

УДК 159.9:316.6: 355.23

Олег Анатолійович МАТЕЮК,
доктор психологічних наук, професор, професор кафедри психології
та морально-психологічного забезпечення
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА СКЛАДОВА ГІБРИДНОЇ ЗБРОЙНОЇ БОРОТЬБИ

У статті розглянуто поняття “інформаційна боротьба”, “інформаційне протиборство”, “інформаційна війна” та “гібридна війна”, визначено їх ієрархічність. Виділено можливі форми, сили та засоби інформаційного впливу на ймовірного противника у мирний та воєнний час, охарактеризовано декілька специфічних рис, що властиві інформаційній війні.

Ключові слова: вплив, інформаційний вплив, інформаційна боротьба, інформаційне протиборство, інформаційна війна, гібридна війна.

Постановка проблеми у загальному вигляді. Один із авторів концепції “гібридної війни”, консультант міністерства ВМФ США Френк Хоффман визначив, що кожній епосі властиві свої специфічні форми війни. На його думку, сучасна епоха характеризується процесами гібридизації, у тому числі і у військовій сфері. Традиційні форми війни змішуються з діяльністю організованої злочинності, іррегулярними конфліктами та тероризмом [1, с. 34–39]. Для характеристики цього феномена він пропонує застосовувати поняття “гібридна війна”, яке дає змогу оперативного відобразити сутність змін предметності сучасної війни та спонукає до виокремлення нового типу воєнних конфліктів – гібридного [2], інформаційного.

Як зазначає О. Шевченко, предметом цього типу конфліктів (у його психологічній складовій) є інформація, яка, на відміну від інших ресурсів, придатна для багаторазового використання численними користувачами [3].

Більшість дослідників розуміє ці конфлікти як інформаційне протиборство, підміняючи його війною. Як відмічають М. О. Попов та А. Г. Лук'янець, корені цього слід шукати в досить вільному трактуванні самого терміна "війна". Підміна понять "інформаційна боротьба", "інформаційне протиборство" та "інформаційна війна" призводить до значної методологічної помилки, оскільки стирається різниця між інформаційною боротьбою в мирний та воєнний час, між насильницькими й ненасильницькими формами, між внутрішнім і зовнішнім аспектами інформаційного протиборства, між інформаційною зброєю та звичайними інформаційними засобами [4].

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми і на які опирається автор. Наразі, "інформаційну боротьбу" майбутнього можна визначити як "...боротьбу сторін за завоювання переваги щодо кількості, якості та швидкості добування інформації, її своєчасного аналізу й використання" [5]. Протиборство відображає антагоністичний аспект боротьби й передбачає наявність противника і протидії, унаслідок чого одна сторона досягає своїх цілей за рахунок іншої в боротьбі за спільний ресурс [6].

М. О. Попов та А. Г. Лук'янець під "інформаційним протиборством" розуміють дії, що провадяться для досягнення інформаційної переваги способом впливу на інформацію противника, його інформаційні процеси й інформаційні системи з одночасним захистом власної інформації, інформаційних процесів та інформаційних систем [4].

Термін "інформаційна війна" вживається в багатьох публікаціях: щодо явищ, які не підпадають під поняття війни (наприклад, боротьба за володіння засобами масової інформації, комп'ютерне злочинство); органів, що не уповноважені державою вести війну (наприклад, політичних, етнічних, релігійних груп, організованої злочинності, окремих індивідів, які озброєні інформаційними технологіями [5; 6]); усіх рівнів боротьби (індивідуальна, корпоративна, глобальна інформаційна війна); багатьох традиційних способів боротьби на інформаційному рівні та нетрадиційних, що виникли завдяки технологічним досягненням ХХ ст. (радіоелектронна боротьба, хакерська цифрова, кібернетична, комп'ютерна війна) [4].

Мета статті. Розглянути ієрархічність понять "інформаційна боротьба", "інформаційне протиборство" та "інформаційна війна", можливі форми, сили та засоби інформаційного впливу на ймовірного противника у мирний та воєнний час, виділити декілька характерних рис, що властиві інформаційній війні.

