

УДК 316.485.26:[07:004.77



Оксана Сенченко,
аспірант кафедри видавничої справи
та редагування НТУУ "КПІ ім. Ігоря Сікорського"

Мережевий інструментарій нових війн

Інформаційно-мережеві війни (ІМВ) — нова військова розробка Пентагону, яка дає можливість отримати перемогу над супротивником без застосування традиційної зброї. І це не війна в мережі Інтернет, попри те, що вона також є інструментом інформаційно-мережевого протистояння. Середовищем для ведення ІМВ є сучасне інформаційне суспільство.

Ключові слова: інформаційно-мережеві війни, мережі, мережеві війни, соціальні структури, інформаційні коди, операції базового ефекту, безкомандний опір.

1. Вступ

"Холодна війна" дала поштовх для розробки стратегії й тактики латентних війн, що мають різні назви: гуманні, організаційні, інформаційні, мережеві, інформаційно-психологічні, концепційні та інформаційно-мережеві.

Після закінчення "холодної війни" між Заходом і Радянським Союзом перемогу насправді святкувала американська панівна еліта, що згодом висунула концепцію безумовного глобального панування й однополюсного світу Pax Americana. А влітку 2014 року Барак Обама, не зважаючи на досвід реалізації цієї теорії, по суті, підтвердив її право на існування тезою про американську винятковість [1].

У сфері ведення нових війн реалізацію доктрини глобального панування мав забезпечувати інструментарій "мережецентричних війн", "м'якої сили", технології "керованого хаосу", а для жорсткого політичного протистояння були передбачені ще й засоби "кольорових революцій".

Майже 400 найпотужніших мозкових центрів США ведуть роботу з аналізу стану й моделювання ситуації в різних країнах світу, зокрема і в Україні. Фахівці цих структур використовують базові дані, що збирають численні "незалежні" організації, враховують економічну ситуацію, фінансують екстремістські структури, під прапором демократії використовують людей, які вболівають за країну й організують революції [2].

У середині 1990-х років група співробітників корпорації "РЕНД" під керівництвом Дж. Аркілли і Д. Ронфельда розробила концепцію ведення мережевих війн. Власне бачення ІМВ вони виклали у статті "Пришестя мережевої війни" [3]. Прибічниками і політичними лобістами нової теорії були Д. Рамсфельд, П. Вулфовіц і ряд інших фігур з-поміж американських неоконсерваторів.

До розробки теми долучився Пентагон, внаслідок чого було створено Департамент трансформації військ (Office of Force Transformation), відповідальний за реформування збройних сил США згідно з принципами теорії ведення "мережевих війн". Саме таку назву отримала концепція ведення війн з використанням різних типів мереж.

Основні положення нової доктрини було сформульовано у двохсотсторінковій доповіді Міністерства оборони США під назвою "Мережецентричне військове мистецтво" від 27 липня 2001 року [4]. Напрями подальшого розвитку мережевих війн визначено у роботі "Реалізація мереже-

центричного військового мистецтва", виданій Департаментом трансформації військ 2005 року, а також у низці спільних монографій американських воєначальників і експертів [5].

У чому полягає відмінність між мережецентричними і мережевими війнами?

Мережецентричні бойові дії (Net-Centric Warfare) — це суто військова концепція, що пройшла тривалий шлях від інтелектуальних розробок і мозкових штурмів через експерименти до практичних дій, які вплинули на зміну інфраструктури Пентагону і військової стратегії США [5].

Мережева війна (Netwar) — ширший феномен, пов'язаний з особливостями і викликами інформаційної ери та глобалізації. Цей інструмент використовується не тільки у традиційній військовій сфері, а й для впливу на широкі верстви населення на когнітивному рівні [6].

Головна мета інформаційно-мережевої війни — "це захоплення території, встановлення над нею контролю без використання класичної зброї і, якщо це можливо, без прямої воєнної агресії" [7].

