УДК 327.8

КІБЕРВІЙНА: КОНЦЕПТУАЛЬНИЙ ВИМІР

Запорожець О. Ю.
Кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

Анотація. *У добу новітніх інформаційних технологій кіберпростір стає середовищем, в якому все частіше відбувається протиборство між суб'єктами міжнародних відносин. Незважаючи на активне використання терміну «кібервійна», сьогодні не існує загальноприйнятого й вичерпного визначення цього поняття. Відправною точкою для визначення терміну «кібервійна» доцільно вважати трактування війни у класичному розумінні цього слова. З огляду на це, кібервійну можна визначити як комплекс ретельно спланованих і скоординованих суб'єктами міжнародних відносин кібератак деструктивного характеру на (критичну) інформаційну інфраструктуру супротивника, з метою послаблення позицій об'єкта впливу та досягнення політичних, економічних та військових цілей. Кібервійна є продовженням політики держави іншими засобами. Водночас вона має низку специфічних рис, що суперечать сутності війни, й обмежують її можливості у досягненні стратегічних цілей. Як наслідок, кібервійна сьогодні є здебільшого складовою інформаційного протиборства, додатковим і досить ефективним засобом психологічного тиску на супротивника. Зважаючи на динаміку розвитку і вдосконалення інформаційних технологій, у майбутньому кібервійна може досягти рівня класичної війни й кардинально змінити термінологію і методологію її ведення.*

Ключові слова: *кібервійна, кіберпростір, війна.*

В сучасному світі спостерігається постійний розвиток і вдосконалення інформаційних технологій. Під впливом інформаційних технологій змінюється сутність, форми, способи, методи і засоби ведення війни у міжнародних відносинах. Сьогодні надзвичайно популярним є термін «кібервійна». В медійному просторі цим терміном позначається широкий спектр агресивних дій в кіберпросторі, починаючи від хакерських атак на комп'ютерні мережі і закінчуючи пропагандистськими кампаніями в мережі Інтернет.

У зв'язку з цим **метою даної статті** є визначення сутності та особливостей кібервійни як складової протиборства між суб'єктами міжнародних відносин.

Кіберпростір, кіберзброя та кібервійна є об'єктом дослідження таких зарубіжних і вітчизняних науковців і практиків, як Р. Кларк, М. Лібікі, К. Коулман, Ф. Шрайер, Ш. Івен, Д. Сіман-Тов, Дж. Аркілла, В. Каберник, О. Ларіна, В.Овчинський, С. Гриняєв, М. Ожеван, Д. Дубов, О. Мережко та інші.

Термін «кібервійна» складається з двох ключових понять «кіберпростір» та «війна». Жоден з цих понять не має чіткого, загальноприйнятого визначення, закріпленого в офіційних документах на національному та міжнародному рівнях.

Слово «кібер» походить від слова кібернетика, що, в свою чергу, є похідним від грецького слова kybernetike, яке дослівно перекладається як «мистецтво управління».

За визначенням в англомовних словниках, «кібер» означає те, що відноситься до комп'ютерів, комп'ютерних мереж (зокрема мережі Інтернет) та віртуальної реальності; електронне середовище, в якому відбувається он-лайн комунікація [1, 2].

Незважаючи на активне використання терміну «кіберпростір» на сьогодні не існує загальноприйнятого визначення цього поняття.

За визначенням Міжнародного союзу електрозв'язку, кіберпростір – це фізичний і нефізичний простір, що складається з комп'ютерів, комп'ютерних систем, мереж та комп'ютерних програм, комп'ютерних даних, контенту, даних трафіку та користувачів.

У документах Збройних Сил США кіберпростір визначається як глобальний простір в межах інформаційного середовища, що складається з взаємозалежної мережі об'єктів ІТ-інфраструктури, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори та контролери [3].

В Стратегіях кібербезпеки Великої Британії та Німеччини даються такі визначення терміну «кіберпростір»: всі форми мережевої, цифрової активності, що охоплюють контент та дії в цифрових мережах; віртуальний простір всіх ІТ-систем, пов'язаних на рівні даних в глобальному масштабі. Основою кіберпростору є мережа Інтернет [3; 5].

