ІНФОРМАЦІЙНИЙ КОМПОНЕНТ У СУЧАСНИХ КОНЦЕПЦІЯХ ВЕДЕННЯ ВІЙНИ

Пєвцов Г.В., доктор технічних наук, професор, Гордієнко А.М.,
Залкін С.В., кандидат військових наук, старший науковий співробітник,
Сідченко С.О., кандидат технічних наук, старший науковий співробітник,
Хударковський К.І., кандидат технічних наук, старший науковий співробітник
Харківський національний університет Повітряних Сил імені Івана Кожедуба

Сьогодні між провідними державами світу розгорнулося геостратегічне протиборство за досягнення переваги у світовому інформаційному просторі. Акцент методів протиборства, що використовуються, поступово зміщується у бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невоєнних мір. Особливо важливу роль стало відігравати інформаційне протиборство, у тому числі в воєнній сфері. У цей час найбільш розвинені країни мають у своєму розпорядженні потужний інформаційний арсенал, що за певних умов забезпечує досягнення ними поставлених політичних цілей. Гострота і непередбачуваність інформаційного протиборства загострюється тією обставиною, що до цієї пори немає розроблених міжнародних юридичних норм його ведення та протидії йому.

У США для опису інформаційного протиборства найчастіше використовуються такі терміни, як «інформаційні операції» («information operations») та «інформаційна боротьба» («information warfare»). «Інформаційні операції» в ході ведення воєнних дій являють собою сукупність методів впливу на інформаційні ресурси та системи противника при захисті власних інформаційних ресурсів і систем з метою захоплення інформаційної переваги, домінування в інформаційному просторі. Поняття «інформаційна

боротьба» передбачає комплексне застосування сил і засобів інформаційних операцій і збройної боротьби в загрозливий період і при веденні бойових дій.

Однією з найбільш цікавих особливостей до інформаційних операцій є те, що вони розглядаються як складова так званих операцій впливу (influence operations). Тобто ключовим поняттям є термін «вплив», який визначається, як «сила (можливість) впливати на переконання та дії будь-кого, або персона (речі), які мають таку можливість».

Безпосередньо сама операція з впливу визначається як комплекс дій, які спрямовані на зміну усвідомлення, поведінки, намірів та процесів прийняття рішень лідерів, груп або цілих народів шляхом надання відповідної інформації на когнітивному рівні. Відомі з відкритих джерел публікації свідчать, що операції з впливу містять 4 основні компоненти: цивільно-військове співробітництво, операції з безпеки, операції в засобах масової інформації (медіа-операції) та інформаційні операції.

Цивільно-військове співробітництво згідно з документами ООН визначається як необхідний діалог та взаємодія між військовими та цивільними, які спрямовані на захист та просування гуманітарних принципів, запобігання та мінімізації конфліктів та досягнення наміченої загальної мети.

Операції з безпеки спрямовані на захист інформації про план операції по впливу та її елементи, що суттєво впливає на досягнення успіху і уповільнює процес прийняття рішення противником. Безпека означає протидію усім видам розвідки в усіх сферах і здійснюється під безпосереднім керівництвом командирів на всіх рівнях (стратегічному, оперативному та тактичному).

Операції в засобах масової інформації (медіа-операції) спрямовані на забезпечення передачі цільового повідомлення і створення локальних можливостей для комунікації з місцевим населенням та лідерами. Вони є суттєвою складовою можливостей командирів оцінювати та впливати на населення.

Ключова різниця між медіа-операціями та інформаційними операціями полягає в тому, що медіа-операції не контролюють процес проходження повідомлення на відміну від інформаційних операцій, які намагаються контролювати проходження повідомлення на всіх стадіях доставки його до цільової аудиторії.

Реалізацію інформаційного компонента у сучасних воєнних конфліктах на сьогоднішній день відображає концепція мережецентричної війни, що представляє собою інфраструктурно-технологічний компонент сучасної системи управління військами і організації бою. Основу даної концепції складає завоювання безумовної інформаційної переваги над будь-яким противником на будь-якому театрі воєнних дій. У США також втілюються в життя положення доктрини глобально інтегрованих операцій, спрямованої на створення в найкоротший термін високомобільних міжвидових угруповань військ (сил).

Так, якщо у 1991 році збройні сили США в ході операції «Буря в пустелі» в Іраку на практиці реалізовували концепції «Глобальний розмах – глобальна міць» і «Повітряно-наземна операція», то в 2003 році в ході операції «Воля Іраку» воєнні дії вже велися відповідно до «Об'єднаної перспективи-2020» з широким використанням елементів мережецентричної війни.

Мережецентрична війна являє собою розгалужену мережу добре інформованих, але географічно розосереджених сил. Модель мережецентричної війни як системи, що складається із трьох решіток-підсистем: інформаційної, сенсорної та бойової. Головними компонентами цих сил є високоефективна «інформаційна решітка», що надає доступ до всієї необхідної інформації, «бойова решітка» – високоточна зброя з великою дальністю ураження цілі і маневреністю, високоефективна система управління і командування, інтегрована «сенсорна решітка», об'єднана в єдину мережу із системою ураження і системою управління і командування. Основними характеристиками мережецентричної війни є швидкість управління і принцип самосинхронізації.

Мережецентрична війна може вестися на всіх рівнях ведення бойових дій – тактичному, оперативному та стратегічному. Принципи її ведення жодним чином не залежать від географічного регіону, бойових завдань, складу і структури застосовуваних військ (сил).

Розвиток теорії і практики мережецентричних війн відбувається у більшості провідних країн світу, у тому числі США, Німеччині, Російській Федерації, Україні, у напрямку розробки сучасних комплексів автоматизованого управління всіх рівнів видів і родів збройних сил з урахуванням вимоги інтеграції всіх сил і засобів у єдиному інформаційному просторі.

