УДК 94+327+63.3 (0)

Бережна М.С.

ІНФОРМАЦІЙНІ ТА МЕРЕЖНІ ВІЙНИ У ВІЙСЬКОВИХ ДОКТРИНАХ США

У статті розглянуто базові принципи інформаційних та мережних війн у військових доктринах США кінця XX – початку XXI століття. Аналізується діяльність Міністерства оборони США та трансформація військового сектора.

Ключові слова: *інформаційна війна, мережна війна, військова доктрина, трансформація військового сектора.*

В статье рассмотрены базовые принципы информационных и сетевых войн в военных доктринах США в конце XX – начале XXI века. Анализируется деятельность Министерства обороны США и трансформация военного сектора.

Ключевые слова: *информационные войны, сетевые войны, военная доктрина, военная трансформация.*

This article concerns pivotal principles of information warfare and Network-Centric Warfare in the USA military doctrine, which were accepted in the end of the XX – beginning XXI century. Analyzing The Ministry of Defense's activity military sector and transformation.

Key words: *information warfare, Network-Centric Warfare, military doctrine, military sector transformation.*

Інформаційні системи у військовій сфері почали відігравати не тільки забезпечувальну роль. Вони перетворилися в могутній засіб впливу як на діючого або потенційного супротивника, так і на державу в інтересах трансформації його в дружнє або союзне. В сучасних умовах значення інформаційних, у тому числі мережних операцій, буде постійно збільшуватися. Необхідність та важливість інформаційного впливу на потенційного супротивника була завжди очевидною.

На початку XXI століття інформаційні війни та інформаційні мережні операції остаточно перестали вважатися вельми теоретичною проблемою та перейшли до практичної площини. На сучасному етапі концепція мережних воєн, яка була розроблена Пентагоном, реалізується на державному та військовому рівнях. Для держави мета інформаційного протиборства в широкому сенсі слова міститься в послабленні позицій конкуруючих держав, підриві їх національно-державних підвалин, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери існування суспільства, проведенні психологічних операцій, підривних атак та інших деморалізуючих пропагандистських акцій.

Метою цієї статті є вивчення базових принципів проведення інформаційних та мережних війн у сучасній зовнішній політиці США, визначених відповідними доктринальними документами та статутами військових сил США. В історичній літературі ця тема не знайшла свого висвітлення.

Мережні операції на даному рівні можуть вирішувати задачі захисту національних інтересів США, попередження міжнародних конфліктів, провокаційних терористичних акцій, а також забезпечення безпеки національних інформаційних ресурсів [1].

Результатом усвідомлення необхідності виконання таких завдань стала поява теорії мережної організації (Network-Centric Warfare). ЇЇ авторами вважаються віце-адмірал ВМС США Артур Цебровські та Джон Гарстка. Хоча ця теорія з'явилася відносно недавно, вона вже посилено впроваджується у практику.

Концепція мережної організації військових сил базується на використанні інформаційних технологій і, в першу чергу, свідчить про тотальну інтеграцію сенсорів (супутників, безпілотних літаючих апаратів), комп'ютерних та комунікаційних систем, систем управління (відповідальних за прийняття рішень) та бойових платформ. Як відмітив А. Цебровські, колишній директор Управління трансформації сил Міністерства Оборони США, «концепція мережної війни говорить не про технології. Вона є продовженням військової теорії» [2].

На військовому рівні мережні операції являють собою комплекс заходів, які проводяться в масштабах збройних сил країни, їх видів, об'єднаних командувань, і є складовою частиною військових кампаній та операцій. Вони скеровані на досягнення інформаційної переваги над супротивником (у першу чергу, в керуванні військами) та захист своїх систем управління. Для цього можуть бути використані будь-які військові і технічні сили та засоби, які є в розпорядженні, за умов формального дотримування правових, моральних, дипломатичних, політичних та військових норм. Перед військовими силами вперше поставлена задача впливати на супротивника ще до початку активних бойових дій з тим, щоб забезпечити вигідну для США направленість процесів управління та прийняття рішень проти діючої сторони [3].

Як засіб впливу інформаційні системи були застосовані під час війни «Буря в пустелі» в 1991 році, хоча тільки в 1992 році термін «інформаційна війна» був закріплений офіційно директивою міністра оборони США DODD 3600 від 21 грудня 1992 року. Інформаційна обробка супротивника в ході операції «Буря в пустелі» призвела до здачі в полон 70 000 (83 %) іракських військово-службовців.

