УДК 327.5

А.В.Слобдянюк
К. М. Писаренко

АНАЛІЗ НЕБЕЗПЕКИ КІБЕРВІЙНИ НА СУЧАСНІЙ СВІТОВІЙ АРЕНІ

Вінницький національний технічний університет

Анотація
У статті розглядаються військово-політичні та теоретичні аспекти сучасного стану та можливості подальшого розвитку практики кібервійни.
Ключові слова: кібервійна; кіберпростір; кібертероризм; кібератака; кіберзброя.

Abstract
The article describes military-political and theoretical aspects of the current state and opportunities in further developing the practice cyberwar.
Keywords: cyberwar; cyberspace; cyberterrorism; cyberattack; cyberweapons.

Вступ

Сучасний період розвитку цивілізації характеризується істотним зростанням комунікативних технологій. Сьогодні інформація та інформаційні потоки можуть використовуватися як в конструктивних, так і деструктивних цілях. Вони зробили свій вплив на характер, форми і способи ведення бойових дій. У XXI столітті війни ведуться не тільки на землі, у морі, повітрі, але і в «кіберпросторі». Проблеми «кібервійни» і «кібертероризму» є новими видами загроз для національної і міжнародної безпеки і вимагають вивчення і політологічної концептуалізації.

Метою роботи є розгляд поняття «кібервійна» й аналіз сучасного стану даної проблеми у світі.

Результати дослідження

В останній час терміни з приставкою «кібер» все частіше вживаються в міжнародно-політичному дискурсі та знаходять відображення в стратегічних доктринах не тільки держав, але і міжнародних організацій, включаючи НАТО. