РОЗДІЛ 6

ОСОБЛИВОСТІ СУЧАСНОГО ПЕРІОДУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

6.1. Глобальне інформаційне протиборство нового типу

У сучасних умовах безперервний розвиток техніки сприяє послідовному підвищенню обсягу і швидкості поширення інформації. Удосконалюються можливості інформаційного охоплення великих територій та мас людей у найкоротші терміни. Разом із позитивними явищами глобальної інформатизації, чіткіше проступають контури нових міжнародних проблем. Передусім це стосується сфери інформаційної безпеки та інформаційного протиборства. Не можна стверджувати, що такі проблеми виникли лише в умовах глобальної інформатизації, але поява єдиного інформаційного простору дозволила перетворити його на ще одне поле протиборства в міжнародних відносинах.

Усе більш очевидною стає залежність політичної влади від можливостей здійснювати інформаційне протиборство у зовнішньо- та внутрішньополітичній сферах. Основні тенденції зміни характеру геополітичної боротьби держав, розвиток процесу глобалізації на початку XXI століття свідчать про те, що разом із традиційними силовими методами та засобами вирішення завдань у цій царині все частіше використовуються інформаційні.

Основним засобом ведення інформаційного протиборства є національні й транснаціональні ЗМІ, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали та ціннісні установки окремої людини, так і на суспільство в цілому.

Теорія інформаційної боротьби під впливом комплексу об'єктивних і суб'єктивних чинників пройшла складний еволюційний шлях: від сприйняття її як допоміжного засобу при вирішенні бойових завдань на тактичному рівні до надання їй глобальної функції управління політичними процесами на стратегічному рівні.

Комплекс заходів, який у XX столітті отримав назву СІО, ще з незапам'ятних часів супроводжував бойові дії. Наприклад, бойове розфарбування первісних воїнів служило як підняттю бойового духу, так і дезорієнтації противника щодо складу протидіючих сил. Воно повинно було створити у ворога уявлення, що він має справу не з армією, а з надприродними, містичними силами. Як відомо, цілеспрямоване дезінформування противника стосовно складу, розташування, чисельності сил суперника досі є одним із найважливіших елементів ведення бою.

Ще в IV ст. до н. е. з'явилась перша фундаментальна праця блискучого китайського стратега й мислителя Сунь-Цзи "Мистецтво війни", в якій було написано: "Засобом, завдяки якому освічені правителі та мудрі полководці виступали і підкоряли інших, а їхні досягнення мали перевагу над багатьма, було попереднє знання. Попереднє знання не можна отримати від демонів та духів, не можна одержати з явищ або небесних знамень; воно має бути отримане від людей, які знають справжній стан противника".

Сунь-Цзи вперше запропонував використовувати інформаційні заходи як альтернативу бойовим діям. Він сформулював дев'ять заповідей, дотримання яких забезпечувало такий потужний вплив на загальний духовний світ армії противника, що вона просто "розкладалася" ще до початку битви. По суті, концепція Сунь-Цзи лежить в основі сучасних АІВ та СІО. Але до того, як відбулося повернення до принципів цього древнього китайського стратега й мислителя, технології інформаційного впливу пройшли довгий шлях розвитку.

Спочатку інформаційні заходи розглядалися як засоби військово-політичної дезорієнтації противника і зводилися до двох основних напрямів:

1) дезінформація щодо власних ресурсів;

2) дії, спрямовані на поразку чи блокування каналів передання даних із метою дезорієнтації й дезорганізації противника (в результаті успішного проведення подібних операцій противник втрачає здатність діяти скоординовано, що значно підвищує його уразливість).

Для виконання зазначених вище завдань (особливо другого напряму) у складі збройних сил країн функціонують війська радіоелектронної боротьби. Вони займаються зашумленням каналів радіозв'язку, перешкоджають роботі засобів радіоелектронної розвідки противника тощо. У наступальних операціях, як відомо, цілями, що підлягають першочерговому знищенню, є вузли зв'язку: телефонні АТС, сервери стільникових операторів і провайдерів інтернетного зв'язку, передавальні комплекси телевізійних і радіомовних станцій. Здебільшого наступу передує пеленгація всіх джерел електромагнітних полів, які можуть використовуватися як засоби зв'язку.

Комплекс описаних вище дій належить до так званого першого покоління інформаційної зброї, або до техногенної сторони інформаційного протистояння. Із часом паралельно розвитку техногенної стала оформлятися гуманітарна сторона. Все більше уваги приділяється необхідності впливу на психологічні характеристики керівництва й особового складу армії противника, а також цивільного населення в тилу.

Із 50-х років XX століття фахівці Пентагону стали розглядати авіаційні нальоти і як психологічну зброю. У роки Корейської кампанії була розроблена концепція, що значно підвищувала результативність бомбових ударів за раху-

нок їх (здавалося б побічного) психологічного ефекту. Хаос і паніка, спричинені бомбовими ударами, вийшли на передній план щодо традиційних завдань із знищення живої сили, військових, промислових чи цивільних об'єктів. Бомбові удари стали розглядатися не як засоби знищення інфраструктури противника, що передують сухопутному вторгненню, а як механізми, за допомогою яких можливо переконати противника припинити опір.