Після аналізу війни в Іраку в 1991 році стало зрозумілим, що такий розподіл компетенції може забезпечити необхідну ефективність дій США на всіх етапах розвитку конфлікту [4].

Концепція ведення мережних операцій є ключовим елементом трансформації військових сил, яка втілюється Міністерством оборони США (МО США) і мета якої – забезпечення американських національних інтересів за рахунок військової переваги над будь-яким потенційним противником. У МО США стверджують, що для вирішення цього завдання необхідно створення мережної структури, яка дозволить більш оперативно реагувати на загрози, що виникають. У зв'язку з цим військове відомство, окрім закупівлі та випробування нової техніки, змінює основні доктрини, систему навчання та відбору кадрів [5; 6].

Основні принципи ведення інформаційних мережних воєн щодо військових сил були сформульовані в Директиві міністра оборони США № TS 3600.1 «Інформаційна війна». В ній перед об'єднаним штабом Комітету начальників штабів та штабами видів військових сил ставились задачі щодо розробки військового аспекту нової концепції. Ця робота була завершена до кінця 1993 року та знайшла своє відображення в Директиві голови КНШ № 90-93. В ній вихідні достатньо аморфні положення інформаційної війни були трансформовані в концепцію «боротьби з системами управління». Ця боротьба визначалася як «комплексне проведення згідно єдиному задуму та плану психологічних операцій, заходів щодо оперативного маскування, радіоелектронної боротьби та фізичного знищення пунктів управління та систем зв'язку супротивника з метою позбавити його інформації, вивести з ладу чи знищити його системи управління, одночасно захистивши свої від аналогічних дій». Однак пізніше військове керівництво було змушене розширити перелік цілей проведення інформаційних операцій.

Ідея завоювання інформаційної переваги над супротивником шляхом проведення інформаційних операцій послідовно втілювалася в документах КНШ МО США «Єдині перспективи 2010» та «Єдині перспективи 2020», а також в документах МО США «Чотирирічний огляд стану військових сил» від 2001 та 2006 рр. У них визначалися цілі, задачі та основні принципи інформаційної боротьби, обов'язки керівних органів та службових осіб щодо її організації та планування в мирний час і в кризових ситуаціях. Практична реалізація цих доктринальних положень повинна втілюватися в рамках ведення інформаційних операцій [7; 8; 9].

Прикладом послідовного втілення такого підходу є американський польовий статут «Інформаційні операції, доктрина, тактика, техніка та принципи проведення», який був опублікований у листопаді 2003 року [10]. В цьому документі визначені основні поняття, які пов'язані з виконанням інформаційних операцій, тактика їх ведення та необхідні технічні засоби. Характерно, що при цьому розглядається не тільки принципова можливість проведення інформаційних операцій американцями, але й приділяється велика увага питанням протидії асиметричним загрозам в інформаційній сфері, дається детальна класифікація як загрозам, так і їхнім джерелам.

Статут трактує інформацію як елемент військової могутності, а інформаційні операції – як синхронізоване та ефективне керування й розвідку, що дозволяє командирам досягати інформаційної переваги над супротивником. Статут визначає інформаційні операції як використання основних можливостей радіоелектронної та психологічної боротьби, порушення працездатності комп'ютерних мереж, військового обману та заходів щодо забезпечення безпеки у сукупності з допоміжними та забезпечувальними діями, які, в свою чергу, покликані порушувати або захищати інформаційні ресурси та системи й впливати на процес прийняття рішень. Таким чином, поняття «інформаційні операції» на сучасному етапі поєднує раніше розрізнені напрямки бойових та забезпечувальних дій.

З цієї доктрини очевидно, що до спектру інформаційних операцій відносять практично всі основні теоретичні напрямки інформаційної війни, в тому числі мережну війну, які були розроблені в 90-х рр. XX століття.

Серед новітніх методів інформаційних операцій статут розглядає несанкціонований доступ, упровадження злісного програмного забезпечення, ведення радіоелектронного заглушення, проведення електронних атак, фізичне знищення інформаційних систем та систем управління, а також прямий вплив на процеси прийняття рішень.