2. Становлення суспільства мережевих структур

Особливість ведення нових війн є використання соціальних мереж, не інтернет-мереж, а мереж реального суспільства, колективів, груп, рухів, організацій для формування необхідного контексту. Соціум потрібно підготувати — створити такий контекст, що допоможе виробити позитивне ставлення до радикальних соціальних і політичних трансформацій. У такому стані суспільство легко сприймає нові ідеї, інші стратегічні моделі, чужу логіку, а отже його можна вважати завойованим. Подібні війни ведуть як проти ворогів, так і проти союзників чи нейтральних сил, формуючи їхню поведінку. Важливою складовою ІМВ є мережа, її структура, типи і призначення.

Поняття мережі потребує пояснення. Мережа, якою транслюється будь-яка інформація — побутова, суспільно-політична, енергетична, військово-стратегічна тощо, — із суто технічного засобу поступово перетворюється на головну життєву артерію сучасного соціуму. "Мережею є будь-яке середовище, через яке можна передати, отримати, а загалом — прокачати потрібну інформацію, активуючи мережу, змусивши її працювати. Якісною, правильною налагодженою мережею є та, що відтворює "потрібну", передбачувану або принаймні передбачену дію, вписану в загальну стратегію.

Контентом наповнення мережі є інформація, виокремлена із загального інформаційного потоку за допомогою певного мережевого коду. При цьому він може бути чинним, тобто розробленим у процесі створення мережі, і сформованим, тобто штучно привнесеним у наявну мережу. Сформований мережевий код є свого роду перепрошивкою мережі" [7].

Мережевими структурами є фонди, засоби зв'язку, мас-медіа, транснаціональні корпорації, банківські структури, громадські, релігійні, неурядові й некомерційні організації, політичні осередки, спецслужби різних держав, редакцій газет і журналів — як великих, так і аматорських мережевих видань або блогів, котрі певним чином ангажує одна зі сторін конфлікту. Це можуть бути асоціації чи клуби мисливців, філателістів або збирачів антикваріату, що мають зв'язок з іншими подібними клубами в різних точках планети, члени яких періодично з'їжджаються на загальні збори або форуми. Нарешті, мережа — це невеликі терористські групи, що підтримують контакти через Інтернет або за допомогою мобільного чи супутникового зв'язку, об'єднані загальними світоглядними установками і цілями. Мережі поступово інтегруються у загальну надзвичайно гнучку і різномірну структуру, в якій у взаємозв'язок вступають елементи, які ніколи раніше не стикалися.

Мережа — це середовище, через яке можна пропустити певний сигнал, що буде сприйнятливим, переданий далі та втілений у життя. Мережа може бути створена і може бути налагоджена певним чином. Вона може бути змінена, а може бути використана в початковому вигляді з первісними параметрами. Отже, мережа — це все, що має контакт між собою, але не має ієрархії. При цьому ієрархічні структури також можуть входити до мережі як окремі вузли.

Кількість учасників мережі та її обсяг не є запорукою якості. Зрештою, будь-який контакт між двома людьми, що передали певну інформацію один одному, — це проста модель мережі, що зароджується. Чиновник у Києві, який працює в держструктурі та передає одного разу електронною поштою інформацію для репортера в Берлін, навіть якщо вони незнайомі, — це зародки мережі. А повторний контакт — це вже діюча мережа, яку можна застосувати у поточній мережевій операції. Інакше кажучи, інформаційне суспільство є ідеальним середовищем для створення, функціонування і використання мереж, що нині діють усюди, і це не метафора, а об'єктивна реальність сучасного суспільства.

"Саме мережі становлять нову соціальну морфологію наших суспільств, а поширення "мережевої" логіки значною мірою позначається на ході та результатах процесів, пов'язаних із виробництвом, повсякденним життям, культурою і владою. Так, мережева форма соціальної організації була й раніше, і в інших місцях, проте парадигма нової інформаційної технології забезпечує матеріальну основу для всебічного проникнення такої форми у структуру суспільства. До того ж подібна мережева логіка спричиняє появу соціальної детермінанти вищого рівня, ніж конкретні інтереси, що знаходять втілення у формуванні подібних мереж: влада структури виявляється сильніше за структуру влади.

