

Опроценко Ю. О.

**МЕРЕЖЕЦЕНТРИЧНА ВІЙНА:
ОСНОВНІ РИСИ, ОСОБЛИВОСТІ ТА
ПРИНЦИПИ ВЕДЕННЯ**

У статті розглядається концепція мережецентричної війни, як спосіб орієнтований на досягнення військової переваги за допомогою об'єднання військових об'єктів у інформаційну мережу.

Ключові слова: мережецентрична війна, *Network-centric warfare*, інформаційна мережа, GIG або «Глобальна інформаційна решітка».

Постановка проблеми. Останні десятиліття продемонстрували докорінне перетворення традиційного розуміння поняття «поле бою», зсув у розумінні військової та загальної геостратегії.

Глобалізація і технічний прогрес обумовили формування інформаційного простору як «поля бою», де відбуваються відкриті бойові дії проти серверів державних інститутів економічної, енергетичної, адміністративної транспортної інфраструктури. Поняття «кібер-простір», «кібер-безпека», «Кібер-війна», «кібер-атака» стали звичайними у повсякденному житті розвинутих країн, що спрямовують свої сили на «стримування» противника. Використання інформаційного простору як тактичного поля бою для ведення нового типу «гібридних» воєн (воєн непрямыми засобами) передбачає зменшення військових операцій та людських втрат.

Втім, новацією стало і інше поріднене попереднім поняття – це поняття «мережецентричної війни», що передбачає застосування інформаційних технологій для підвищення якості традиційних військових операцій.

Аналіз актуальних досліджень і публікацій. Коректність використання цих понять та їх зв'язок досі залишаються

об'єктом уваги дослідників. Від автору терміну «кібервійна» експерта США Р.А. Кларка в його роботі «Кібервійна», автору терміна «інформаційна війна» - Т. Рона у звіті «Системи зброї та інформаційна війна 1976 р. для компанії «Boeing», авторів терміну «мережецентрична війна» – А. Себровські, Дж. Гарсткі і Дж. Джонсона, до сучасних інтерпретаторів цих понять та їх зв'язку – наприклад, американського вченого М.К. Лібіцкі у роботі «Що таке інформаційна війна», який виокремив 7 форм інформаційної війни, чи української авторки Ю. Разметаєвої, яка в статті «Кібервійна: загально теоретичні аспекти», визначила три споріднені сфери, де найбільша – сфера інформаційної війни, всередині неї – сфера мережевої війни, а найменшою, що розташована всередині мережевої – є кібервійна [6; 4].

Аналіз нової термінології, нових стратегічних та технічних підходів для забезпечення відповідної державної системи безпеки та оборони став предметом діяльності таких дослідників як Ю. Бабенко, В. Буренок, І. Воробьов, Я. Дубовий, А. Кондратьєв, А. Кузьмович, О. Мережко, Ю. Разметаєва, Л. Таліпова, О. Трофіменко та багатьох інших. Особливого значення набувають роботи українських вчених та військових, які визначають технологічну уразливість та шляхи її подолання в Україні, які досліджують досвід військових операцій в системі ведення мережецентричної війни. Тим більш, що прояви мережецентричних воєн мають місце з кінця 90-х років минулого сторіччя. Ще воєнна кампанія коаліційних сил проти Іраку, операція «Буря в Пустелі», у 1991 р. продемонструвала значення інформаційної та технологічної переваги у веденні сучасної війни.

Метою статті є аналіз та визначення механізму ведення мережецентричної війни, виявлення основних рис та принципів нового виду воєнних дій.

Основна частина. Величезна робота експертів і дослідників, яка отримує підтримку з боку військового відомства

США, призводить до появи нових військових концепцій, покликаних забезпечити ефективність дій американських збройних сил в нових умовах, проти нових ворогів, з якісно новим арсеналом сил і засобів збройної боротьби. Однією з таких концепцій стала концепція мережецентричної війни (англ. Network-centric warfare) розроблена трьома американськими військовими: віце-адміралом Артуром Себровскі, науковим співробітником Пентагону Джоном Гарсткі і адміралом Джеймсом Джонсоном. Вперше вона була описана у статті, опублікованій у 1998 році [5]. В її основу покладено постулат, що значно підвищити ефективність своїх військ можна за рахунок їх об'єднання в єдину інформаційну мережу, яка працює у режимі реального часу [2]. Це звучить досить просто, але для того щоб втілити цю ідею в реальність американцям знадобилося кілька років, десятки проведених експериментів і симуляцій, а також сотні мільйонів доларів, витрачених на нове обладнання, програмне забезпечення та навчання військ.

Мережецентрична війна – це не зовсім точний переклад англійського терміна «network-centric warfare». Більш точний переклад – «мережецентричні військові дії». Від неточного перекладу йде і неточне розуміння або навіть нерозуміння суті проблеми. І все ж термін «мережецентрична війна» отримав поширення, і завдання тепер полягає не в тому, щоб його змінити, а в тому, щоб його правильно розуміти і вживати.

Отже, мова не йде про якийсь новий вид війни, а про мережецентричний підхід до організації та ведення військових дій. Більш того, в майбутньому такий підхід буде аксіомою, і всі військові дії будуть незмінно ґрунтуватися на принципі мережецентричності.

Створення єдиної інформаційної мережі здатне в кілька разів збільшити потужність збройних сил без збільшення їх чисельності. Мережецентрична війна дозволяє піднятися на новий рівень управління військами, значно зменшуючи час прийняття рішень. Застосування нових інформаційних технологій дозволяє

змінити класичне співвідношення сил наступаючих і тих, що обороняються, на протилежне. Але це справедливо за умови, що сторона оборони не має можливості вести мережецентричну війну [3].

Якщо порівнювати доктрину мережецентричної війни (далі МЦВ) з концепцією «Бліцкригу» Альфреда фон Шліффена (1905 рік) і з концепцією «Глибокої операції» Володимира Триандафіллова (1931 рік), то стає очевидним, що «Network-centric warfare» відрізняється більшою гнучкістю і забезпечує більшу ефективність ведення бойових дій. У традиційних доктринах вся інформація збирається і передається вгору в штаби, де обробляється і спускається вниз у формі наказів. Швидкість реакції такої системи залежить від пропускну здатності каналів зв'язку і швидкості роботи командування. Якщо управління в системі є повністю централізованим, то при знищенні штабу або каналу зв'язку уся система «зависає» [5]. Отже, як вже вказувалося, в основу концепції мережецентричної війни було покладено ідею досягнення інформаційної та комунікаційної переваги, шляхом об'єднання військових сил в єдину мережу.

Мережецентричність дозволяє значно підвищити якість управління військами, збільшити темп проведення операцій і ефективність вогневого ураження. Також, на думку розробників доктрини, об'єднання збройних сил в єдину інформаційну мережу підвищить їх гнучкість, рівень самосинхронізації, дозволить оптимізувати постачання. Один з засновників концепції – адмірал Джеймсон вказував, що створення загальної військової інформаційної мережі, здатної діяти в реальному часі, підвищить швидкість командування військами і зменшить час прийняття консолідованих рішень. Отже, мережецентрична війна передбачає кібернетичну модель управління бойових дій OODA (Observe (Спостерігати) – Orient (Орієнтується) – Decide (Вирішуй) – Act (Дій)), розроблену полковником ВПС США Джоном Бойдом [6].

МЦВ не можна назвати новим видом війни, скоріше, це революційний спосіб

організації і ведення бойових дій. Завдяки наявності повної інформації про сили і розташування ворога, а також про поточну конфігурацію власних військ, у командування з'являється можливість випереджати супротивника на всіх етапах розгортання і ведення бойових дій. Сторона противника завжди буде відставати на кілька кроків, що позбавить її можливості чинити будь-які дії у відповідь, що призведе її, в кінцевому рахунку, до хаосу і втрати боєздатності. Концепція мережецентричних бойових дій включена у військову доктрину США – так зване «Спільне бачення» розвитку збройних сил США (версії «Joint Vision 2010» і «Joint Vision 2020»). Так, у версії «Joint Vision» (2010) вказувалося, що «відтепер ми ставимо більший акцент на підвищення оперативної сумісності між Службами та багатонаціональними партнерами» [7, с.32]. Велику увагу приділено зростанню технологічного оснащення та питанням навчання військовослужбовців, балансу сил. В якості мети розвитку збройних сил в концепції вказувалося: «Ми повинні підтримувати обережний баланс між оснащенням і підтримкою наших сил і між зубом і хвостом в нашій силовій структурі» [7, с.7-8]. До моменту доктринального визнання, концепція була апробована на практиці в 2003 році у війні між коаліцією США і Великобританії, з одного боку, та Іраком – з іншого [1].