Безумовно, волю противника до опору можна зламати не лише ракетно-бомбовими ударами. Вже в 30-і роки XX століття в Європі бурхливо розвивався відносно новий напрям, названий пропагандою, здійснювалися перші, досить успішні кроки з використання ЗМІ як зброї. На початок Другої світової війни абсолютними лідерами у сфері інформаційних технологій були німці. Німецьким фахівцям удалося організувати внутрішній інформаційний простір таким чином, що зовнішні інфогенні загрози просто розчинялися в ньому. Громадяни Рейху були упевнені в непереможності своєї країни та святості цінностей, на яких вона трималася. Була створена ціла індустрія, що відповідала за зміст інформаційного поля: друкована преса, радіо, кінематограф, студії звукозапису, візуальна реклама тощо. Рейх серйозно опікувався створенням нової культури та засобами її поширення. Німецьке короткохвильове радіо цілеспрямовано працювало із зарубіжними аудиторіями, насаджуючи їм уявлення про Німеччину як найпрогресивнішу й непереможну країну. Варто відмітити, що подальший розвиток аналогічних систем в інших державах був реакцією на активність німців. Німецькі пропагандистські технології перейняли такі країни, як СРСР, США, Велика Британія тощо. На початок "холодної війни" ЗМІ, а особливо радіо як засіб інформаційно-психологічного впливу, використовували практично всі держави, що були втягнуті у протистояння (як лідери, так і сателіти).

Отже, на початок останньої чверті XX століття інформаційно-психологічне протистояння оформилося як комплекс, що складається з техногенного й гуманітарного рівня та забезпечує вирішення таких завдань:

- блокування чи пошкодження каналів управління і зв'язку противника;
- дезінформування противника;
- створення атмосфери напруженості та паніки в тилу противника від постійного очікування ударів;
- вплив на соціальну свідомість противника з метою його деморалізації.

У період, про який іде мова, основою класичного підходу до спеціальних інформаційних операцій були суто лінійні погляди, згідно з якими результат зовнішньої управлінської діяльності є однозначним і лінійним, пропагандистські зусилля відповідають схемі: управляючий вплив – бажаний результат. Тобто, зростання інтенсивності впливу завжди збільшує віддачу. Нацистський міністр пропаганди Й.Геббельс називав це "жорстким утлумаченням". Упродовж XX століття принцип "жорсткого утлумачення" уважався універсальною паради-

гмою ведення інформаційної політики. Проте, починаючи з 80-х років, на Заході вперше відчули, що ефект впливу не завжди прямо пропорційний його інтенсивності.

Криза класичної концепції пропаганди збіглася з новим витком інформатизації, а точніше, стала його результатом. Лінійний підхід до здійснення інформаційних операцій, що передбачає прямий зв'язок між інтенсивністю впливу й результатом, усе менше відповідав новим умовам. Розвиток інформаційних технологій привів до значного збільшення чисельності доступних каналів інформації. Можливість діалогу, що відродилася в комунікативних процесах, стала природним бар'єром сприйняття пропаганди. Навіть найпотужніший пропагандистський імпульс просто згасав у системі, що прискореними темпами розширювалася й розгалужувалася. Зростання кількості каналів передбачало утворення так званих субреальностей. Реципієнт тепер сам вибирав джерело інтерпретації реальності, яке б відповідало його картині світу. Можна констатувати, що інформаційна система стала формуватися за зразком системи суспільної, як ключовий носій суспільної свідомості, або, іншими словами, своєрідна віртуальна проекція самого суспільства. Природно, що в подібних умовах симетричний, лінійний підхід як до вивчення інформації та комунікації, так і до організації інформаційних операцій мав би бути замінений на щось більш відповідне умовам.

У дослідженнях процесу зміни характеру зв'язку між системою ЗМІ та споживачами інформації відбулися суттєві зміни: була здійснена спроба пояснити їх із точки зору синергетичних законів, які в подальшому увійшли до арсеналу фахівців із масових комунікацій як база сучасної інформаційної політики. Суспільство стало розглядатися як надзвичайно складна система, кожен із елементів якої має багато ступенів свободи, інакше кажучи, становить систему, що перебуває в стані постійного вагання перед вибором одного з можливих еволюційних шляхів. На вибір шляху розвитку згідно із сучасними уявленнями може вплинути імпульс навіть мінімального напруження.

З одного боку, нові умови значно ускладнили завдання фахівців з інформаційних операцій, а з іншого – вивели потенційні можливості "інформаційної зброї" на принципово новий рівень. Якщо раніше про інформаційні операції говорилося як про щось супутнє бойовим діям і таке, що має допоміжну функцію щодо традиційної військової сили, то в нових умовах інформаційна стратегія може замінювати традиційні методи.

Є думка, що Україна в її нинішньому стані обійшлася США в 14 млн доларів. Натомість сума, витрачена в Іраку, за даними на 2007 рік перевищила 450 млрд доларів. Слова президента США Ніксона, проголошені в 60-х рр., виявилися пророчими. Він заявив, що вважає один долар, вкладений в інформацію, цінніше, ніж 10 доларів, вкладених у створення систем озброєнь, оскільки останні навряд чи будуть колись застосовані, в той час як інформація працює постійно та

скрізь. Військове вторгнення поступово стає крайнім заходом, уживаним лише тоді, коли фахівці з інформаційних операцій не справляються з поставленими завданнями.

Останнім часом у рамках ініціативи "Інформаційна революція" програми стратегічних оцінок Національної ради з розвідки США аналітичною корпорацією РЕНД (REND Corporation) було проведено низку міжнародних наукових конференцій і семінарів, у процесі яких вивчалися й оцінювалися думки провідних експертів із проблеми трансформації суспільства під впливом інформаційної революції.

Результати виконаної роботи були узагальнені експертами РЕНД у звіті "Глобальний курс інформаційної революції: загальні питання і регіональні відмінності" ("The global course of the information revolution: recurring themes and regional variations", MR-1680-NIC), опублікованому влітку 2003 року.

Основна мета проведеного дослідження – виявити характер впливу інформаційних технологій та інформаційної революції на економічну, фінансову, політичну, культурну, соціальну й інші сфери життєдіяльності сучасного суспільства, а також спрогнозувати розвиток ситуації на найближчі 10–20 років.

У дослідженні наголошується, що сьогодні прогрес в інформаційних технологіях уже торкнувся більшості сфер бізнесу, державної й суспільної діяльності практично в усіх регіонах світу. Інформаційні технології та пов'язана з ними інформаційна революція перетворилися на один із найбільш значущих чинників, які сприяють динамічній трансформації суспільства, його переходу від постіндустріального до інформаційного.

Результати аналізу дали змогу виявити особливості розвитку інформаційних технологій і впливу інформаційної революції, причому як характерні для більшості регіонів світу, так і специфічні, притаманні окремим регіонам планети.

Так, для більшості регіонів світу, які прагнуть використовувати досягнення інформаційної революції, експерти РЕНД визначають такі особливості:

1. Розроблення нових технологій безперервно стимулюватиме інформаційну революцію.

2. Інформаційна революція породить нові бізнес-моделі, які суттєво трансформують діловий і фінансовий світ.

3. Інформаційна революція істотно торкнеться механізмів управління суспільством і створить нових політичних гравців.

4. Інформаційна революція залишиться багатоликою й формуватиметься соціальними та культурними цінностями.

5. Збережеться багатофакторна форма і характеристика національного підходу до сприйняття інформаційної революції.

Крім того, експерти РЕНД прогнозують такі основні тенденції розвитку геополітичної обстановки у світі:

1. Найближчі 10–20 років США залишаться в авангарді інформаційної революції.

2. Інформаційна революція в Європі розвиватиметься повільніше та іншим шляхом, ніж у США й Канаді.

3. У найближчі 10–20 років низка країн Азіатсько-тихоокеанського регіону продовжуватимуть стрімкий розвиток і масштабне використання інформаційних технологій.

4. Геополітичні тенденції, яким сприяє інформаційна революція, можуть відзначити нові виклики національній безпеці Сполучених Штатів й інших розвинутих країн світу.

Оскільки темпи зазначених технологічних революцій, а також їх синергетичний вплив збільшуються, зростає й розуміння наслідків їхнього впливу на суспільство майбутнього. Експерти РЕНД констатують, що в процесі указаних технологічних революцій збережеться нерівність окремих націй і регіонів планети; більше того, прискорення темпів технологічної революції призведе до поглиблення нерівності і, як наслідок, – до небувалого зростання напруження у всьому світі.

Нині, на думку американських фахівців, інформаційне протиборство є не просто видом забезпечення операцій збройних сил шляхом порушення процесів контролю та управління військами, але й виходить далеко за межі цих проблем. Про це говорять основні результати досліджень, проведених фахівцями американської корпорації РЕНД у кінці 90-х років. У цьому дослідженні вперше застосовано термін “стратегічне інформаційне протиборство”. Таке протиборство згідно із заявами авторів звіту є використанням державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій і зменшення впливу на власний інформаційний ресурс. Ці дослідження дозволили виділити ключові особливості такого виду протиборства: відносно низька вартість створення засобів інформаційного протистояння і крах статусу традиційних державних кордонів при підготовці й проведенні інформаційних операцій.

Подальше вивчення проблеми привело до уведення поняття “стратегічного інформаційного протиборства другого покоління”. У звіті воно визначене як принципово новий тип стратегічного протиборства, породжений інформаційною революцією, що уводить інформаційний простір до кола можливих сфер протиборства. Наголошується, що розвиток і вдосконалення підходів до ведення стратегічного інформаційного протистояння другого покоління в перспективі може привести до повної відмови від використання військової сили. По суті, інформаційне протиборство другого покоління зводиться до зусиль із видозміни противника: до знищення його традиційного змісту та наповнення новим. Тобто, йдеться не про навіювання певних уявлень окремим людям чи групам, а про

формування повноцінного суспільного світогляду, що має здатність до саморозвитку в потрібному напрямі.

Із початку 70-х і до кінця 90-х років XX ст. абсолютними лідерами у сфері інформаційного протистояння були американці. Вони, здавалося, успішно впоралися із завданням інтенсифікації використання глобального інформаційного ресурсу та блокування своїх ресурсів для інших країн. У результаті у 2003 році, за підрахунками китайських фахівців, потік інформації з країн розвинутих у ті, що розвиваються, становив 80% усього інформаційного обміну між ними.