Належність до певної мережі або брак такої разом із динамікою одних мереж щодо інших є найважливішими джерелами влади і змін в нашому суспільстві; отже, можемо визначити його як суспільство мережевих структур (network society), характерною ознакою якого є панування соціальної морфології над соціальною дією", — зауважує американський соціолог М. Кастельс у роботі "Становлення суспільства мережевих структур" [8].

Учений описує мережеву структуру як комплекс взаємопов'язаних вузлів, зміст яких залежить від характеру конкретної структури мережі. Такі структури надзвичайно різноманітні — це банки, ринки цінних паперів, кримінальні угруповання, політичні осередки держав, телевізійні канали тощо. При цьому структури є відкритими і можуть розширюватися завдяки залученню нових вузлів, якщо ті відповідають коду комунікації (тобто їхні цінності або завдання збігаються).

3. Що таке "мережа" у військовому сенсі?

У теорії інформаційно-мережевої війни основним поняттям є термін "мережа". У сучасній американській мові, окрім іменника "the network" — "мережа", використовують неологізм — дієслово "to network", що переводиться як "омережити", "охопити мережею", "впровадити мережу", "під'єднати до мережі". Зміст "мережі", "мережевого принципу" полягає в тому, що головним елементом моделі є "обмін інформацією" — максимальне розширення форм її виробництва, доступу, розподілу, зворотного зв'язку. "Мережа" є новим інформаційним простором, в якому і розгортаються основні стратегічні операції — як розвідувального, так і військового характеру, а також відбувається їхнє медійне, дипломатичне, економічне і технічне забезпечення.

У широкому розумінні поняття "мережа" охоплює різні складові, які раніше розглядали лише окремо. Бойові одиниці, система зв'язку, інформаційне забезпечення операції, формування громадської думки, дипломатичні кроки, соціальні процеси, розвідка і контррозвідка, етнопсихологія, релігійна і колективна психологія, економіка, фінанси, академічна наука, технічні інновації тощо — нині це взаємозв'язані елементи єдиної "мережі", між якими має відбуватися постійний інформаційний обмін.

Зміст військової реформи США у межах "нової теорії війни" інформаційної епохи полягає у створенні потужної і всеосяжної мережі, яка заміняє наявні моделі та концепції військової стратегії, інтегрує їх в єдину систему. Війна стає мережевим явищем, а воєнні дії — різновидом інформаційно-мережевих процесів. Регулярна армія, всі види розвідок, технічні відкриття і високі технології, журналістика і дипломатія, економічні процеси і соціальні трансформації, цивільне населення і кадрові військові, регулярні частини й окремі групи — все інтегрується в єдину мережу, якою циркулює інформація. Формування такої мережі становить суть військової реформи збройних сил США.

Інформаційно-мережеві війни здебільшого відбуваються без використання класичних засобів озброєння. Ці конфлікти є логічним наслідком геополітики і ніколи не ведуться прямо. Для початку мережевої операції потрібно створити умови, за яких сторони протистояння будуть зацікавлені в реалізації певного сценарію. При цьому немає єдиного центру ухвалення рішень, а лише певний контекст (намір командира), який підхоплюють та інтерпретують учасники мережі. Немає прямих команд, є певні очікування, що озвучують представники центру мережевих операцій (мозкового центру вироблення концептуальних рішень). Виконавці отримують тільки загальне уявлення про завдання, а головне — їм надають можливість самостійно шукати шляхи найефективнішого його розв'язання залежно від конкретних умов. Припустимо, що хтось уміщує в ЗМІ інформацію, яка згодом поширюється мережею, а її учасники вже сприймають відомості як керівництво до дії, виходячи з обставин і, що важливо, самостійно приймають рішення.

У разі негативного результату центр не несе прямої відповідальності, навпаки, виявляє гнучкість у прийнятті нових рішень. Жодного узгодження між центром ухвалення рішення і виконавцем немає, вузлові елементи мережі також можуть діяти автономно від центру. Навіть у разі, якщо між

мережевою структурою і центром управління виявлено зв'язок, його можна довести тільки побічно. Це ідеальний варіант ведення війн.

Важливою властивістю мережевої структури є відхід від ієрархічного управління, відмова від прямих наказів. Наміри командира — це управління через систему натяків.

