних груп.

Допоміжними компонентами ІО, за американською концепцією, є Public Affairs (PA), цивільно-військові операції, публічна дипломатія [3].

Public affairs (суспільні справи або суспільно-політична комунікація) - це заходи з поширення інформації про діяльність оборонного відомства США для внутрішньої і зовнішньої аудиторій. Основними принципами РА є правдивість, своєчасність, точність, узгодженість, послідовність поширюваної інформації. Пріоритетними об'єктами впливу є особи і групи, об'єднані явним чи потенційним інтересом до діяльності оборонного відомства.

Загальною метою РА є переконати цільові аудиторії у соціальній значущості оборонного відомства, тобто у тому, що відомство працює на благо країни і тому заслуговує на суспільну підтримку. Спеціалісти з РА надають допомогу військовим у розробці та поширенні повідомлень для ЗМІ, проводять моніторинг сприйняття подій внутрішньою і зовнішньою аудиторією, визначають базові принципи медіа супроводу військових операцій, протидіють дезінформації з боку супротивника, розробляють стратегії інформування внутрішньої і зовнішньої аудиторії про військові можливості та рішучі наміри держави, роз'яснюють цілі та наміри військового керівництва у потенційному конфлікті, забезпечують розуміння з боку громадськості місії військових та їх внеску у зміцнення національної безпеки тощо [6].

Цивільно-військові операції – це діяльність військового командування щодо встановлення, підтримки та здійснення впливу на відносини між військовими силами, урядовими і неурядовими громадськими організаціями та цивільним населенням. Ці операції проводяться під час військових кампаній з метою подолання причин нестабільності, надання допомоги у постконфліктній реконструкції тощо.

Публічна дипломатія – це відкрита міжнародна інформаційна діяльність американського уряду, спрямована на просування зовнішньополітичних цілей держави шляхом розуміння, інформування та впливу на зарубіжні аудиторії, а також розширення діалогу з громадянами інших країн.

На оперативному рівні публічна дипломатія включає презентації і брифінги з висвітленням політики Міноборони; просування політики уряду шляхом створення відповідних суспільно-політичних організацій і проведення ідеологічних заходів; управління діяльністю регіональних інформаційних центрів тощо [2].

Серед вказаних вище компонентів ІО ключова роль у реалізації ІО належить психологічним операціям. ПсО є змістовним наповненням ІО, а радіоелектронна боротьба, комп'ютерні мережеві атаки, оперативне маскування та інші є технологіями реалізації.

Про визначальну роль саме психологічного впливу свідчить, зокрема, звіт експертів провідного американського аналітичного центру RAND «Стратегічне інформаційне протиборство» (1998 р.). В звіті йдеться про інформаційне протиборство другого покоління, яке призведе до повної відмови від використання силових методів. За допомогою інфор-

маційного протиборства другого покоління можуть бути реалізовані такі завдання, як створення атмосфери бездуховності, негативного ставлення до культурної спадщини супротивника; маніпулювання масовою свідомістю і політичною орієнтацією соціальних груп населення для породження політичної напруженості і хаосу; дестабілізація політичних відносин між партіями і рухами з метою провокування конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби; зниження рівня інформаційного забезпечення органів влади; дезінформування населення про роботу державних органів, підрив їхнього авторитету; ініціювання страйків, масових заворушень; підрив міжнародного авторитету країни тощо [2].

Від ефективності ПсО значною мірою залежить успіх всієї інформаційної операції. У зв'язку з цим американські експерти приділяють значну увагу плануванню психологічних операцій [7]. Процес розробки психологічної операції включає декілька етапів: 1. складання плану ПсО; 2. аналіз цільової аудиторії; 3. розробка концепту матеріалів ПсО та плану їх розповсюдження; 4. виробництво і поширення матеріалів ПсО; 5. оцінка ефективності ПсО.

В плані ПсО чітко визначено місію, цілі операції, цільові аудиторії, їхню бажану реакцію та засоби впливу (ЗМІ, листівки і т.п.).