Колишній радник Президентів США Б. Клінтона та Дж. Буша молодшого Річард Кларк в свої книзі «Кібервійна: нова загроза національній безпеці та шляхи її подолання» визначає кіберпростір як всі комп'ютерні мережі світу і все, що їх об'єднує та контролює [4].

Українські державні відомства, відповідальні за національну безпеку, трактують кіберпростір як сформоване інформаційними, телекомунікаційними та комп'ютерними системами віртуальне середовище, що функціонує як єдине ціле у глобальному масштабі, та в якому відбуваються процеси виробництва, зберігання, обробки, передачі й обміну інформацією [6].

Дослідники Національного інституту стратегічних досліджень пропонують таке визначення кіберпростору: це об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління, а також інформація, що в них циркулює [6].

Наведені визначення свідчать, що кіберпростір не обмежується мережею Інтернет, а охоплює середовище, створюване сучасними інформаційно-комунікаційними технологіями, та безпосередньо обладнання, що відноситься до ІТ-інфраструктури.

Кіберпростір є керованою системою, в якій певним чином зберігається, обробляється і передається інформація. Дана система характеризується цілісністю, взаємозалежністю компонентів, динамічністю, глобальністю, вразливістю до зовнішніх впливів, здатністю до постійного копіювання і швидкого відтворення, а також постійно зростаючою кількістю суб'єктів впливу.

Останнім часом кіберпростір перетворюється на арену боротьби між акторами міжнародних відносин. За цих умов набув поширення термін «кібервійна». Даний термін не є усталеним. Дослідниками та експертами пропонується широкий спектр визначень кібервійни, зокрема [7]:

- кібервійна – чітко скоординована цифрова атака однієї держави, спрямована на проникнення у комп'ютери та мережі іншої держави, з метою завдання шкоди або руйнування;
- кібервійна – конфлікт, що передбачає використання ворожих, незаконних атак на комп'ютери та мережі, з метою руйнування комунікацій та інших елементів інфраструктури як механізм завдання економічної шкоди або підриву системи оборони країни;
- кібервійна – застосування комп'ютерних технологій та мережі Інтернет однією державою, або за її безпосередньої підтримки, проти іншої держави, спрямоване проти її безпеки і оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави [8].

Американський дослідник Мартін Лібікі визначає два рівні кібервійни: стратегічний та оперативний. На стратегічному рівні кібервійна – це комплекс кібератак, націлених проти держави та її суспільства, з метою впливу на поведінку цієї держави. На оперативному рівні кібервійна складається з кібератак у воєнний період проти військових об'єктів та пов'язаних з військовими цивільних об'єктів [9].

Наведені визначення свідчать про відсутність консенсусу серед науковців щодо характеристик кібератак, які дали б змогу трактувати дії країни в кіберпросторі як війну.

При визначенні терміну «кібервійна» доцільно спиратись на трактування війни у класичному розумінні. В словниках та енциклопедіях війна визначається як крайня форма вирішення політичного конфлікту між суб'єктами міжнародних відносин, що регулюється принципами і нормами міжнародного права і реалізується у формі організованої боротьби сторін з використанням насильницьких методів і засобів для досягнення певних цілей.

Традиційна війна передбачає кардинальну зміну характеру відносин між учасниками, що проявляється, насамперед, у розриві дипломатичних відносин. Для традиційної війни притаманні також такі риси, як комплексність, досить чіткі часові (початок і завершення) і просторові (поле бою) обмеження, заздалегідь сплановані учасниками стратегії і тактики ведення боротьби, наявність принаймні двох учасників з конкретними політичними цілями, а також значні людські жертви та руйнування інфраструктури задіяних сторін [10; 11].

Вважається логічним, що кібервійна як своєрідна форма війни має зберігати хоча б базові характеристики традиційної війни.

З огляду на це, термін «кібервійна» можна визначити як комплекс ретельно спланованих і скоординованих суб'єктами міжнародних відносин кібератак деструктивного характеру на (критичну) інформаційну інфраструктуру супротивника, з метою послаблення позицій об'єкта впливу та досягнення політичних, економічних та військових цілей.