Нині США активізують проведення робіт, направлених на реалізацію національної інформаційної стратегії з метою забезпечити інформаційну перевагу шляхом нав'язування інформації, що спонукала б вище військово-політичне керівництво інших країн приймати вигідні для США рішення. Ключовими елементами у справі досягнення цілей національної інформаційної стратегії є управління сприйняттям цільової аудиторії та формування "громадської думки" шляхом маніпулювання інформацією.

Цілі національної політики США досягатимуться шляхом ведення стратегічного інформаційного протиборства з використанням атакуючої інформаційної зброї. Останнім часом усе частіше розглядаються не апаратно-програмні засоби впливу на інформаційні системи й інформаційний ресурс противника, а засоби та методи маніпулювання інформацією. Про це говорить аналіз напрацювань із зазначеної тематики – в зарубіжній пресі останнім часом зросла чисельність робіт із розроблення засобів і методів маніпулювання свідомістю (зокрема нейролінгвістичного програмування, гіпнозу й інших сугестивних методів), дослідженнях психології особистості тощо. З'явилася низка нових понять, наприклад "реальна віртуальність", коли освітлення певної події в пресі стає важливішим, ніж сама ця подія.

У процесі наукових досліджень за такими програмами, як "МК-ультра", "Артишок" тощо, проведеними ще в 60-70 роках, установлено, що найбільш перспективними методами ведення інформаційної війни є саме методи впливу на індивідуальну, групову та суспільну свідомість. Реалізація подібних методів на державному рівні потребує перегляду ключових підходів до проведення зовнішньої й внутрішньої політики держави в інформаційну епоху.

Основними силами, задіяними в сучасному стратегічному інформаційному протиборстві, будуть невеликі групи висококласних політтехнологів, спічрайтерів та іміджмейкерів, що створюють і обігрують заданий сценарій. Робота таких фахівців сьогодні називається "зв'язками з громадськістю" (public relation, PR). Така група фахівців на чолі з Джиммі Шеа освітлювала конфлікт у Югославії. Саме в Югославії був апробований у повному обсязі весь цикл заходів щодо стратегічного інформаційного протиборства: від дискредитації політичного керівництва перед початком конфлікту до вигідного висвітлення подій збройної агресії.

Варто зазначити, що багато в чому процеси глобалізації об'єктивні й викликані рівнем науково-технічного прогресу; відмовитися від передових досягнень сьогодні просто неможливо. США та інші розвинуті країни одними з перших усвідомили переваги, які дає глобалізація, та спробували збудувати модель нового глобального суспільства відповідно до власних, багато в чому егоїстичних, інтересів. Проте уразливість цієї ідеї очевидна: стабільне глобальне суспільство може бути побудоване лише на основі мережевої, а не ієрархічної структури, в якій кожен вузол буде рівноправним у своїх відносинах. За цих умов однією з нагальних проблем постає вироблення нових ідей подальшого позитивного розвитку глобального суспільства.

6.2. Інформаційна зброя в сучасних умовах

Третє тисячоліття відзначається стрімким глобальним розвитком комп'ютерних інформаційних технологій, засобів електронної телекомунікації, масовим упровадженням їх у всі сфери суспільної діяльності. Швидкі темпи розвитку комп'ютеризації та інформатизації суспільства неминуче ведуть до створення єдиного світового інформаційного простору, в якому акумулюються всі засоби збирання, накопичення, оброблення, обміну та зберігання інформації.

Інформаційний простір фактично стає театром воєнних дій, де кожна протиборча сторона прагне отримати перевагу, а в разі потреби розгромити противника. Розмах протиборства в інформаційній сфері досяг таких масштабів, що викликало необхідність створення спеціальної концепції, яка отримала назву "інформаційної війни" або "інформаційного протиборства".

Уперше роботи із створення концепції "інформаційної війни" почалися в США на початку 90-х років. Нині є декілька варіантів трактувань терміна "інформаційна війна". Відмінності між ними незначні, тому з повною підставою можна використовувати варіант, представлений у Статуті Сухопутних військ США FM 100-6 "Інформаційні операції" (серпень, 1996 року). Згідно з цим документом "інформаційна війна – це комплекс заходів щодо досягнення інформаційної переваги шляхом впливу на інформацію, інформаційні процеси, інформаційні системи та комп'ютерні мережі противника при одночасному захисті своєї інформації, інформаційних процесів, інформаційних систем і комп'ютерних мереж".

У рамках інформаційної війни проводяться заходи наступального й оборонного характеру. Відповідно удосконалюються наявні та активно розробляються нові оборонні й наступальні засоби ведення інформаційного протиборства, які дозволять досягти інформаційної переваги над противником. Засобом ведення інформаційної війни чи протиборства є інформаційна зброя.