У 2003 році Ірак володів численними збройними силами, що мали багаторічний бойовий досвід, у тому числі військового протиборства з американськими військами. У результаті іракські війська виявилися повернені фронтом на південний захід, маючи в тилу територію нейтральної держави (Ірану), створивши глибоку ешелонну оборону з трьома лініями природних перешкод – річкою Єфрат, болотистого межиріччя і річкою Тигр [1]. Оборона іракських дивізій будувалася у вигляді набору опорних пунктів, розташованих за периметром міст. Польові оборонні позиції в вигляді окопів повного профілю і бойових машин поєднувалися з міськими оборонними позиціями у вигляді будівель і споруд, пристосованих під

укриття бойових машин і довготривалі вогневі точки.

Військові дії були розпочаті 19 березня 2003 р. вторгненням на північ Іраку (в райони, населені курдами) сил спеціальних операцій. Наступного дня було завдано масованого ракетно-бомбового удару по комплексам ППО, радіолокаційним станціям і аеродромам по всій території Іраку. Завдання завоювати панування в повітрі і створити безпілотну зону було вирішено. 21 березня авіація завдала удару по прикордонним опорним пунктам іракської армії, дозволив висунування на територію Іраку сухопутним силам американо-британської коаліції. Одна британська дивізія блокувала район навколо Басри, три американських дивізії (дві експедиційні дивізії морської піхоти і 82-а повітряно-штурмова) завдали удару по флангу першого ешелону оборони іракських військ, дві американські дивізії (3-я механізована і 101-я повітряно-штурмова) пішли в рейд на Багдад [5].

Багдад був взятий в кільце. Протягом трьох днів американо-британська авіація придушувала оборонні позиції іракських військ безпосередньо в межах міста, після чого в нього вступили передові частини 3-ї механізованої дивізії. Всі контратаки найбільш боєздатних дивізій Республіканської гвардії Іраку «Медіна» і «Навуходонсор», а також армійського спецназу були відбиті з великими втратами для її захисників. 9 квітня почалося масове дезертирство військовослужбовців іракських військ по всій території країни, за винятком Тикрита – міста походження президента Іраку, гарнізон якого припинив опір 13 квітня.

Причиною швидкої поразки іракських збройних сил постав ефект від реалізації концепції мережецентричних бойових дій, вперше відпрацьованої американськими збройними силами. Усі без винятку опорні пункти в смузі наступу коаліційних сил незалежно від їх місцезнаходження (в польових умовах або в межах міста) були знищені наступаючими без особливого збитку для себе, незважаючи на чисельну перевагу іракських сил у бойовій техніці і живій силі. За період з 19 березня до

13 квітня 2003 року втрати вбитими американо-британської коаліції склали 172 людини, іракських збройних сил - 9200 осіб [4].

Концепція мережецентричної війни ґрунтується на останніх наукових досягненнях в галузі комп'ютерних та комунікаційних технологій і електроніки. За інформаційним каналам передаються дані у вигляді цифрових і голосових повідомлень, потокового відео. Основу інформаційного простору МЦВ становить GIG або «Глобальна інформаційна решітка» [1], функціонування якої забезпечує потужне угруповання навігаційних, розвідувальних і комунікаційних супутників.

Інформаційно-комунікаційна мережа складається з трьох основних елементів:

- розвідки;
- органів управління;
- засобів ураження (придушення).

Теорія МЦВ базується на трьох основних постулатах:

- якщо об'єднати збройні сили потужними і надійними мережами, то це дозволить перейти на якісно новий рівень обміну інформацією. Під час проведення мережецентричних бойових операцій командування може отримувати інформацію від окремих бойових машин і військовослужбовців, про їх поточне розташування, стан і потреби. Не менш повною є інформація і про противника, яка надходить відразу від безлічі джерел: численних дронів, засобів наземної і радіоелектронної розвідки. Крім того, користувачі інформації є одночасно і її постачальниками.

- постійний обмін інформацією підвищує її якість і рівень загальної інформованості про процеси, що відбуваються на театрі військових дій. Досягається так звана загальна поінформованість (shared awareness).

- підвищення інформованості дозволяє забезпечувати співпрацю і самосинхронізацію між різними підрозділами та родами військ, що, в свою чергу, різко підвищує ефективність виконання бойового завдання. Однією з особливостей МЦВ є можливість

самоорганізації на низовому рівні і горизонтальних зв'язків між різними підрозділами на полі бою.