Подібно до класичної війни кібервійна передбачає масштабне вторгнення на «територію» супротивника, якою в даному випадку є електронні системи і мережі об'єкта впливу; наявність певного стратегічного плану; використання насильницьких засобів у вигляді шкідливого програмного забезпечення; завдання значної шкоди цим системам (тобто певні руйнування і жертви) тощо.

Кібервійна так само є продовженням політики іншими засобами й використовується для здійснення впливу на волю і можливості прийняття рішень політичного та військового керівництва супротивника.

Водночас особливості кіберпростору як середовища ведення війни породжують низку специфічних рис кібервійни. Перш за все, в кібервійні неможливо ідентифікувати «агресора», навіть коли причетність до кібератаки державних структур певних країн багатьом здається очевидною. До того ж, географічним джерелом кібератаки є, як правило, зовсім не та держава, якій така атака може бути об'єктивно вигідною [5].

По-друге, характерною рисою кібервійни є прихованість впливу і відсутність видимих руйнувань. Ця особливість пов'язана, з одного боку, з основним принципом кібервійни – експлуатацією уразливостей інформаційної інфраструктури супротивника, а з іншого – із непомітністю дій шкідливих програм, які, зазвичай, не призводять до людських жертв [7]. Як наслідок, надзвичайно важко виявити початок кібератаки (тобто момент вторгнення), застосувати превентивні заходи для попередження таких атак, а також адекватно оцінити рівень загрози і масштаб завданих збитків.

По-третє, кібервійна відрізняється надзвичайною швидкістю проведення атак, коли проміжок часу між початком «агресії» та її наслідками скорочується до мінімуму. До того

ж, шкідливі програми мають здатність швидко «розмножуватись» копіями і практично безперешкодно поширюватись у різних напрямках [4; 7].

По-четверте, для кіберзброї не мають значення кордони і відстань, а також відсутні технологічні, юридичні та інші перешкоди для проникнення в комп'ютерні системи і мережі супротивника та віддаленого управління його ресурсами. Як наслідок, кібератаки важко піддаються контролю з боку державних систем розвідки та безпеки.

На відміну від звичайної зброї, кіберзброя необов'язково знищує об'єкт впливу, а скоріше впроваджує певний набір даних і команд, що змінюють існуючі алгоритми функціонування системи й активізують потрібні реакції (від виконання бажаних дій чи невиконання певних функцій аж до самознищення).

Важливою особливістю кібервійни є також певна незавершеність або нескінченність, оскільки жоден з учасників протистояння не може напевно сказати, що супротивник припинив атаки. Крім того, кібервійна може проводитись як у мирний час, так і в період звичайної війни.

Слід зазначити, що не всі шкідливі дії в кіберпросторі можна назвати кібервійною. Так, на думку Мартіна Лібікі, до кібервійни не можна віднести шпигунство (яке може передувати кібервійні), фізичні атаки на мережі, створення радіоперешкод для пошкодження каналів радіозв'язку, а також психологічні операції (навіть якщо кібератаки мають психологічний ефект) [9].

Вважається також за доцільне відокремити кібервійну від інформаційних операцій в мережі Інтернет. Як зазначають ізраїльські дослідники, основна відмінність між інформаційною війною у кіберпросторі та кібервійною полягає в тому, що в першому випадку використовується інформація та повідомлення, представлені у зрозумілому для звичайних людей вигляді, а в другому випадку використовується мова, зрозуміла лише інженерам та експертам з інформаційних технологій [3].

Інформаційні операції в мережі Інтернет проводяться відкрито і передбачають безпосередній психологічний вплив на масову аудиторію. Кібервійни націлені на технічні об'єкти, реалізуються приховано й здійснюють опосередкований психологічний вплив на осіб, що приймають рішення та фахівців ІТ-сфери, задіяних в управлінні об'єктами інформаційної інфраструктури.

Отже, кібервійну можна розглядати як комплексне використання можливостей сучасних інформаційних технологій для впливу і віддаленого управління критично важливими ресурсами і системами супротивника.