Щоб з'ясувати, чи має поняття "інформаційна зброя" право на існування, варто передусім звернутися до визначення зброї. У "Радянській військовій енциклопедії" зброя тлумачиться як "пристрої й засоби, вживані в збройній боротьбі для поразки та знищення противника". Основним у визначенні зброї убачається мета її використання – поразка противника. Під поразкою об'єктів (цілей) мається на увазі дія різними засобами на об'єкти (цілі), в результаті якої вони повністю або частково (тимчасово) втрачають здатність до нормального функціонування (виконання бойового завдання). Поразка об'єктів полягає в їх знищенні (руйнуванні), придушенні та виснаженні (живої сили об'єктів).

Знищення об'єкта передбачає завдання йому такого збитку, при якому він повністю втрачає боєздатність.

Придушення означає завдання об'єкту такого збитку (пошкоджень) і створення для нього таких умов, при яких він тимчасово позбавляється боєздатності, обмежується (забороняється) його маневр або порушується управління.

Виснаження полягає в тривалому веденні по об'єкту вогню обмеженою кількістю сил і засобів або завдаванні по ньому періодичних ударів авіації. Основною його метою є морально-психологічний вплив на живу силу об'єкта й тим самим зниження його боєздатності та нормального функціонування.

Отже, чи здатна так звана інформаційна зброя уражувати противника?

Інформаційна зброя, за одним із наявних визначень, – це комплекс програмних і технічних засобів, призначених для контролю інформаційних ресурсів об'єкта впливу та втручання в роботу його інформаційних систем.

Інформаційну зброю можливо класифікувати за методами впливу на інформацію, інформаційні процеси та інформаційні системи противника. Цей вплив може бути *фізичним, інформаційним, програмно-технічним* або *радіоелектронним*.

Фізичний вплив може бути здійснений шляхом застосування будь-яких засобів вогневої поразки. Проте більш коректним було б віднести до інформаційної зброї фізичного впливу засоби, призначені виключно для впливу на елементи інформаційної системи: протирадіолокаційні ракети, спеціалізовані акумуляторні батареї генерування імпульсів високої напруги, засоби генерування електромагнітного імпульсу, графітові бомби, біологічні й хімічні засоби впливу на елементну базу.

За допомогою протирадіолокаційних ракет у перші дні повітряної операції коаліційних миротворчих сил у зоні Перської затоки (1991 р.) було виведено з ладу 80% наземних РЛС Іраку.

Ефективним також є використання генераторів електромагнітного випромінювання. Проведені експерименти показали, що прості малогабаритні генератори на відстані до 500 м можуть унести небезпечні пошкодження в роботу приладів літака, що здійснює зліт або посадку, а також заглушити двигуни сучасних автомобілів, оснащених мікропроцесорною технікою.

Графітові бомби застосовувалися американськими збройними силами в ході війни в Перській затоці та Косово. Їх уражуючий ефект досягається шляхом створення над об'єктом хмари площею до 200 $м^2$ із вироблених на основі вуглецю тонких надпровідних волокон. При зіткненні волокон із струмопровідними елементами (ізолятори, дроти тощо) відбувалося коротке замикання та виведення з ладу електромереж.

Біологічні засоби – особливі види мікробів, здатні знищувати електронні схеми та ізоляційні матеріали, що використовуються в радіоелектронній техніці.

Інформаційні методи впливу реалізуються за допомогою всієї сукупності засобів масової інформації та глобальних інформаційних мереж типу Інтернету, станцій голосової дезінформації.

Оскільки основним елементом інформаційної інфраструктури є люди, мотивація діяльності яких базується на їхніх фізіологічних, соціальних та інформаційних потребах, то правильно розраховане використання так званих інформаційно-психологічних методів впливу здійснює прямий вплив на рівень безпеки держави. Науково-технічний прогрес у галузі інформаційних технологій, розвиток ЗМІ стерли національні кордони в інформаційному просторі та створили безпрецедентні можливості для придушення противника за допомогою нетрадиційних засобів поразки, що не викликають фізичних руйнувань. Проходячи через свідомість кожного члена суспільства, тривалий масований інформаційно-психологічний вплив руйнівного характеру створює реальну загрозу існуванню нації в результаті трансформації її культури, що історично склалася, основних світоглядних та ідеологічних установок.

Наявні факти, що засоби масової інформації, прикриваючись гаслами "об'єктивності інформаційного висвітлення" тих чи інших подій, завдають збитку інформаційній безпеці країни шляхом маніпулювання інформацією, поширення дезінформації, інформаційної підтримки певних екстремістських та кримінальних угруповань. І ця проблема може посилюватися за рахунок як монополізації вітчизняних ЗМІ, так і неконтрольованого розширення сектору зарубіжних ЗМІ в інформаційному просторі країни.

Станції *голосової дезінформації*, що розробляються нині в США, дозволять входити в радіомережі об'єкта впливу та змодельованим комп'ютерними засобами голосом командира підрозділу (частини) противника віддавати накази й розпорядження підлеглим військам, тим самим порушуючи управління ними.

Засобами реалізації *програмно-технічних методів* є комп'ютерні віруси, логічні бомби та апаратні закладки, а також спеціальні засоби проникнення в інформаційні мережі. Ці засоби використовуються для збирання, зміни та руйнування інформації, що зберігається в базах даних, а також для порушення чи уповільнення виконання різних функцій інформаційно-обчислювальних систем.