У лютому 1996 року Міністерство оборони США ввело в дію «Доктрину боротьби з системами контролю та управління», а в 1998 році – «Об'єднану доктрину інформаційних операцій» [11]. У прийнятих документах інформаційна війна визначалась як «комплексна взаємодія на систему державного та військового управління супротивника, на її військово-політичне керівництво, яке вже в мирний час призводило до прийняття рішень, слушних для сторони-ініціатора інформаційного впливу, а в ході конфлікту повністю паралізувало б функціонування інфраструктури управління супротивника».

На підставі доповіді 1996 року спеціальної комісії із захисту критичної інфраструктури в 1998 році було видано президентську директиву PDD-63, а в 2000 році розроблено та затверджено президентом національний план захисту американських інформаційних систем.

У США організація та проведення інформаційних операцій увійшли в число основних завдань Стратегічного командування (CDR USSTRATCOM). У рамках Стратегічного командування в червні 2009 року було створене Кіберкомандування (USCYBERCOM).

Несанкціонований доступ слугує інструментом для розкрадання, додавання, викривлення або видалення інформації із системи управління. Доступ до окремих їхніх ланок, які підключені до каналів зв'язку, здійснюється, наприклад, через Інтернет. Такі канали зв'язку повинні бути захищеними програмними та апаратними засобами безпеки. У випадку, якщо вони нездатні попередити несанкціонований доступ, вважається, що будь-яка система управління наражається на небезпеку.

Упровадження злісного програмного забезпечення змушує інформаційні системи функціонувати інакше, аніж це визначено їхнім завданням. Таке програмне забезпечення включає в себе віруси, логічні бомби, а також програми, які призначаються для подолання захисних засобів та фільтрів. Упровадження злісного програмного забезпечення є допоміжною задачею для втілення несанкціонованого доступу або порушення працездатності інформаційних структур, які залежать від їхнього формального функціонування.

Введення радіоелектронного заглушення – це генерування, спотворення, заглушення, поглинання, посилення або перевідбиття електромагнітної енергії з метою ввести в оману супротивника (або його радіоелектронні системи чи зброю) і тим самим знизити чи ліквідувати його боєздатність.

Проведення електронних атак – це тип радіоелектронної боротьби, яка має на увазі використання електромагнітної зброї, систем радіоелектронного знищення для виводу з ладу обладнання, апаратури, а також особового складу. Електронні атаки включають у себе дії, що запобігають або знижують можливості супротивника ефективно використовувати інформаційні та радіоелектронні мережі.

Фізичне знищення. Супротивник може знищити, вивести з ладу або знизити працездатність систем управління шляхом фізичного знищення їхніх компонентів. У якості інструментів може використовувати весь спектр впливу – від терористичних атак до традиційних ударних засобів. Першорядне значення приділяється високоточній зброї та засобам розвідки і навігації (супутникові системи), які збільшують ефективність застосування високоточної зброї.

Керування сприйняттям здійснюється за рахунок дозування та відбору інформації для зарубіжної аудиторії, які дозволяють керувати її мотивацією, емоціями та цільовими настановами, знижувати волю до опору. Аналогічний вплив на розвідувальні структури та органи державного управління усіх рівнів дозволяє впливати у потрібному напрямку на офіційні оцінки та зовнішньополітичний курс держави. Керування сприйняттям включає широкий спектр заходів, у тому числі психологічні операції, пропаганду, військовий обман та ін.

Таким чином, під інформаційними операціями розуміється використання основних можливостей електронної боротьби, операцій у комп'ютерних мережах, психологічних операцій, військового обману та забезпечення режиму секретності з метою впливу або захисту інформації та інформаційних систем й впливу на процеси прийняття рішень.

Природа інформаційного простору така, що інформаційні операції практично неможливо виявити. Наприклад, якщо метою противника є не порушення працездатності інформаційних систем, а розкрадання важливої інформації, то виявити сам факт такої атаки можна тільки тоді, коли викрадена інформація вже використовується супротивником. З іншого боку, більш важливо досягнути негайного впливу, наприклад, знищити або вивести з ладу ланки інформаційних систем у системах управління.