Мережі легко пронизують державні кордони, долають економічні та юридичні перешкоди, вбудовуються в життя країни-мішені, стають для неї вкрай необхідними. Люди поступово перетворюються на елементи глобальної мережі. Змінюються їхні думки, смаки, позиції щодо широкого кола явищ і проблем, які коригують та підлаштовують під думку мас. Через під'єднаних до мережі осіб можна пропускати будь-яку інформацію, як позитивну, так і негативну, при чому, темні імпульси, що спонукають до здійснення деструктивних дій, які людині, що дотримується певних морально-етичних цінностей, ніколи не спало б на думку зробити.

4. Оператор мережі — "мережевик"

У процесі поширення мереж виникло поняття "оператор мережі", або "мережевик". Це людина, яка в класичній науці може бути дилетантом, проте в контексті мережевих війн є головним оператором. Мережевик — фахівець, здатний швидко освоїти будь-яку сферу діяльності, не занурюючись детально в її особливості. Це відрізняє його, наприклад, від класичного фізика, який ґрунтовно вивчає та добре знає цю науку, проте в царині хімії орієнтується значно слабше, а про соціологічні закони взагалі не має уявлення. Мережевик — талановита людина, здатна до навчання і швидкого переформатування, а найголовніше — він має певну парадигмальну систему поглядів, якої неухильно дотримується.

Архетипом мережевика є журналіст, адже саме журналістське середовище зазвичай слугує основним джерелом політичних кадрів у сучасному світі. Журналіст — це мобільний інтелектуал, який добре орієнтується в усіх сферах. Сьогодні він може писати про озброєння, завтра про соціальне невдоволення, післязавтра може стати парламентським кореспондентом і писати про ухвалення законів, згодом — прес-секретарем президента, а надалі розпочати власну політичну кар'єру. Саме мережевик є носієм мережевого коду.

Мережевий код — це світоглядна парадигма, за допомогою якої оператор мережі може фільтрувати інформацію, вишуковуючи з її нескінченного потоку контент, потрібний для реалізації певної операції.

Особливістю інформаційного суспільства, яке сформувалося в постіндустріальну епоху, є те, що кількість інформації досягла такого обсягу, що жодна людина не в змозі засвоїти його чи бодай упевнено в ньому орієнтуватися. Але саме цей, не розпізнаний людською свідомістю контент надає одну з головних переваг мережевику під час ІМВ.

Є сталий штамп інформаційної епохи: "Хто володіє інформацією, той керує світом". Більшість людей сприймає його буквально, розмірковуючи: "Зараз я ввімкну телевизор, радіо, Інтернет, отримаю багато інформації та правитиму світом". І через 10 хвилин свідомість переповнена такою кількістю інформації, що від неї починає нудити. Людина усе вимикає, йде на вулицю, обираючи безінформаційний спосіб життя, оскільки відбулося інформаційне отруєння.

Проте інформацію продовжують генерувати і поширювати. Що це означає? Насамперед — перевагу для реалізації мережевих стратегій, адже контент, потрібний для ведення бойових дій у мережевій війні, передається відкритими каналами. Тобто у середовищі значних інформаційних потоків, які неможливо досягнути й усвідомити,

таємна інформація, як і будь-яка інша, надходить доступними каналами. Щоб краще зрозуміти цей механізм, розглянемо основні поняття мережевої війни.

Невідома мережа приховує колосальну загрозу, проте, як і будь-яка зброя, може бути використана як агресором, так і проти нього. Ворожу мережу можна вивчити і застосувати проти розробника.

Приймаючи руйнівні для країн СНД світоглядні моделі, агенти американізму залишалися невразливими, у тому числі й для спецслужб країн-мішеней. І не лише тому, що останні підкорялися політичній волі вищого керівництва, підтримуючи зрадницький курс геополітичного ворога. Мережева технологія настільки гнучка, що не потребує постійного прямого контакту "центру" з "резидентурою", тому, що мережа не оперує такими застарілими категоріями, використовуючи їх лише як алегорію. Принцип мережі виключає таку потребу, замінюючи і "центр", і "резидентуру" головним для мережі поняттям — "самосинхронізація".