Однак, попри потенційний масштаб і серйозність наслідків кібервійна має досить обмежені можливості у досягненні політичних, економічних та військових цілей. Як зазначає Мартін Лібікі, за допомогою кібервійни неможливо роззброїти супротивника, окупувати його територію або змінити політичний режим в країні. На його думку, кібервійна може слугувати лише засобом здійснення психологічного тиску на ворога, а також може на певний час завадити йому використовувати свої інформаційні системи та мережі належним чином [9].

Дійсно, відомі на сьогоднішній день резонансні кібератаки, такі як масовані DDoS-атаки на урядові та комерційні комп'ютерні мережі Естонії у 2007 році, впровадження вірусу Stuxnet у комп'ютерні системи ядерних об'єктів Ірану у 2009 році, зараження українських комп'ютерних мереж вірусом «Uroburos» у 2014 році тощо, спричинили лише тимчасові, локалізовані проблеми в політичній, економічній або інших сферах життєдіяльності країн-об'єктів впливу. Подібні атаки були скоріше способом попередження та психологічного тиску на іншу країну. За масштабом впливу та наслідками їх можна від-

нести до оперативно-тактичного рівня, а не стратегічного. До того ж, більшість атак не мали самостійного характеру й були інтегровані у цілий комплекс методів і засобів ведення інформаційного протиборства.

Таким чином, термін «кібервійна» є дискусійним і певним чином метафоричним. Слово «війна» в цьому терміні втрачає значною мірою той смисл, який в нього вкладався раніше. Водночас використання терміну «кібервійна» дає змогу підкреслити нові форми, способи, методи і засоби протиборства між впливовими акторами міжнародних відносин, зумовлені інтенсивним розвитком і впровадженням інформаційних технологій.

На сучасному етапі розвитку людства навряд чи можна говорити про повномасштабні кібервійни, скоріше – про кібердиверсії в рамках інформаційного протиборства та/або звичайної війни.

Однак, не виключено, що у майбутньому технологічно розвинуті країни зможуть вивести кібератаки на стратегічний рівень, подібний за рівнем організованості, комплексності, масштабності та наслідками до традиційної війни. Тоді можливо, враховуючи специфіку кіберпростору та інформаційних технологій як зброї, доведеться відмежуватися від класичних уявлень про війну й розробляти якісно іншу термінологічну базу.

Список використаної літератури

1. Oxford Dictionaries [Електронний ресурс]. – Режим доступу: http://www.oxforddictionaries.com/definition/english/cyber.
2. Dictionary.com [Електронний ресурс]. – Режим доступу: http://dictionary.reference.com/browse/cyber.
3. Even S., Siman-Tov D. Cyber Warfare: Concepts and Strategic Trends [Електронний ресурс]. – Режим доступу: http://www.inss.org.il/index.aspx?id=4538&articleid=2487.
4. Clarke R. A., Knake R. K. Cyberwar. The Next Threat to National Security and What to Do About It. – Ecco, HarperCollins, 2010. – 290 p.
5. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. – К. : НІСД, 2011. – 30 с.
6. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454/.
7. Schreier F. On Cyber warfare [Електронний ресурс]. – Режим доступу: http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.
8. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3233.
9. Libicki M. Cyberdeterrence and Cyberwar [Електронний ресурс]. – Режим доступу: http://www.rand.org/content/dam/rand/pubs/.../2009/RAND_MG877.pdf.
10. Война и мир в терминах и определениях / Под ред. Д. Рогозина. –М. : ИД «ПоРог», 2004. – 334 с.
11. Социология: Энциклопедия / Сост. А. А. Грицанов, В. Л. Абушенко, Г. М. Евелькин, Г. Н. Соколова, О. В. Терещенко. – Минск : Интерпрессервис; Книжный Дом, 2003. – 1312 с.

CYBER WARFARE: CONCEPTUAL FRAMEWORK

Zaporozhets O. Yu.

Ph.D. (Political Sciences), associate professor, Department of International Information of the Institute of International Relations Taras Shevchenko National University of Kyiv.