Виклад основного матеріалу дослідження. Поняття “інформаційна війна” трактується у вузькому та широкому сенсах. У вузькому сенсі інформаційна війна іноді трактується як польова інформаційна війна, тобто бойові дії у сфері управління військами. Сюди входять активне використання засобів розвідки, заходи з уведення супротивника в оману й оперативного маскування, психологічні операції, послідовне ураження його інформаційних систем, систем бойового управління та зв’язку, а також дії із захисту своїх власних аналогічних систем. У широкому сенсі інформаційна війна іноді трактується як великомасштабні бойові дії з переважанням інформаційної складової, що характеризуються застосуванням спеціально призначених для її ведення військових формувань і високоточної зброї. Якщо основним засобом досягнення успіху на полі бою у ХХ ст. були танки, то наразі ним стає комп’ютер. Це, у свою чергу, передбачає застосування комп’ютерних вірусів, що здатні руйнувати програмне забезпечення технічних засобів органів бойового управління і зв’язку, ініціювати зброю у системах управління та наведення високоточної зброї, тобто значно знижувати бойовий потенціал супротивника [7].

На думку О. Г. Старунського, поняття “інформаційна війна” наразі може визначатись як “безконтактна війна майбутнього”. Її полігоном став Ірак, де вперше у військовій історії в такому масштабі було застосовано високоточну зброю і були проведені комплексні інформаційно-психологічні операції [8].

О. Ю. Пермяков, В. В. Рябцев, І. Є. Вернер та інші вважають, що одним з основних типів дій, які проводитимуться в початковому періоді війни, є так звані інформаційно-ударні (інформаційні) операції, основне завдання яких – досягнення інформаційної переваги над противником (насамперед в управлінні військами) та захист інформаційного простору власних систем управління. Інформаційні операції можуть проводитись як традиційними засобами, якими є ударні компоненти, засоби радіоелектронної боротьби тощо, так і принципово новими (зброя на нових фізичних принципах – електромагнітна, психотронна, геофізична тощо), а також засобами програмно-математичного впливу на інформаційні системи противника [9].

На думку військового керівництва США, у сучасних умовах організація і ведення психологічних операцій є обов’язковим елементом участі збройних сил у збройних конфліктах різної інтенсивності, миротворчих, гуманітарних і контртерористичних операціях.

Згідно з керівними документами збройних сил США, вони здійснюють психологічні операції (в американській термінології – військові психологічні операції (Military Psychological Operations – PSYOPS) – це програми підготовки продукції та (або) програми дій, які впливають на оцінки, думки й емоції іноземних об'єктів впливу (уряди, організації, групи та індивіди) для формування їх поведінки, яка відповідає цілям зовнішньої політики США і задуму відповідних командувачів на стратегічному, оперативному і тактичному рівнях [8].

Психологічні операції є складовою інформаційних операцій, а також міжнародного суспільного інформування. Заходи психологічних операцій плануються, організовуються і здійснюються до початку, під час і після конфліктів різного ступеня інтенсивності. У минулому існували значні відмінності між трьома рівнями ведення психологічних операцій: стратегічним, оперативним і тактичним. На сьогодні таких глибоких відмінностей немає, оскільки практично неможливо локалізувати будь-яку інформаційну кампанію.

Стратегічні психологічні операції відзначаються як такі, що мають глобальні наслідки. Вони плануються, організовуються та здійснюються на державному рівні. Психологічні операції збройних сил США здійснюються для підтримки стратегічних психологічних операцій. Вони повинні гарантувати відповідність дій командувачів театрів воєнних дій у мирний і військовий час національному плану стратегічних психологічних операцій.

