

УДК 303.6:351.746

Ігор Олександрович Ляшенко

## МЕРЕЖОЦЕНТРИЗМ У ВІЙСЬКОВІЙ СПРАВІ

Розглядаючи можливі форми ведення локальних війн та збройних конфліктів, слід пам'ятати, що військова думка складається із сукупності теорій, підходів, поглядів та парадигм, які належать до конкретної епохи, суспільства або особи. Військова теорія пов'язана з історичним спостереженням і систематичним вивченням організації, стратегій, тактик, технік і процедур від античності до наших днів. Вона є засобом освіти як для військових, так і для політиків. Вона також дає основу для вироблення доктрини, яка, у свою чергу, створює загальну філософію і практику для вирішення проблем у реальному світі (чи за допомогою бойових дій, чи іншими способами). *Мета статті:* провести аналіз виникнення нової концепції ведення збройної боротьби — мережових війн. *Завдання статті:* розглянути зміст мережових війн, їх відмінності від традиційних форм ведення воєн, переваги й недоліки.

Як писали у своїй гучній роботі “Війна та анти-війна” Алвін і Хейді Тофлери “...шлях ведення війни відображає методи зміцнення добробуту — шлях ведення анти-війни повинен відображати шляхи ведення війни” [1]. Відповідно, історія воєн може бути поділена на три великі періоди (або, по термінології авторів, хвилі), які відповідають історії розвитку людських цивілізацій: аграрний, промисловий та інформаційний. Відповідно до моделі Тофлерів майбутні війни для цивілізацій третьої хвилі повинні приймати форму інформаційних воєн. Часто вважають, що інформаційна війна — це війна, що ґрунтується на досконалих системах зв'язку, доступу до космосу, і процесу ухвалення рішень в реальному часі. Насправді, просте застосування подібних технологічних новин — це новий шлях ведення старих бойових дій. Це війна інформаційної епохи, а не інформаційна війна. Боротьба за інформацію відрізняється від боротьби за територію або природні ресурси. Фінансово-промислові групи і навіть держави, які борються за інформацію, значно відрізнятимуться від тих, які воювали за матері-

альні ресурси. Сама природа інформації повинна впливати на політику уряду, встановлювати обмеження на державний суверенітет. У. Швартау, автор книги “Інформаційна війна: Хаос на електронному суперхайвеї”, визначив інформаційну війну як “електронний конфлікт, в якому інформація є стратегічним активом, гідним завоювання чи знищення. Комп'ютери та інші комунікаційні й інформаційні системи будуть цілями для першого удару та, одночасно, зброєю в новій війні” [2].

Із найдавніших часів війни велись у п'яти вимірах — політичному, соціальному, технологічному, операційному та у сфері постачання — які пов'язані з чотирма елементами національної потужності — політичним, соціально-психологічним, військовим і економічним. Ігнорування навіть одного з них може привести до катастрофічної поразки (рис. 1).



Рис. 1. Виміри ведення війни.

Політичний вимір складається з політичної мети та політики — як процесу. Політична мета завжди направляла війни, хоча й не завжди до кінця послідовно.

Соціальний вимір — переконання й зобов'язання людей — також залишається важливим.

Технологія впливає на кожне вимірювання та на всі рівні війни. Вона взаємодіє з культурою і подіями в часі та просторі, здійснює вплив на тривалість, природу та результати конфлікту. Операційне вимірювання пов'язано з веденням війни. Воно складається в основному зі спроб домінувати на полі бою і придушити ворожу волю до ведення боротьби.

Розглянемо останній вимір більш детально. Останньою домінуючою операційною концепцією доінформаційної епохи була концепція послідовних операцій, коли в бій поступово (ешелонами) вводилися всі нові й нові резерви, і перемога залежала від наявності цих резервів та правильного вибору моменту для їх застосування. Проте вже до середини 1980-х років здатність завдати удар одночасно на всьому полі бою зробила послідовні операції застарілими. Бойові дії в майбутньому включатимуть безліч завдань та одночасних дій, що проводитимуться на величезних територіях.

Як показує досвід локальних війн та військових конфліктів, у протиборстві із застосуванням традиційних і, особливо, нових засобів збройної боротьби велике значення надається інформаційній взаємодії всіх учасників операції. Своєчасно усвідомивши значення цього чинника, США та їх союзники по НАТО різко активізували свої зусилля зі створення так званої мережевої системи управління бойовими діями, підпорядкувавши стратегії інтеграції в цю систему сьогодні всі розробки нових озброєнь.