5. Мережева самосинхронізація

Шеф-редактор московського бюро газети Financial Times, американець за походженням Ч. Кловер так позначив суть мережевого підходу: "Мережеві технології — це мережа, структура без "голови", без керівника. Не ієрархічна, а горизонтальна, децентралізована структура. "Інформаційний простір" — це не ієрархія. Так, я представляю газету, але ніхто не говорить мені, що друкувати, реально нам ніхто не вказує, які думки викладати в наших статтях". Це доволі показове висловлювання, оскільки точно передає мережеву атмосферу.

Мережевик самотужки приймає рішення та орієнтується в тому, як відреагувати на певну подію, адже заздалегідь налаштований на те, що його рішення синхронізується із загальними параметрами мережі. Саме тому шеф-редактором московського бюро впливової британською Financial Times призначено американця, який пройшов спеціальну підготовку і навчання (деканом Ч. Кловера був відомий П. Волфовіц). Це показовий момент мережевого підходу — **реальність сформована, запрограмована заздалегідь**.

Мережева самосинхронізація перетинається з таким поняттям, як таймінг — ретельне планування заходів. У мережевій війні вирішальне значення має оперативність ухвалення і виконання рішення. Якщо наказ про початок операції не реалізовано через 5 хвилин, то через 6 хвилин він уже не актуальний, виконувати його недоцільно, адже за цей час ситуація докорінно змінилася і потрібно виконувати інший наказ. Поняття "таймінг" запозичено в мережеві стратегії з фондових ринків, у брокерів, що займаються купівлею і продажем акцій. Якщо ціна на акцію за 10 хвилин зросла, то через 12 хвилин впала, і хто не встиг продати її через 10 хвилин, через 12 продавати її вже не буде.

Отже, якщо Ч. Кловер оперативно, в момент конфлікту подасть статтю про те, що, наприклад, Росія напала на Грузію, а через місяць напише спростування, це вже нікого не зацікавить. Йому ніхто не телефонував із Вашингтона: "Чарльз, пиши про те, що Росія напала на Грузію". В той момент він і сам це чудово розумів. Американець, який пройшов навчання у П. Волфовіца і відповідним чином сформований, — це готовий продукт американської стратегії: в будь-якій ситуації, де б він не перебував: у Росії, Казахстані, на Близькому Сході, в Китаї, він діятиме з позиції інформаційної стратегії США, адже так сформований. Йому не треба щохвилини віддавати накази або скеровувати на певні дії. Він знає та інтуїтивно відчуває, що потрібно робити. Опинившись на місці подій, навіть отримавши два повідомлення, які суперечать одне одному, — він все одно латентно, через власне світосприймання, обере те,

що відповідає сформованій американській стратегії. Згодом, аби зберегти неупередженість, він напише матеріал, відштовхуючись від протилежної позиції, — через певний час, коли це вже не критично. Тобто журналіст самосинхронізується з потрібною стратегією.

Чому шеф-редактором газети Financial Times в Москві не може бути, наприклад, індус? Тому що він інакше мислить. І звичайно, станься така війна при ньому, він, поперше, нікуди не поїде. По-друге, навіть якщо він, врешті-решт, і опиниться у Москві, після того, як йому неодноразово зателефонує головний редактор, довго медитуватиме. У результаті напише про те, які хороші росіяни, який це великий народ з чудовими традиціями, а про конфлікт і не згадуватиме.

А ось американець, що закінчив університет у США і пройшов інструктаж ЦРУ, — журналіст — оперативно реагує, швидко виїжджає, одразу налаштовується на ситуацію в потрібному ключі. Перевага заздалегідь створених вузлів мережі в тому, що вони функціонують тоді, коли треба. Тривалий час можуть бути пасивними і нічого не робити, займатися, приміром, збиранням марок та обміном ними. Але в потрібний момент активуються, самосинхронізуються і виконують свою мережеву місію.

Отже, самосинхронізація — це стан попереднього налаштування, внаслідок якого в момент активації мережевий вузол вмикається самостійно, без додаткового імпульсу. Ніхто його покровоно не контролює, не скеровує, не віддає щохвилини накази. Він сам знає, що і як йому робити, адже це правильно налагоджений, якісний елемент американської мережі.