Висновок. Відмінними рисами мережецентричної війни від інших доктрин є те, що у командування з'являється можливість використовувати збройні сили, розділені географічно. Раніше було необхідно, щоб підрозділи і служби їх забезпечення знаходилися поруч один з одним і в безпосередній близькості від противника або об'єкта, який утримується. Тепер ці обмеження зняті, що було підтверджено в ході реальних бойових дій. Будь-яка війна - це не тільки підрозділ солдатів, що йде в атаку, але і складне логістичне завдання, особливо важко вирішувати яке в сучасній маневреній війні. Використання мережецентричних методів обіцяє справжню революцію в організації адресного тилового постачання.

Однією з основних обставин чому такі бойові дії не стали єдиною формою бойових дій є те, що на ведення МЦВ здатні тільки високорозвинені держави з великим військовим бюджетом. Користуючись просунутими комп'ютерними та інформаційними технологіями, армії таких країн здатні встановити всеохоплююче спостереження над театром військових дій. Перед початком другої війни в Іраку (2003 р.) американці розмістили над цією країною супутникове угруповання, що складається з більш ніж сорока сателітів.

Створення загальної інформаційної мережі дозволяє налагодити ефективну взаємодію між різними суб'єктами в бойовому просторі. Це створює можливість підрозділам, розділеним географічно, проводити спільні дії, розподіляти між собою завдання і обсяги виконання робіт, що дозволяє швидше реагувати на зміну ситуації. Подібна особливість мережецентричних бойових дій сприяє самоорганізації збройних сил на низових рівнях, створення між різними підрозділами горизонтальних зв'язків. Самоорганізація і самосинхронізація забезпечує можливість для низових підрозділів діяти практично автономно, самостійно формулювати і вирішувати

оперативні завдання, виходячи з доступу до загального масиву інформації і розуміючи задум командування.

Список використаної літератури:

1. Воробьёв И. Н., Киселёв В. А. Тактика сетцентрических действий // Армейский сборник: журнал. — 2014. — Т. 238 – № 4. — С. 44-46
2. Долгополов А. Ещё раз о сетцентрических войнах) // Армейский сборник: журнал. — 2015. — Т. 248 – № 2). — С. 3-10
3. Кондратьев А. Сетцентрические концепции ведущих зарубежных стран // Армейский сборник: Научно-методический журнал МО РФ. — М.: Редакционно-издательский центр МО РФ, 2013. — № 03. — С. 36-42
4. Разметаева Ю.С. Кібервійна: загальнотеоретичні аспекти // Вісник АМСУ. Серія «право» – 2015 – № 1 (14) – С. 12-22.
5. Савин, Л. Новые способы ведения войны: Как Америка строит империю / Л. Савин. – Санкт-Петербург: Питер, 2016. – 352 с.
6. Трофименко О.Г., Дубовой Я.В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства // Порівняльно-аналітичне право – 2017 – №1 – С. 189-192 // [Електронний ресурс] – Режим доступу: http://www.pap.in.ua/1_2017/58.pdf
7. Joint Vision 2010 // [Електронний ресурс] – Режим доступу: <http://www.au.af.mil/AU/AWC/AWCGATE/dod/jv2010.pdf>

Oproschenko J. – Student of the Faculty of International Relations, Political Science and Sociology of the Odessa National University named after I.I. Mechnikov **Network-centric war: the main features, features and principles of conduct**

The article considers the concept of Network-centric warfare as a method aimed at achieving military advantage by combining military objects into the information network.

The article considers that the globalization and technological progress have led to the formation of an information space as

a "battlefield", where open hostilities against the servers of state institutions of economic, energy, and administrative transport infrastructure take place. The notions of "cyber space", "cyber security", "Cyber War", "cyber attack" have become less than natural in the everyday lives of developed countries that direct their forces to "detering" the enemy. The use of the information space as a tactical battlefield for conducting a new type of "hybrid" wars (wars indirectly) involves a reduction in military operations and human losses. However, the innovation has become another related to the previous concept - the concept of "Network-centric war", which involves the use of information technology to improve the quality of traditional military operations. The correct use of these concepts and their relationship is still the focus of the researchers.

On an example of an analysis of the American military operation in Iraq in 2003, the author reviewed the process of approbation of network-centric warfare, revealed the general features, features and tactics of such a war.

Key words: *Network-centric warfare, "Cyber War", information network, GIG or Global Informational Grid.*

*Рекомендовано до друку –
к. політ.н , доцентом Узун Ю.В.*

Стаття надійшла в редакцію 11.01.2018.