Abstract. *In the era of advanced information technologies the cyberspace becomes a place of confrontation between actors of international relations. Despite the increased use of the term «cyber warfare», today there is no generally accepted and comprehensive definition of this term. The reference point for the definition of the term «cyberwar» should be traditional notion of the war. In this context cyberwar can be defined as a set of destructive, thoroughly planned and coordinated by actors of international relations cyberattacks on enemy's (critical) information infrastructure in order to undermine the capacities of the target and to achieve political, economic and military goals. The cyber warfare is the continuation of politics by other means. At the same time cyberwar has a number of specific features that don't match the essence of war and therefore limit its potential in achieving strategic goals. Today the cyber warfare is an integral part of information warfare and serves as the additional and rather effective method of psychological pressure on the enemy. Taking into account the rapid development of modern information technologies, cyber warfare is very likely to reach the level of traditional war in the future and dramatically change basic concepts and methods of warfare.*

Key words: *cyber warfare, cyberspace, war.*

Referances

1. Oxford Dictionaries [Electronic resource]. – URL: http://www.oxforddictionaries.com/definition/english/cyber.
2. Dictionary.com [Electronic resource]. – URL: http://dictionary.reference.com/browse/cyber.
3. Even S., Siman-Tov D. Cyber Warfare: Concepts and Strategic Trends [Electronic resource]. – URL: http://www.inss.org.il/index.aspx?id=4538&articleid=2487.
4. Clarke R. A., Knake R. K. Cyberwar. The Next Threat to National Security and What to Do About It. – Ecco, HarperCollins, 2010. – 290 p.
5. Dubov D. V., Ozhevan M. A. Kiberbezpeka: svitovi tendencii' ta vyklyky dlja Ukrai'ny. Analitychna dopovid'. – K.: NISD, 2011. – 30 s.
6. Problemy chynnoi' vitchyznjanoi' normatyvno-pravovoi' bazy u sferi borot'by iz kiberzlochynnistju: osnovni naprjamy reformuvannja. Analitychna zapyska [Electronic resource]. – URL: http://www.niss.gov.ua/articles/454/.
7. Schreier F. On Cyber warfare [Electronic resource]. – URL: http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.
8. Merezhko O. Problemy kibervijny ta kiberbezpeky v mizhnarodnomu pravi [Electronic resource]. – URL: http://www.justinian.com.ua/article.php?id=3233.
9. Libicki M. Cyberdeterrence and Cyberwar [Electronic resource]. – URL: http://www.rand.org/content/dam/rand/pubs/.../2009/RAND_MG877.pdf.
10. Vojna i mir v terminax i opredeleniyax / Pod red. D. Rogozina. – M. : ID «PoRog», 2004. – 334 s.
11. Sociologiya: E'nciklopediya / Sost. A. A. Gricanov, V. L. Abushenko, G. M. Evel'kin, G. N. Sokolova, O. V. Tereshhenko. – Minsk : Interpresservis; Knizhnyj Dom, 2003. – 1312 s.

КИБЕРВОЙНА: КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ

Запорожец О. Ю.

Кандидат политических наук, доцент кафедры международной информации Института международных отношений Киевского национального университета имени Тараса Шевченко.

Аннотация. *В эпоху новейших информационных технологий киберпространство становится средой, в котором все чаще происходит противоборство между субъектами международных отношений. Несмотря на активное использование термина «кибервойна», сегодня не существует общепринятого и исчерпывающего определения этого понятия. Отправной точкой для определения термина «кибервойна» целесообразно считать трактовку войны в классическом понимании этого слова. Учитывая это, кибервойну можно определить как комплекс тщательно спланированных и скоординированных субъектами международных отношений кибератак деструктивного характера на (кри-*

тическую) информационную инфраструктуру противника, для ослабления позиций объекта воздействия и достижения политических, экономических и военных целей. Кибервойна является продолжением политики государства другими средствами. Вместе с тем она имеет ряд специфических черт, которые противоречат сущности войны, и ограничивают ее возможности в достижении стратегических целей. Как следствие, кибервойна сегодня является составляющей информационного противоборства, дополнительным и достаточно эффективным средством психологического давления на противника. Учитывая динамику развития информационных технологий, в будущем кибервойна может достичь уровня классической войны и кардинально изменить терминологию и методологию ее ведения.

Ключевые слова: *кибервойна, киберпространство, война.*