Планування інформаційних операцій залежить від наявності необхідних інструментів та чітко визначених цілей, які можуть варіюватися в дуже широкому діапазоні. У зв'язку з цим статут FM 3-13 передбачає для виконання усіх рівнів управління більшу свободу прийняття рішень при проведенні інформаційних операцій. Чим більш складною та цілковитою системою управління володіє супротивник, тим більш складним є вибір для проведення проти нього інформаційних операцій. Планування таких операцій потребує від командування, з одного боку, творчого підходу, з іншого – максимально повного уявлення про можливості супротивника. Окрім цього, висока швидкість проведення інформаційних операцій та відсутність універсальних тактик ставлять високі вимоги до якості планування. Відповідальність за ці заходи доручається командуванню на рівні

бригади та вище і залежить від виду інформаційної операції.

У програмному документі Управління трансформації військових сил «Мережна війна: забезпечення переважної військової переваги», який був опублікований у січні 2004 року, зазначаються основні напрямки модернізації військових сил згідно з мережними принципами:

- проведення моделювання, випробувань, експериментів та військових навчань із метою подальшого розвитку теорії та правил мережної війни;
- апробація мережних принципів у МО США;
- прискорення процесу створення єдиної інформаційної інфраструктури в інтересах військових сил;
- прискорення процесу впровадження мережних принципів та технічних елементів;
- перевірка окремих концепцій ведення мережної війни та пошук шляхів подальшого їхнього розвитку;
- вироблення рекомендацій для союзників щодо впровадження мережних принципів;
- створення адекватних доктрин і тактик для мережних військових сил [12].

Таким чином, американський підхід до втілення інформаційних операцій міститься в комплексному використанні новітніх військових доктрин, тактик та досягнень в області інформаційних технологій.

Сьогодні США, маючи значні переваги в сфері розробки й використання новітніх радіоелектронних систем і комп'ютерних технологій та спираючись на нові концепції, намагаються закріпити за собою домінуючу роль не тільки в політичній, економічній і військовій сферах, але й у всесвітній інформаційній інфраструктурі.

ЛІТЕРАТУРА

1. Wilson C. Network Centric Warfare: Background and Oversight Issues for Congress / C. Wilson // CRS Report for Congress. – 2004. – P. 3-6.
2. Cebrowski A. K., Garstka J. J. Network-Centric Warfare: Its Origin and Future / A.K. Cebrowski, J.J. Garstka // Proceedings. – 1998. – January. – P. 32. [Електронний ресурс] Режим доступу: http://www.iwar.org.uk/rma/resources/ncw/ncw_2nd.pdf.
3. Жуков В. Взгляды США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. – № 1. – С. 2-5.
4. Cordesman A.H. Arms Control and the Revolution in Military Affairs / A.H. Cordesman. – Washington: Center for Strategic and International Studies, 2000. – P. 61. [Електронний ресурс] Режим доступу: http://www.iwar.org.uk/rma/resources/ncw/ncw_2nd.pdf.
5. Network Centric Warfare Creating a Decisive Warfighting Advantage // DoD, Office of Force Transformation. – 2004. – January. – P. 11.
6. Libicki M.C. What Information Architecture for Defence / M.C. Libicki // New Challenges, New Tools for Decissiommaking. – RAND Corporation. – 2003. – P. 78.
7. Joint Vision 2010 // US DoD. – 1996. – P. 41.
8. Joint Vision 2020. The Joint Chiefs of Staff. – Washington, DC: US Government Printing Office. – June 2000. – P. 72. [Електронний ресурс] Режим доступу: http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/01-020.pdf.
9. Quadrennial Defense Review // US DoD. – 2001. – P. 87. – [Електронний ресурс] Режим доступу: http://www.defense.gov/pubs/pdfs/qdr2001.pdf.
10. Information Operations: Doctrine, Tactics, Techniques, and procedures. – Headquarters, Department of Army-November, 2003. – 54 p. [Електронний ресурс] Режим доступу: http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.htm.
11. Joint Publication 3-13, Joint Doctrine for Information Operations. 9 October 1998. – [Електронний ресурс] Режим доступу до доктрини: http://www.iwar.org.uk/iwar/resources/us/jp3_13.pdf.
12. Network Centric Warfare Creating a Decisive Warfighting Advantage // DoD, Office of Force Transformation. – 2004. – January. – P. 16. – [Електронний ресурс] Режим доступу: http://permanent.access.gpo.gov/lps42083/document_318_J2568-NCW_GateFold %20.pdf.

Рецензенти: д.і.н., проф. О.В. Крапівін,
к.і.н., доц. Є.Г. Сінкевич

Стаття надійшла до редколегії 18.02.2010 р.