Величезну кількість вузлів такої мережі не можна налаштувати штучно, примусово, подзвонивши з Вашингтона, проконтролювавши і проінструктувавши кожного. Вони самостійно налаштовуються і ухвалюють поточні рішення: як їм діяти, на чий бік стати, яку тематику обрати для статті — на підтримку президента чи опозиції, тощо.

Мережа — це велика кількість самоналагоджувальних вузлів, що діють на основі принципу самосинхронізації відповідно до заздалегідь сформованої світоглядної парадигми.

6. Сфери дії мережевих війн

Теорія мережевих війн передбачає дію в чотирьох сферах людського життя: фізичній, інформаційній, когнітивній, соціальній. При цьому вагомим результатом у мережевих війнах досягають завдяки синергії всіх елементів.

Фізична сфера. Це традиційна сфера війни, в якій відбувається зіткнення фізичних сил. Охоплює середовища ведення бойових дій (море, сушу, повітря, космічний простір), бойові одиниці та фізичні носії комунікаційних мереж. В інформаційну епоху фізичну сферу слід розглядати тільки як частину середовища дії мережевих технологій, основна кількість яких перебуває в інших царинах.

Інформаційна сфера. В ній створюється, обробляється і розподіляється інформація, налагоджені системи передачі інформації, моделі її опрацювання тощо. Інформаційна сфера пов'язує всі рівні ведення війни і є пріоритетною.

Когнітивна сфера. Когнітивною сферою є свідомість бійця. Основні війни точаться саме в цьому сегменті. Також в ньому формуються такі складники, як команди, доктрини, тактика, техніка і процедури.

Соціальна сфера. Це поле взаємодії людей, де переважають історичні, культурні, релігійні цінності, психологічні установки, етнічні особливості. В соціальному просторі розгортаються стосунки між людьми, структуруються природні ієрархії в групах — лідери, ведені тощо, формуються системи групових стосунків.

Війни інформаційної епохи засновані на свідомій інтеграції всіх наведених сфер. З них і створюється мережа, що становить основу воєнних дій. Мережеві війни точаться

завжди і проти всіх у багатовимірному просторі — соціокультурній, когнітивній, інформаційній і фізичній сферах.

У змістовому плані мережеві війни — це, передусім, війни психологічні, когнітивні і навіть культурні.

Розробники теорії "мережевих війн" фактично отожднюють трансляцію на інші народи власного "культурного коду", світогляду, національної системи цінностей із суттю війни. Це фундаментальна теза, згідно з якою війна з використанням зброї трансформувалась у війну ідей, а ідеї перетворилися на єдину ефективну зброю. Саме так збройні сили США навіюють світовій спільноті думки про безглуздя військової конкуренції з Америкою.

Уперше за історію людства ідеологічний, інформаційний, пропагандистський вплив на супротивника позбавив війну її основної соціально-політичної функції.

Популяризація власного способу життя, думок, системи цінностей, "лабораторна" розробка і подальше впровадження небезпечних для супротивника світоглядних та ідеологічних концептів, диригування протестними і релігійними рухами, створення "п'ятих колон", маніпуляція внутрішньою опозицією, підтримка дисидентів і перебіжчиків, політичні вбивства і перевороти, — поступово усе це почало трансформуватися в новітню форму ведення війни, що оптимально відповідала рівню розвитку індустріального суспільства в ядерну епоху і потребувала принципово іншої системи національної безпеки.

Американські технологи зауважували: "Те, що ми шукаємо, рухаючись з індустріальної епохи в інформаційну, максимально відповідає новій теорії війни: могутність надходить сьогодні з іншого джерела, використовується по-іншому і здатна викликати ефекти, яких не було раніше. В період індустріального суспільства потужність залежала від мас. Тепер вона має тенденцію залежати від інформації, доступу до неї і швидкості цього процесу. Нам довелося назвати цю нову теорію війни мережецентричним військовим мистецтвом".