Психологічні операції в 21 столітті свідчать, що пріоритетною місією американських ПсО є зміна політичного керівництва/режиму в країні (інформаційна операція проти Іраку, операція в Лівії, «кольорові революції» тощо). Цілями таких операцій є, насамперед, дискредитація політичного керівництва супротивника, підвищення авторитету опозиції, деморалізація збройних сил країни-супротивника, посилення впливу неурядових організацій тощо. Цільовими аудиторіями, як правило, є власне населення, політичне керівництво та населення інших країн, політичне керівництво, військові та населення країни-супротивника.

Аналіз цільової аудиторії передбачає відбір цільової аудиторії, ідентифікацію умов, в яких знаходиться аудиторія та її вразливих місць, визначення способів переконання, символів та каналів комунікації.

При відборі цільової аудиторії враховуються дві основні характеристики: схожість умов проживання і вразливих місць та здатність реагувати на поширювані повідомлення належним чином. Найкращою цільовою аудиторією вважаються так звані «вторинні групи», тобто групи, що створюються для досягнення певної мети. Коли мету досягнуто, то група розпадається або переключається на іншу мету. Такими групами є політичні або законодавчі органи, організації, асоціації тощо.

Умови, в яких живе цільова аудиторія, – це існуючі обставини, які впливають на цільову аудиторію (ЦА), але ЦА має обмежений контроль над ними. Спеціаліст з ПсО визначає проблему і досліджує ці умови: демографічні, політичні, економічні, соціальні, екологічні та інші. Результатом дослідження є документ з детальною характеристикою проблем в різних сферах життєдіяльності цільових аудиторій та ставлення ЦА до існуючих обставин.

Вразливі місця аудиторії – це потреби, які є наслідком умов, в яких живе цільова аудиторія, та які цільова аудиторія прагне задовольнити. Потреби цільової аудиторії класифікуються, зокрема, на фізіологічні, потреби в безпеці, потреби у визнанні та любові, у повазі та самоактуалізації, та визначаються найбільш пріоритетні/нагальні потреби.

Визначення способів переконання передбачає формулювання основного та підтримуючих аргументів та визначення типу звернення до цільової аудиторії і способів (прийомів) подачі аргументів цільовій аудиторії.

Аргумент – це певна ідея, в яку має повірити цільова аудиторія. Дана ідея підкріплюється конкретними фактами і доказами. Для утримання інтересу цільової аудиторії до аргументу використовуються звернення, тобто апеляція до значущих для аудиторії цінностей, подій, потреб тощо. Наприклад, пропагандистські повідомлення можуть апелювати до закону і традицій, до «добрих старих часів» та ін.

Для забезпечення ефективності звернень використовуються різноманітні маніпулятивні прийоми, такі як навішування ярликів, блискучі загальності, спрощення, порівняння і контраст, цитування авторитетних осіб, створення образу ворога і т.д.

Для посилення впливу на цільову аудиторію відбираються символи – візуальні, аудіо або аудіовізуальні засоби, які розпізнаються аудиторією, мають для неї певне значення та здатні донести до аудиторії основні аргументи.

Невід'ємною складовою аналізу цільової аудиторії є визначення каналів комунікації, які найбільш ефективно донесуть пропагандистські повідомлення до цільової аудиторії. Для цього розробники ПсО досліджують, з яких медіа цільова аудиторія отримує інформацію, з якими цілями аудиторія використовує наявні медіа, частоту використання даних медіа тощо [7].

Наступний етап – розробка концепту матеріалів ПсО та плану розповсюдження. Цей етап включає детальний опис пропагандистських матеріалів (в тому числі розмір, кольори, звуки тощо), пояснення символів, які будуть використовуватися та способів їх використання, а також визначення каналів поширення повідомлень, тривалості та частоти появи пропагандистської інформації.

Розроблені пропагандистські матеріали затверджуються вищим військовим або політичним керівництвом. Лише після цього тиражуються і розповсюджуються серед цільових аудиторій.