Питання управління військами і бойовими діями із застосуванням засобів автоматизації тісно пов'язані з питаннями інформаційної боротьби. Вперше інформаційні технології як засоби ведення бойових дій були використані у війні проти Іраку в 1991 році, а термін “інформаційна війна”, офіційно — в директиві міністра оборони США від 21 грудня 1992 року. В 1996 році Пентагон затвердив доктрину інформаційної війни (“Доктрина боротьби з системами контролю і управління”), а в 1998 році міністерство оборони США вводить в дію “Об’єднану доктрину інформаційних операцій”. Згідно з останньою інформаційна війна визначається як “комплексний вплив (сукупність інформаційних операцій) на систему державного і військового управління противника, на його військово-політичне керівництво з метою ухвалення ним вже в мирний час сприятливих для країни-ініціатора інформаційної дії рішень і повного паралічу інфраструктури управління противника в процесі конфлікту”. Інформаційна зброя згідно з “Об’єднаною доктриною” розглядається як арсенал засобів несанкціонованого доступу до інформації та виведення з ладу електронних систем управління. Проект Пентагону “Бойові системи майбутнього” й передбачає досягнення збройними силами США до 2010 року повної інформаційної переваги над будь-яким противником. Цьому сприяє і швидке збільшення числа користувачів Інтернету. Так, якщо в 2000 році їх було близько 150 млн осіб, то до 2010 року збільшення їх кількості планується більше як 1 млрд. На думку фахівців у цій галузі, поразка в інформаційній війні може надовго (якщо не назавжди) відкинути країну, що

програла, назад у її розвитку, а країна-переможець отримає необмежені можливості щодо управління переможеними.

Після терористичного акту 11 вересня міністр оборони США Д. Рамсфелд заявив, що Америка повинна готуватися до війни нового типу, яка різче відрізнятиметься не тільки від воєн ХХ століття, але і від війни з міжнародним тероризмом. У зарубіжних джерелах майбутня війна, що вимагає нових принципів оперативного мистецтва, отримала назву “мережевої війни” (network-centric warfare). Концепція “мережевої війни” лежить в основі програми військового будівництва в США до 2010 року (“Joint Vision 2010”), а для її ведення вже сьогодні створюється нова глобальна інформаційна мережа Пентагону (проект Defense Information Grid), першими полігонами для якої стали Балкани, Ірак та Афганістан. “Мережева війна” заснована на досягненні інформаційної переваги над противником, яке перетворюється в пригнічуючу бойову могутність за рахунок зв'язку інтелектуальних об'єктів (мережі датчиків, штабів і виконавчих вузлів) в єдиний інформаційний простір театру бойових дій. При цьому, трансформуючи поняття “поля бою” в поняття “бойовий простір”, концепція “мережевої війни” як віртуальна ціль, окрім традиційних, виокремлює емоції людей, людську психіку і т.ін.

Концепція мережевої війни взята на озброєння не лише в ЗС США. У командуванні Об'єднаних збройних сил (ОЗС) НАТО вона наявна під назвою “мережецентричні можливості ЗС” (Network Centric Capability — NCC), в командуванні ЗС Великої Британії — “комплексні мережеві можливості ЗС” (Network Enabled Capability — NEC), командуванні ЗС Франції — “інформаційно-центрична війна” (Info-Centric Warfare — ICW), командуванні ЗС Австралії — “комплексна мережева війна” (Network Enabled Warfare — NEW), Нідерландів — “мережецентричні операції” (Network Centric Warfare — NCW), Швеції — “мережева оборона” (Network Based defense — NBD).

Щоб розібратися, що таке мережеві війни, чому вони набули такого поширення серед ЗС провідних країн світу та в чому їх відмінність й перевага, звернімося до історії.

Кінець холодної війни співпав за часом з інформаційною революцією в США та провідних Західних країнах. Ці обставини створили підґрунтя для переоцінки наявних військових стратегій та доктрин. Трохи пізніше з'явився і термін “мережецентрична війна”. Сьогодні він став модним не лише в риториці військових відомств багатьох зарубіжних країн, але і в Україні. Проте без розуміння суті проблеми, а також без технічних і, найголовніше, — технологічних можливостей реалізація перспективних концепцій та перехід до нового вигляду будуть ускладнені.

Термін “мережоцентризм” уперше з’явився в комп’ютерній індустрії і став результатом прориву в інформаційних технологіях, які дали змогу організувати взаємодію між комп’ютерами, незважаючи на використання в них різних операційних систем. Стосовно військової справи, мережоцентризм — ширше й насиченіше поняття, яке, по суті, визначає парадигму ХХІ століття і стає невід’ємним елементом революції, що відбувається у військовій справі. І хочемо ми того чи ні, необхідно враховувати його вплив у формуванні Збройних Сил України.