Логіка мережевого суспільства трансформує звичні раціональні структури в психології особи. Як відомо з когнітивної психології, кожна людина сприймає зовнішній світ, інших людей і себе крізь призму пізнавальної системи, "персональних конструктивів". Розробники "нової теорії війни" стверджують, що сьогодні зміни відбуваються і на глибинному рівні людської свідомості. Коли індивід створює науково-технічні досягнення, вони, зі свого боку, чинять фундаментальний вплив на психіку, свідомість і внутрішній світ людини.

У мережеві війни реальне є вторинним щодо віртуального. Імідж, інформація набагато важливіші за реальність. Власне, реальність стає "реальною" лише після того, як повідомлення про неї потрапляють в інформаційне поле. Звідси висновок: головне — контроль над інформаційним полем і той, хто його контролює, — контролює усе. Інформаційний супровід війни стає не другорядним елементом обслуговування (як класична пропаганда), а сенсом і суттю війни, що вже має інформаційно-мережевий характер.

7. Операції базових ефектів

Сьогодні сегментом, в якому перетинаються задуми ініціаторів і виконавців терористичних і екстремістських дій, стали "операції базових ефектів" (Effects-based operations), далі — ОБЕ, що визначають як "сукупність дій, спрямованих на формування моделі поведінки друзів, нейтральних сил і ворогів у ситуації миру, кризи і війни" [9].

Основний компонент ОБЕ — когнітивна сфера — свідомість бійця, що атакує, і супротивника, якого атакують. Саме вона є простором, де здійснюються ОБЕ.

У когнітивній сфері також перебувають такі явища, як доктрина, тактика, техніка і процедури, "здатність до опору" або "готовність до прийняття нових сенсів і цінностей".

Зауважимо, що застосовувані в ОБЕ когнітивні технології трансформації соціальної поведінки (КТТСП) у процесі розвитку розділилися на лонгетюдні (систематично повторювані) способи трансформації сенсів й історичної пам'яті та смартформи організації соціальної поведінки. Отже, КТТСП впливають як на стійкі структури особистості (ціннісні орієнтації), так і на оперативні мотивації. Основними технологіями лонгетюдного впливу нині є трансгенні культури, субкультури і комп'ютерні ігри.

Операції базового ефекту спрямовано на формування структур поведінки усіх учасників політичного процесу. Не лише союзники, а й сили, що обрали нейтральну позицію, і вороги (без їхнього відома) залучаються до нав'язаного ззовні сценарію і діють відповідно до волі тих, хто керує ОБЕ (тобто США), перетворюючись на маріонеток. Це означає поразку ще до початку війни. А коли справа доходить до відкритого протистояння, і супротивник, і нейтральні сили, і союзники повністю підкоряються правилам ініціаторів конфлікту, виконуючи запрограмовані дії.

До цього додамо принцип самосинхронізації, що забезпечує можливість акторів мережевого процесу функціонувати майже в автономному режимі, самостійно формулювати і вирішувати оперативні завдання на основі загальної обізнаності та розуміння наміру командира.

Об'єкт впливу при застосуванні ОБЕ дезорганізується одночасно в усіх сферах:

— у соціокультурній і когнітивній — внаслідок розгортання по всьому світу лобістських груп і "соціальних мереж" (маркетингового, правозахисного, науково-дослідного, освітнього, добродійного і подібного спрямування), які відкрито або приховано пропагують і поширюють американський спосіб життя, експортують ліберальну систему цінностей, транслюють відповідні культурні та світоглядні коди, здійснюють "мережеві" революції;

— в інформаційній — внаслідок тотального панування американського військово-стратегічного комплексу, приватних корпорацій, ЗМІ і комунікаційних провайдерів у галузі збирання, опрацювання і поширення інформації;

— у фізичній — внаслідок швидкої та ефективної поразки сил і засобів супротивника в "гарячій війні" завдяки використанню "високоточної зброї" й інших новітніх військово-технічних досягнень.

ОБЕ означає встановлення повного контролю над усіма учасниками актуальних або можливих бойових дій (тобто не лише під час прямого протистояння стосовно супротивника, як класичні війни промислового періоду, а й в періоди миру чи кризи і не лише проти супротивника, а й щодо союзника або нейтральних сил) і тотальне маніпулювання ними в усіх ситуаціях. У цьому полягає сутність інформаційно-мережевої війни — вона не має початку і кінця, триває постійно, а її мета — абсолютний контроль над усіма учасниками історичного процесу у світовому масштабі. Отже, впровадження "мережі" позбавляє країни, народи, армії та уряди світу самостійності, суверенності й суб'єктності, перетворюючи на жорстко керовані, запрограмовані механізми.