Оперативні психологічні операції здійснюються на всьому театрі воєнних дій для підтримки відповідних командувачів діями об'єднаної оперативної групи сил і засобів психологічних операцій або невеликих тактичних підрозділів психологічних операцій. Оперативні психологічні операції полягають у широкомасштабній трансляції телевізійних і радіо-програм, розповсюдженні газет, журналів і листівок. Концепція оперативних психологічних операцій збройних сил США передбачає передове базування невеликих підрозділів сил і засобів психологічних операцій для підтримки командувачів на театрі воєнних дій. Відповідні матеріали для них готуються для них командуванням психологічних операцій у Форті-Брегг (штат Північна Кароліна). Ця концепція (під назвою “Reachback”) здійснюється через передачу інформації за засекреченими каналами зв'язку сухопутних військ США.

Тактичні психологічні операції – це дії сил і засобів психологічних операцій, що здійснюються у певних районах із сфокусованою дією на об'єкти.

Тактичні психологічні операції проводяться невеликими підрозділами через розповсюдження листівок, трансляції телевізійних і радіопрограм, усне мовлення та наочну агітацію.

За організацію і здійснення психологічних операцій збройних сил США безпосередньо відповідає об'єднане командування спеціальних операцій збройних сил США, основним компонентом якого є командування спеціальних операцій сухопутних військ, яке в адміністративному відношенні також підпорядковується військовому міністерству. У командуванні спеціальних операцій сухопутних військ є командування зі зв'язків з цивільною адміністрацією і психологічних операцій, якому підпорядковані регулярні частини і підрозділи психологічних операцій по роботі з цивільним населенням. У їх складі налічується біля 9 500 осіб особового складу (зокрема, біля 1 300 осіб – у регулярних військах, біля 8 000 осіб – в організованому резерві).

Кожен вид збройних сил США має у своєму розпорядженні власні сили і засоби психологічних операцій. Проте основний потенціал у цій галузі (близько 85 %) зосереджений у сухопутних військах, які є єдиними із видів збройних сил, що мають регулярні частини і підрозділи психологічних операцій в мирний час і значні резервні компоненти психологічних операцій з високим ступенем мобілізаційної готовності. Основним регулярним військовим формуванням психологічних операцій сухопутних військ (і, одночасно, ядром усієї структури психологічних операцій збройних сил США) є 4-та (повітрянодесантна) група психологічних операцій у Форт-Бреггу. Її склад: штаб, штабна рота і п'ять батальйонів психологічних операцій: 1, 6 і 8-й регіональний, 9-й – тактичних психологічних операцій і 3-й батальйон підготовки та розповсюдження матеріалів психологічних операцій. Чисельність групи складає 1 135 осіб [8].

На відміну від безпосередньо військовослужбовців, у інформаційній війні також беруть участь і цивільні особи, які можуть ухвалювати стратегічні рішення як персонал так званих мозкових центрів. Їх основу складають фахівці високої кваліфікації в галузі інформаційних технологій. Саме тому швидка мобілізація особового складу збройних сил у період розвитку конфліктів втрачає свою актуальність. Натомість передбачається “мобілізація” інформаційних центрів і вступ їх у війну першими.

Вплив на ймовірного противника може здійснюватися і непрямим шляхом, наприклад, через Інтернет. У цьому випадку протилежній сторо-

ні конфлікту не завжди вдасться визначити, що відбувається несанкціонований доступ в інформаційну мережу комп'ютерного хакера або підступи ворога. Такий характер дій передбачає наявність у кожного "комп'ютерного солдата" високого рівня незалежності й ініціативи. Він у змозі працювати самостійно, без взаємодії з будь-ким, і вводити в інформаційні мережі ймовірного противника величезну кількість "баластних" відомостей. Це призводить до перевантаження каналів зв'язку ймовірного противника і блокування нормальної роботи його інформаційних систем, зниження ймовірності дій у відповідь [7].