Американська концепція “мережоцентричної війни” — це не лише розгортання цифрових мереж із метою забезпечення як вертикальної, так і горизонтальної інтеграції. Це ще зміна тактики дії перспективних формувань із розосередженими бойовими порядками, оптимізація способів розвідувальної діяльності, спрощення процедур узгодження й координації вогневого ураження, а також деяка нівеляція розмежування засобів по ланках управління.

Розробники концепції “мережоцентричної війни” (віце-адмірал ВМС США Артур Цевровські й експерт Міністерства оборони Джон Гарстка) стверджують, що її вплив має ще масштабніший характер. Підвищення бойових можливостей (по вогнево-му ураженню, маневру, управлінню, живучості і т. д.) формувань — прямий наслідок підвищення рівня інформаційного обміну і зростання ролі самої інформації.

Принципи ведення воєнних дій, будівництва збройних сил і управління бойовими формуваннями в ХХ столітті отримали найменування “платформочентричної війни”. У той час успіх операцій і битв залежав здебільшого від індивідуальних можливостей бойових засобів, а об’єднання мережами, хоча і передбачалося, не дало змоги досягти ефекту, який дають сучасні інформаційні технології. Саме тому упродовж минулого століття військові фахівці всього світу займалися розробкою технічних рішень, пов’язаних насамперед із підвищенням мобільності, точності, а також вогневої потужності засобів збройної боротьби. За своєю суттю, цей процес був підвищенням потенційних можливостей або, по-іншому, бойового потенціалу, основа якого — технічна оснащеність військ. Проте, як показала практика, існують обмеження для їх подальшого зростання та значно підвищується вартість подібних розробок. Крім того, засоби збройної боротьби, більшість із яких перебуває на озброєнні не один десяток років, і бойові формування, що є на сьогодні, вже мають достатній рівень бойового потенціалу, й проблема полягає в тому, як реалізувати цей потенціал. Іншими словами, перед військовими постало завдання досягнення необхідного рівня бойових можливостей, які залежать від багатьох факторів (ефективності розвідки й

управління, впливу природних і кліматичних умов, характеру місцевості, а також дій противника і ін.).

Як відомо, у всьому світі в основі математичних методів визначення бойових можливостей формувань лежить система диференціальних рівнянь Ланчестера. Серед них лінійні і квадратичні закони, які розроблені ще в 1916 році для розрахунку відносних сил пари протистоячих сторін. Рівняння застосовуються й сьогодні, а ступінь впливу різних чинників у сучасних умовах оперативної (бойової) обстановки визначається системою спеціальних коефіцієнтів розмірністю менше одиниці, що цілком логічно, оскільки бойові можливості формувань не можуть бути вище потенційних, тобто апіорі максимальних. Можна, правда, перевернути з ніг на голову всю військову науку і придумати свою систему коефіцієнтів (із розвідки, управління, маневреності і т. д.) більше одиниці, забезпечивши цим “неперевершені” можливості бойовим формуванням нового вигляду. Але весь світ йде іншим шляхом. Його можна визначити як чесніший, такий, що більш відповідає бойовим реаліям. Якщо поглянути інакше, це означає, що лише такий шлях дає можливість мінімізувати людські втрати на майбутніх театрах воєнних дій.

Саме тому в ХХІ столітті таким інструментарієм досягнення нових бойових можливостей, тобто підвищення ступеня реалізації бойового потенціалу, стали сучасні інформаційні технології. І зараз справді можна говорити про фундаментальне зрушення від “платформочентричної” до “мережоцентричної війни”, яка, за твердженням її розробників, визначає нові принципи управління військами й силами.

Поняття “мережоцентрична війна”, або “ведення бойових дій, в єдиному інформаційно-комунікаційному просторі” розглядає бойові формування як своєрідні пристрої, підключені до єдиної мережі. Залежно від вибору мережної архітектури та її типу такими пристроями можуть бути кораблі, літаки, засоби ураження, управління, зв’язку, розвідки і спостереження, група військово-службовців або окремі солдати, а також комбінація і тих, і інших. У цьому випадку можливості бойових формувань визначаються не стільки індивідуальними тактико-технічними характеристиками окремих зразків озброєння та військової техніки (ОВТ), скільки можливостями всієї групи підключених до мережі засобів як єдиного цілого. Саме тут, власне, і виявляється ефект синергізму ( $2+2=5$ ), коли під цілим уявляється щось більше, ніж сума його часток. Стосовно військової справи синергізм — це ефект від спільної дії об’єднаних у мережу засобів збройної боротьби, який за сукупним результатом перевищує суму ефектів від застосування тих же засобів окремо.