За невігадливою "технічною" аббревіатурою "ОБЕ" стоїть план прямого планетарного контролю, світового панування нового типу, коли управління підлягають не окремі суб'єкти, а їхній зміст, мотивації, дії, наміри тощо. Це проект глобальної маніпуляції й тотального контролю у світовому масштабі.

Висновки

В умовах нестримної світової глобалізації соціально-економічна, політична і культурна мережі пронизані інформаційними каналами й утворюють інформаційно-мережеві структури. Це дає можливість вести ІМВ на новому рівні,

що зачіпає, окрім збройних сил, усю сферу соціуму: дипломатичні канали, інформаційну, соціально-культурну, світоглядну, фінансово-економічну, політичну й технологічну сфери, а також науку, психологію і внутрішній світ людини.

Виходячи з цього, пропонуємо системний погляд на проблему ведення ІМВ, щоб на концептуальному рівні дати уявлення про війни в глобальному контексті, розкрити їхню суть, роль і значення у сучасному житті.

Колосальна робота багатьох експертів і дослідників мозкових центрів, що одержала підтримку з боку військового відомства США, призвела до появи великої кількості нових військових концепцій і теорій, покликаних забезпечити високу ефективність дій американських збройних сил в нових умовах, проти нових ворогів, з якісно новим арсеналом сил і засобів озброєної боротьби. Однією з таких теорій стала концепція "інформаційно-мережевої війни".

За минулі роки ця теорія не лише опанувала уми військових експертів, а й оформилася доктринально. Збройні сили США та їхні союзники по блоку НАТО активно впроваджують різноманітні підходи до введення ІМВ у практику військового будівництва і підготовки військ.

Для активної протидії інформаційно-мережевим війнам потрібно ґрунтовно вивчити їхні функціональні складники, стратегії й технології ведення.

Список використаної літератури

1. *Mixednews*. Сеть новостных блогов. — Режим доступа: <http://mixednews.ru/archives/59576>. — Загл. с экрана.
2. *Петрик В.* Сучасні технології маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій / В. Петрик, В. Остроухов [та ін.] : навчальний посібник. — Київ : 2006. — С. 196.
3. *Arquilla J.* The Advent of Netwar / Arquilla J., Ronfeldt D. — Santa Monica, CA : RAND, 1996. — P. 47.
4. *Network Centric Warfare*, Report to Congress, 27.07.2001 г. — Mode of access: http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf. — Title from the screen.
5. *Alberts D. S.* Network Centric Warfare: Developing and Leveraging Information Superiority / Alberts D. S., Garstka J. J., Stein F. P. — Washington, D. C., 1999.
6. *Forgues P.* Command in a network-centric warfare // Canadian Military Journal. — Summer 2001.
7. *Коровин В.* Третья мировая сетевая война / В. Коровин. — Санкт-Петербург : Питер, 2014. — 352 с.
8. *Кастельс М.* Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе: Антология ; Под ред. В. Л. Иноземцева. — Москва : Academia, 1999. — С. 492—505.
9. *Edward A.* Effects-based Operations. Applying Network-centric Warfare in Peace, Crisis and War / Edward A., Smith Jr. — Washington, DC : DoD CCRP, 2002.

Информационно-сетевые войны (ИСВ) — новая военная разработка Пентагона, которая дает возможность одержать победу над противником без применения традиционного оружия. И это не война в сети Интернет, несмотря на то, что она также используется как инструмент информационно- сетевого противостояния. Средой для ведения ИСВ является современное информационное общество.

Information and network warfare (INW) is a new Pentagon military knowhow that makes it possible to defeat an opponent without the use of conventional weapons. This is not Internet war, despite the fact that the Internet is also a tool for information and network wars. Modern information society becomes the environment for INW.

Надійшла до редакції 12 січня 2017 року