Програмно-технічні засоби можна класифікувати відповідно до виконуваних

із їхньою допомогою завдань на *засоби збирання інформації, засоби спотворення і знищення інформації та засоби впливу на функціонування інформаційних систем.* Причому деякі засоби можуть бути універсальними й використовуватися як для спотворення (знищення) інформації, так і для впливу на функціонування інформаційних систем об'єкта впливу.

Засоби збирання інформації дозволяють здійснювати несанкціонований доступ до комп'ютерних систем, визначати коди доступу, ключі до шифрів або іншу інформацію про зашифровані дані та каналами обміну передавати отримані відомості зацікавленим організаціям.

На сьогодні розроблені спеціальні програмні продукти, так звані "ноуботи" (Knowbot – Knowledge Robot), які здатні переміщатися в інформаційній мережі від комп'ютера до комп'ютера й при цьому розмножуватися, створюючи копії. "Ноубот" уводиться в комп'ютерні системи та, виявивши інформацію, що його цікавить, залишає в цьому місці свою копію, яка збирає і в певний час передає ці відомості. З метою унеможливлення виявлення в "ноуботі" можуть бути передбачені функції самопереміщення і самознищення.

Завдання збирання інформації вирішуються і за допомогою програмних продуктів "Демон" (Demon), "Винюхувачі" (Sniffers), "Двері-пастка" (Trap Door). Програмний продукт "Демон", уведений у систему, записує всі виконувані команди та в певний час передає інформацію про ці команди. Аналогічно діють і "Винюхувачі", які прочитують та передають перші 128 бітів інформації, необхідних для входу в систему. Програми використовуються для викриття кодів доступу й шифрів. "Двері-пастка" дозволяють здійснювати несанкціонований доступ до інформаційних масивів бази даних в обхід коду захисту. При цьому система та елементи захисту їх не розпізнають.

Створені й постійно модернізуються спеціальні технічні пристрої, що дозволяють прочитувати інформацію з моніторів комп'ютерів. Перспективним є також створення мініатюрних спеціалізованих комплексів збирання, оброблення й передання інформації, які можуть упроваджуватися до різних радіоелектронних пристроїв під виглядом звичайних мікросхем.

Засоби спотворення і знищення інформації включають програмні продукти "Троянський кінь" (Trojan Horse), "Хробак" (Worm), а також численні комп'ютерні віруси, кількість яких перевищує 60 тисяч.

"Троянський кінь" дозволяє здійснити прихований несанкціонований доступ до інформаційних масивів. Він активується по команді й використовується для зміни чи руйнування інформації, а також уповільнення виконання різних функцій системи.

"Хробак" – це сторонній файл, сформований усередині інформаційної бази даних системи. Він здатний змінювати робочі файли, зменшувати ресурси пам'яті, а також переміщувати й змінювати певну інформацію.

До *засобів впливу на функціонування інформаційних систем* відносять "Логічні бомби", "Бомби електронної пошти" тощо.

Логічна бомба є інструкцією, що перебуває в неактивному стані до отримання команди про виконання певних дій на зміну або руйнування даних, а також порушення працездатності інформаційно-обчислювальних систем. Так, під час війни в Перській затоці Ірак не зміг застосувати проти багатонаціональних сил куплені у Франції системи ППО, оскільки їхнє програмне забезпечення містило логічні бомби, активізовані з початком бойових дій.

Бомби електронної пошти – це великий обсяг несанкціонованих повідомлень, використовуваний із метою збільшення навантаження на сервер, аби він став недоступним або його ресурси недостатніми для нормальної роботи. Саме таким чином був заблокований у березні 1999 року на три доби сервер НАТО. Невідомий адресат регулярно присилав на адресу Північноатлантичного блоку близько 2 тис. телеграм на день, які переповнили електронну "поштову скриньку".

Радіоелектронні методи впливу передбачають використання засобів радіоелектронного придушення, радіоелектронної розвідки та деяких інших. Основним призначенням такої зброї є контроль інформаційних ресурсів потенційного противника й приховане або явне втручання в роботу його систем управління і зв'язку з метою дезорганізації, порушення нормального функціонування чи виведення їх із ладу як у мирний, так і воєнний час, при самостійному впливі чи в поєднанні з іншими засобами впливу на противника.

Що стосується засобів масової інформації, то використання їх із метою здійснення активного ІПсВ може знизити або навіть позбавити особовий склад противника на певний період боєздатності, змусивши його ухилятися різними шляхами від участі в бойових діях. У цьому випадку ЗМІ виступають як засіб придушення, тобто належать до зброї.

Програмно-технічні та радіоелектронні засоби збирання інформації не потрапляють під класичне визначення зброї, оскільки вони не беруть участь у безпосередній поразці противника, а лише забезпечують умови для ефективного ведення збройного, зокрема інформаційного, протиборства. Але якщо узяти за основу сформульоване вище визначення інформаційної зброї, то засоби збирання інформації, поза сумнівом, забезпечують контроль над інформаційними ресурсами противника та можуть бути зараховані до цього виду зброї.