Водночас, думка, що об'єднання мережею дозволить вирішувати будь-які проблеми, що виникають, — одна з найбільш поширених і помилкових. Мережі, як і всі комп'ютерні системи, працюють за принципом “сміття на вході — сміття на виході”. Це принцип програмування, відповідно до якого неpravильно введені дані не можуть привести до правильного результату. Таким чином, без точних даних про обстановку, одержаних від засобів розвідки і спостереження, що наповнюють інформаційну базу мереж, самі по собі залишаються всього лише високошвидкісними цифровими трактами між платформами. Більше того, якщо перспективні мережецентричні концепції слід розглядати як необхідний інструмент підвищення бойових можливостей, то ні про яке збільшення власне потенціалу ОВТ або бойового формування мови не може бути. Якщо танк, який перебуває на озброєнні, зі штатним боекомплектком не здатний пробити броню танка противника, то він не зможе цього зробити навіть при оснащенні його суперсучасними системами зв'язку й управління.

За останній час у зарубіжних і вітчизняних засобах масової інформації спостерігається багато дискусій про те, чому необхідні мережі і як їх упровадження може вплинути на можливості збройних сил. На жаль, не у всіх публікаціях були представлені вагомі аргументи, і велика частина з них просто була прийнята як факт.

Більше того, іноземні фахівці зазначають, що не було проведено достатньої кількості досліджень у галузі математичного обґрунтування підвищення можливостей бойових формувань при об'єднанні їх системою єдиного інформаційно-комунікаційного мережевого забезпечення. Саме тому, напевне, навіть у США співтовариство військових експертів поділилося на прихильників, котрі серйозно сумніваються, і противників подібної концепції. Так, прибічники мережецентричних концепцій стверджують, що формування єдиного інформаційно-комунікаційного простору, який дає змогу кожному учасникові бойових дій мати точні дані про ситуативну обстановку, підвищує рівень взаємодії, самосинхронізації, швидкість управління підлеглими силами, а, врешті-решт, і бойові можливості формувань.

Інші зазначають, що примусове проштовхування зверху мережецентричних принципів може придушити розумну критику нової концепції з боку командирів оперативної і тактичної ланок управління. Вони ведуть мову про ймовірність того, що Пен-

тагон може реформувати Збройні сили не для проведення операцій, з якими вони швидше за все зіткнуться, а для таких воєн і збройних конфліктів, які самі хочуть вести.

Наприклад, якщо відповідно до мережецентричних принципів швидкоплинність перспективних бойових дій підвищуватиметься, то слабкіший противник, навпаки, буде намагатися затягнути конфлікт і виграти війну лише єдиним способом — спробою уникнути розгрому, тоді як політична воля США танутиме, а воєнні витрати невблаганно зростатимуть.

Противники ж вірять, що принцип “першим побачив і першим розпочав діяти”, який лежить в основі всіх мережецентричних концепцій, може провалитися в тому випадку, коли факт операції випереджатиме здатність командування ЗС США оцінювати ситуацію і схвалювати рішення. Більше того, вони зазначають, що мережецентризм — це теза, що не тільки переоцінює значення інформації та інформаційних технологій, але одночасно з цим і не здатна повністю реалізувати потенційні технічні можливості.

Незважаючи на низку невіршених проблем і відсутність навіть серед військових фахівців США єдиної думки щодо концепції “мережецентричної війни”, забезпечення всебічної інтеграції, підвищення рівня взаємодії, а також досягнення синергетичного ефекту за рахунок реалізації нових принципів управління й ведення бойових дій стають невід'ємною умовою реформування збройних сил більшості країн світу.

Виникає питання — чи варто відмовлятися від технологічної і, найголовніше, інформаційної революції у військовій справі? Звичайно, ні. Навпаки, основні положення американської концепції “мережецентричної війни” мають бути досліджені для подальших досліджень у сфері формування Збройних Сил України.

І тут особливо важлива націленість військово-теоретичної та політико-воєнної думки на концептуалізацію, на агрегацію окремих, часом зовні розрізнених компонентів у цілісну і при цьому багатовимірну та складну формулу, що визначає характер чергової революції у військовій справі і практичні висновки з цього визначення.

## Література

1. Toffler A., Heidi, War and Anti-War: Survival at the Dawn of the 21st Century. — New York : Little, Brown and Company, 1993. — P. 3.
2. Winn Schwartz. Information Warfare: Chaos on the Electronic Superhighway. — New York : Thunder's Mouth Press, 1994. — P. 13.

В статье проведен анализ возникновения новой концепции ведения вооруженной борьбы — сетевых войн. Рассмотрено их содержание, отличия от традиционных форм ведения войн, преимущества и недостатки.

*Ключевые слова:* сетевая (сетевая) война, сетевый центризм, информационная война.

The analysis of origin of a new concept of armed struggle conduct — network wars — is carried out in the article. Their content, differences from traditional forms of wars, advantages and disadvantages are considered there.

*Key words:* network (network-centric) warfare, network centrism, information warfare.