Беззаперечним лідером у розвитку і застосуванні інформаційного компоненту у сучасних воєнних конфліктах є США. Одним з основних напрямків сучасної стратегії національної безпеки США, і це закріплено у відповідних доктринальних документах, на теперішній час є нарощування інформаційної потужності, головними складовими якої вважаються системи військової розвідки, зв'язку і управління.

Ключовим поняттям, введеним у звіті MR-964-OSD, є класифікація стратегічного інформаційного протиборства на перше та друге покоління. При цьому стратегічне інформаційне протиборство першого покоління розглядається поряд із традиційними засобами протиборства (ядерними, хімічними, біологічними та іншими). Підкреслюється, що воно більше орієнтовано на дезорганізацію діяльності систем управління і проводиться скоріше як забезпечення дій традиційних сил і засобів. Таке сприйняття інформаційного протиборства властиве початковому етапу осмислення проблеми. Стратегічне інформаційне протиборство першого покоління визначається як «...один з декількох компонентів майбутнього стратегічного протиборства, застосовуваний разом з іншими інструментами досягнення мети». Таким чином, поняття «стратегічне інформаційне протиборство

першого покоління» фактично увібрало в себе основні методи інформаційної війни, які США реалізують у цей час на державному і військовому рівнях і від яких не мають наміру відмовлятися в доступному для огляду майбутньому.

Подальший розвиток інформаційного протиборства відбувається відповідно до концепції «кібернетичної війни» і «мережецентричної війни», які висунуті співробітниками RAND Corporation Джоном Арквіллой і Девідом Ронфельдтом, які на цей час отримали вже досить широке поширення. Зокрема, концепція «кібернетичної війни» має на увазі, що в ході майбутніх воєнних конфліктів інформація буде відігравати вирішальну роль, а ключем до успіху буде досягнення інформаційної переваги в інформаційних та телекомунікаційних мережах та системах управління озброєнням.

В останні роки для захисту від впливу на інформаційну інфраструктуру критично важливих об'єктів наряду із створенням підрозділів кібернетичного захисту у армії, флоті, морській піхоті США створили Кібернетичне командування (USCYBERCOM). Основними завданнями цього командування є забезпечення інформаційної безпеки міністерства оборони, координація та підтримка воєнних операцій, планування, підготовка, забезпечення та управління воєнними операціями у кіберпросторі.

Аналіз опублікованих матеріалів свідчить, що в цей час фахівці міністерства оборони, розвідувального співтовариства, інших урядових відомств і представники академічних кіл США ведуть посилене відпрацювання нових концепцій і принципів будівництва, управління, організації та застосування збройних сил, які повинні прийти на зміну моделі масової мобілізації, дислокації, оснащення і використання військової потужності, притаманної сучасності.

Подальше вивчення проблеми призвело до появи поняття «стратегічного інформаційного протиборства другого покоління» (2nd Generation Strategic Information Warfare). Це поняття можна визначити як «принципово новий тип стратегічного протиборства, викликаний до життя інформаційною революцією, що вводить у коло можливих сфер протиборства інформаційний простір і ряд інших областей (насамперед економіку) і триваючий довгий час: тижні, місяці та роки». Відзначається, що розвиток і вдосконалювання підходів до ведення стратегічного інформаційного протиборства другого покоління в перспективі може привести до повної відмови від використання військової сили, оскільки скоординовані інформаційні акції можуть дозволити обійтися без цього надзвичайного заходу.

Варто відмітити, що якщо наслідки стратегічного інформаційного протиборства першого покоління ще можуть бути прогнозовані з використанням існуючих методик, то друге покоління протиборства на сучасний момент досить важко формалізувати, і існуючі методики прогнозу можуть бути застосовані до аналізу наслідків досить умовно.

Після завершення перехідного періоду до безконтактних воєн, інформаційне протиборство поступово вийде за межі виду, що забезпечує, і

стане бойовим, тобто набуде самостійного характеру серед інших форм і способів боротьби.

«Мережецентрична війна» є більш складною формою майбутнього військово-політичного конфлікту, у ході якого боротьба за інформаційне домінування сягне соціальних і національних особливостей сторін, залучених у конфлікт.

У роботах представників теоретичної групи Університету ВПС США (Air University, Maxwell Airforce Base, Alabama) Джорджа Стейна, Ричарда Шафранскі і Оуена Дженсена, прогнозується, що в майбутньому конфлікті вирішальну роль буде відігравати сама інформація (точніше, знання), що при цьому буде одночасно і зброєю, і метою, переслідуваної конфліктом. Такий тип конфлікту буде проходити у змінених до невпізнанності умовах. Передбачається, що в ході конфлікту, який принципово відрізняється від традиційного, не будуть застосовуватись не тільки традиційні системи озброєнь, але й такі високотехнологічні системи, як «цифрове поле бою» та ін., які звичайно асоціюються з веденням інформаційного протиборства. Інакше кажучи, нові інформаційні технології дозволять «боротися» безпосередньо із свідомістю противника, активно використовуючи інформаційні мережі та різні засоби масової інформації для ведення адаптованої пропаганди і створення у противника перекрученої картини світу. Власне інформаційні технології розглядаються в даній концепції тільки як засіб, що полегшує стратегічне інформаційне домінування, під яким у цьому випадку розуміється створення таких інформаційних умов, у яких дії противника в остаточному підсумку неминуче виявляться вигідними або будуть спрямовані на обслуговування інтересів протилежної сторони. Як стверджують прихильники цієї теоретичної школи, інформаційне протиборство являє собою свого роду функціональний еквівалент концепції використання повітряної сили для вирішення стратегічних завдань.