Основними способами й методами застосування інформаційної зброї можуть бути:

- завдання збитку фізичним елементам інформаційної інфраструктури (руйнування мереж електроживлення, створення перешкод, використання спеціальних програм, які стимулюють виведення з ладу апаратних засобів, а також біологічних і хімічних засобів руйнування елементної бази);
- знищення чи пошкодження інформаційних, програмних і технічних ре-

сурсів противника, подолання систем захисту, впровадження вірусів, програмних закладень і логічних бомб;

- вплив на програмне забезпечення та бази даних інформаційних систем і систем управління з метою їх спотворення чи модифікації;
- загроза або здійснення терористичних актів в інформаційному просторі (розкриття та загроза обнародування чи обнародування конфіденційної інформації про елементи національної інформаційної інфраструктури, суспільно значущі й військові коди шифрування, принципи роботи систем шифрування, успішний досвід ведення інформаційного тероризму тощо);
- захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації сили та доведення до відома своїх вимог;
- знищення й придушення ліній зв'язку, штучне перевантаження вузлів комутації;
- вплив на операторів інформаційних і телекомунікаційних систем із використанням мультимедійних та програмних засобів для уведення інформації в підсвідомість або погіршення здоров'я людини;
- вплив на комп'ютерне устаткування бойової техніки та озброєння з метою виведення їх із ладу.

Отже, формування єдиного глобального інформаційного простору, що є природним результатом розвитку світової науково-технічної думки та удосконалення комп'ютерних й інформаційних технологій, створює передумови для розроблення та застосування інформаційної зброї. Володіння ефективною інформаційною зброєю й засобами захисту від неї стає однією з головних умов забезпечення національної безпеки держав у XXI столітті.

Сучасні процеси глобалізації якісно змінили зміст і форми ведення інформаційних воєн. Глобалізація подвійно вплинула на характер сучасних конфліктів та війн: по-перше, спричинила ерозію державної влади та соціальну уразливість, по-друге, створила нові можливості й економічні заохочення, що виникають під час громадянської війни.

З урахуванням цього, інформаційну війну можна визначити як комплекс заходів інформаційного забезпечення, інформаційної протидії та інформаційного захисту, які проводять за єдиним задумом і планом із метою захоплення та утримання інформаційної переваги над противником. Поширення інформаційних воєн пояснюється можливістю забезпечення досягнення політичних цілей завдяки проведенню глобальних (стратегічних) психологічних операцій для формування відповідної вигідної системи поглядів, психологічного оброблення населення країни та суміжних держав.

Класичний приклад застосування інформаційної зброї. Під час Другої світової війни Японія здійснила комплекс заходів із формування як серед військовослужбовців, так і усього японського народу культу "камікадзе". Не маючи

військової переваги над американцями, відтягуючи неминучу поразку, японці намагалися залякати противника атаками смертників. У результаті владні структури Японії досягли успіху в психологічній боротьбі – утримали свій статус у суспільстві.

Поширення інформаційних воєн пояснюється неможливістю в сучасних умовах ведення фронтальних агресивних бойових дій, застосування зброї масового ураження. Тому інформаційні війни забезпечують досягнення політичних цілей завдяки проведенню глобальних (стратегічних) психологічних операцій для формування позитивного ставлення міжнародної спільноти до таких дій; завдяки психологічному обробленню регіону конфлікту, а саме військовослужбовців та населення противника й суміжних держав. Психологічно обробляються і власні війська з метою підняття бойового духу, а також формування в них образу визволителів, носіїв демократичних цінностей тощо.

На початку XXI століття найбільшого значення в інформаційній війні набула іміджева складова, яка передбачає негативний вплив на репутацію противника, що згодом має привести до його ігнорування та дискредитації перед світовим співтовариством. Останнє десятиріччя засвідчило феноменальне зростання можливостей інформаційних технологій. Але тільки зараз це питання починає поставати як одне з головних у боротьбі за світовий інформаційний простір. Інформаційні технології не могли не вплинути на таку сферу міжнародних відносин, як інформаційне протистояння, створивши якісно новий рівень ведення інформаційних воєн.

Саме в цьому напрямі діяли США в ході війни Грузії проти Росії у серпні 2008 року або інформаційного протиборства Росії та України під час "затримання" Україною транзиту газу до Європи в грудні 2008 року.

Ведення інформаційно-іміджевої війни спотворює реальність у масовій суспільній свідомості, а її результат може суттєво відрізнятися від підсумків збройного конфлікту, більше того, виявитися важливішим за них. Тут доречно згадати один із постулатів поведінкової соціології: "Якщо ситуація визначається як реальна, то вона реальна за своїми наслідками".

Інформаційна, тобто нематеріальна, перемога має цілком відчутні матеріальні результати. Так, унаслідок війни в Південній Осетії Росія відчула відтік іноземного капіталу, стрімко загострилися загрози розміщення американської ПРО на території Польщі. Щодо наслідків антиукраїнської "газової" інформаційної кампанії варто зазначити, що, окрім підписання "нового" газового контракту, який важко визнати таким, що відповідає національним інтересам, наша держава зазнала серйозних утруднень у політико-дипломатичних відносинах із європейськими країнами.

Сучасна інформаційна війна проявляється в тенденційному висвітленні певних подій, широкому застосуванні дезінформації, інформаційного шантажу з

використанням результатів електронного контролю за життям людей, їхньою політичною діяльністю й особистими планами; використанні усього потенціалу сучасних ЗМІ з метою отримання односторонніх переваг.