Що стосується оцінки ефективності ПсО, то основним показником тут є поведінка і ставлення цільової аудиторії. Наявна поведінка цільової аудиторії може співставлятися із сформульованою у плані ПсО бажаною реакцією цільової аудиторії. Проводиться аналіз відхилень від запланованого і оцінюється, наскільки ці відхилення є критичними для успішної реалізації ПсО.

Для оцінки потенційної ефективності пропагандистських матеріалів часто проводиться попереднє тестування, що передує етапу розповсюдження матеріалів ПсО. Тестування реалізується у вигляді анкетних опитувань цільової аудиторії та фокус-груп, які можуть складатися або з представників цільової аудиторії або експертів.

Процес розробки ПсО обов'язково включає прогнозування можливих реакцій супротивника та визначення найбільш ефективних контрпропагандистських заходів.

Психологічні операції реалізуються приблизно за однаковою схемою: визначення або створення інформаційного приводу, розкрутка інформаційного приводу (тобто проведення масштабної пропагандистської кампанії) та закріплення результатів.

Як правило, в якості інформаційного приводу вибирається резонансна подія або факт (необов'язково правдивий), що дозволяє дискредитувати політичне керівництво країни-супротивника як в очах місцевого населення, так і світової спільноти загалом. Відповідно найбільш поширеними пропагандистськими прийомами є створення «образу ворога», навішування ярликів. Крім того, поширеним є використання таких маніпулятивних технік, як спрощення (наприклад, гасло антитерористичної операції - «Хто не з нами, той – проти нас»), контраст і порівняння (наприклад, на негативному фоні США позиціонуються як друг і захисник), посилання на авторитетних осіб, інформаційна блокада, експлуатація сакральних для народу понять/цінностей тощо.

Таким чином, в США розроблена цілісна концепція інформаційної війни. Інформаційна війна розглядається як комплекс інформаційно-технічних та інформаційно-психологічних методів і засобів впливу на супротивника для досягнення поставлених політичних, економічних та військових цілей. Основними об'єктами впливу є психіка осіб, які приймають рішення, військових, цивільного населення, а також інформаційна інфраструктура супротивника. Основою інформаційної війни є, насамперед, широкий спектр технологій маніпулювання масовою свідомістю. Відповідно визначальна роль відводиться психологічним операціям, успішна реалізація яких може призвести до прийняття супротивником потрібних рішень самостійно, без примусу.

Впродовж багатьох років США активно використовують інструментарій інформаційної війни для реалізації своїх інтересів і цілей в різних країнах світу. При цьому в більшості випадків американцям вдавалося досягти поставлених цілей завдяки ретельно продуманим стратегіям, системності, масштабності та різноплановості інформаційно-психологічного впливу.

Враховуючи значний вплив інформаційних операцій США на систему міжнародних відносин, дослідження даної теми є актуальним і перспективним як з точки зору кращого розуміння тих процесів, які відбуваються у глобальному інформаційному просторі, так і вироблення стратегій протидії інформаційним впливам, що становлять загрозу національній безпеці.

Список використаних джерел

1. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. – 2001г. - №1. – С. 2-9.
2. Гриняев С.Н. Поле битвы – киберпространство. – М.: Харвест, 2004. – 446 с.
3. Joint information operations doctrine. Joint Publication 3-13, February 2006 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
4. Полевой устав Армии США FM 33-1. Психологические операции [Электронный ресурс]. – Режим доступа: http://psyfactor.org/lib/fm-33-1.htm.
5. Кудряшов А. Использование за рубежом сети Интернет в интересах ведения информационных войн // Зарубежное военное обозрение. – 2011г. - №4 - С. 11-20.
6. Joint doctrine for public affairs support. Joint Publication 3-61, May 2005 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/doddir/dod/jp3_61.pdf.
7. Psychological Operations Tactics, Techniques, and Procedures. Field Manual No. 3-05.30. - Washington, DC, 2003 [Електронний ресурс]. – Режим доступу: http://www.fas.org /irp/doddir/army/fm3-05-301.pdf.