Висновки. Згідно з результатами наукових досліджень та узагальнень сучасних наукових розробок, збройні конфлікти останнім часом спонукали виділення декількох характерних рис, що властиві інформаційній війні:

"прозорість" поля бою. Звична "лихоманка бою" поступається місцем "хірургічним" методам роботи підрозділів інформаційної війни. Оператор комп'ютера може здійснювати безперервний контроль за ситуацією, спостерігати за розташуванням своїх військ і військ ймовірного противника, за його об'єктами, концентрацією та переміщенням його сил;

загальна координація дій військ за допомогою створення єдиного каналу управління для всіх бойових підрозділів і підрозділів тилового забезпечення. Усі оперативні функції зазначених формувань (розвідка, управління, зв'язок тощо) у цьому випадку зводяться в єдину систему. Наприклад, оператор інформаційного центру, який має дані про кількість, склад і координати цілей ймовірного противника, проводить розрахунки для їх розподілу за засобами ураження, визначає кількість необхідних боєприпасів тощо;

ведення бойових дій у реальному масштабі часу, тобто негайне реагування на зміну бойової обстановки;

точність ударів, що відрізняються своєю чистотою і акуратністю, що схоже на роботу скальпеля хірурга [7].

Отже, активно поєднуючи людський і штучний інтелект, використовуючи умілу організацію, можна ввести ймовірного противника у стан інформаційного хаосу. Тобто інформаційні технології – це ключ до оволодіння рештою технологій світу, що стрімко розвиваються. А оскільки вони поступово соціалізуються, а сфери зіткнення інтересів людей усе більше розширюються, то ведення інформаційного протиборства перестає бути заняттям виключно збройних сил, які для перемоги в сучасній гібридній війні мають

бути оснащені передовими інформаційними технологіями. Їх огляд і є перспективою подальших розвідок у даному напрямку.

Список використаної літератури

1. Hoffman Frank G. Hybrid Warfare and Challenges / F. G. Hoffman // Joint Force Quarterly (JFQ). – 2009. – Issue 52, Forth Quarter. – P. 34–39.
2. Магда Є. М. Гібридна війна: сутність та структура феномену [Електронний ресурс] / Є. М. Магда. – Режим доступу : journals.iir.kiev.ua/index.php/pol_n/article/download/2489/2220
3. Шевченко О. Збройні конфлікти та шляхи їх врегулювання [Електронний ресурс] / О. Шевченко. – Режим доступу : <http://www.politik.org.ua/vid/magcontent.php3?m=6&n=37&c=690>.
4. Попов М. О. До забезпечення воєнної безпеки в умовах загрози інформаційної війни / М. О. Попов, А. Г. Лук'янець // Наука і оборона. – 1999. – № 2. – С. 37–43.
5. Information Warfare // Defense Intelligence Journal. – 1996 – Vol. 5. № 1 (Spring). – P. 2–69.
6. Бойцов М. Информационная война / М. Бойцов // Морской сб. – 1995. – № 10. – С. 70–74.
7. Дежин Е. Н. Информационная война по взглядам китайских военных аналитиков / Е. Н. Дежин // Военная мысль. – 1999. – № 6. – С. 73–76.
8. Старунский А. Г. Психологические операции вооруженных сил США на современном этапе / А. Г. Старунский // Военная мысль. – 2003. – № 11. – С. 62–71.
9. Пермяков О. Ю. Інформаційні технології в збройній боротьбі: тенденції та перспективи використання / О. Ю. Пермяков, В. В. Рябцев, І. Є. Вернер // Наука і оборона. – 2004. – № 2. – С. 38–41.

Стаття надійшла до редакції 15.07.2015

Матейюк О. А. Информационно-психологическая составляющая гибридной вооруженной борьбы

Статья посвящена рассмотрению понятий “информационная борьба”, “информационное противоборство”, “информационная война” и “гибридная война”, определено их иерархичность. Выделены возможные формы, силы и средства информационного влияния на вероятного противника в мирное и военное время; проведена характеристика нескольких специфических черт информационной войны.

Ключевые слова: *влияние, информационное влияние, информационная борьба, информационное противоборство, информационная война, гибридная война.*

Matyuk O. A. **Information and psychological component hybrid armed struggle**

The article discusses the concept of “information battle”, “information confrontation”, “information war” and “hybrid warfare”, defined by their hierarchy. Highlight possible forms capabilities informational influence on potential enemy in peacetime and wartime, described a number of specific features that are inherent in the information war.

Keywords: *impact, effect information, information struggle, confrontation news, information warfare, hybrid warfare.*