Розглядаючи тенденції глобального інформаційного суспільства, неможливо не згадати явище, що змінює наявну систему сучасних міжнародних відносин. Ідеться про міжнародний кібертероризм, який за допомогою сучасних телекомунікацій продукує "терористичну свідомість", надає можливість терористичним групам завдяки мас-медіа маніпулювати масовою свідомістю. Медіа-інформаційний тероризм став різновидом інформаційного тероризму. Через інтернет тероризм пропагує свої ідеї у світовому масштабі. Дослідження свідчать, що значення всесвітнього терористичного середовища посилюється. При цьому інтернетний тероризм є високо динамічним: сайти швидко з'являються та зникають, змінюють свої назви, доменні імена, однак залишають зміст посилань і статей на сторінках кібервидань. Їхня мета – вплинути на думки, поведінку, свідомість або посіяти страх, паніку, деморалізувати суспільство; викликати почуття провини за дії своєї влади, спричинити громадянське протистояння, розв'язати дискусії на тему тероризму.

Більшість розвинутих країн володіє потужним інформаційним потенціалом, який за певних умов забезпечить будь-якій із них досягнення своїх політичних цілей, до того ж на сьогодні відсутні міжнародні юридичні норми ведення інформаційної боротьби. Моніторинг публікацій у ЗМІ переконливо засвідчує, що головна тенденція інформаційної боротьби полягає в підвищенні її ролі в розв'язанні зовнішньополітичних завдань. Удосконалення нетрадиційних засобів на сучасному етапі науково-технічної революції призвело до виникнення зброї глобального ураження, системне застосування якої здатне знищити середовище існування людства.

Використання інформаційних засобів і систем збільшує можливості державного впливу. Разом із тим зростає уразливість систем управління від цілеспрямованого впливу в інформаційній сфері. Ці тенденції об'єктивно приводять до розширення арсеналу методів і засобів інформаційної боротьби, посилення її впливу на хід і результат воєнних дій, зростання кількості застосовуваних у ній сил і засобів.

На сучасному етапі історичного розвитку домінує тенденція розв'язання зовнішньополітичних конфліктів без збройного насильства. Інформаційна війна перестала бути другорядним чинником, доповненням до "основних" подій. Вона перетворилася на один із найважливіших механізмів ведення війни, про який говорять нарівні з використанням збройних сил і техніки. Інформаційна війна в сучасному світі стала легітимним засобом політичної боротьби.

Незважаючи на те, що значна частина суспільства усвідомлює процес цілеспрямованої інформаційної атаки на противника та допускає можливість вико-

ристання “брудних” технологій, вона все одно піддається маніпулюванню з боку ЗМІ. У результаті в комунікативному протистоянні перемагає не той, хто говорить правду, а той, кому вдалося показати глядачам більш захоплюючий “інформаційний серіал” і гранично чітко обґрунтувати свою позицію. Тобто, чим більшими інформаційними можливостями володітиме країна, тим імовірніша можливість досягнення стратегічних переваг у майбутній системі міжнародних відносин.

Інформаційні війни стали аксіомою сучасних міжнародних відносин і дають змогу досить ефективно, із залученням незначних фінансових та людських ресурсів, досягати потрібних цілей: все залежить від ступеня професіоналізму реалізаторів інформаційних операцій. Відстоювати свої позиції в інформаційному протиборстві буде набагато легше тим країнам, які матимуть гармонійно розвинуте й тому захищене інформаційне суспільство.

Проблеми, що постали у зв’язку з переходом до інформаційного суспільства, ще більше загострюють необхідність осмислення закономірностей, особливостей та наслідків розроблення і впровадження нових засобів масової інформації та комунікації. З огляду на новизну, складність і певну унікальність проблематики, досі немає достатньо диференційованих наукових досліджень щодо сутності інформаційного протиборства, методичних засад вивчення напрацювань у цьому напрямі.

Тому питання просування та закріплення національних інтересів за межами власної держави має неабияке науково-прикладне значення, насамперед стосовно дослідження механізмів державного управління та розроблення науково обґрунтованої стратегії й тактики забезпечення національної інформаційної безпеки.

6.3. Особливості забезпечення інформаційної безпеки в епоху глобалізації

Зміну світогляду на рубежі третього тисячоліття зумовила революція у сфері комунікацій та інформації. Масова комп’ютеризація, упровадження та розвиток новітніх інформаційних технологій привели до вражаючого прориву в освіті, бізнесі, промисловому виробництві й наукових дослідженнях.

До недавнього часу як у теорії, так і на практиці забезпечення державної безпеки основна увага приділялася військовій складовій. Сьогодні стала очевидною обмеженість цього підходу, оскільки науково-технічна революція привела до створення інформаційного суспільства, в якому інформація є головним фактором управління сучасним світом та основним інструментом влади.

Глобальні соціальні зміни, події у світі в кінці XX ст. потребують об’єктивного аналізу інформаційного середовища світової спільноти. До цього проблема забезпечення інформаційної безпеки в нашій державі не лише не розглядалася, але й фактично ігнорувалася. При цьому уважалося за можливе її ви-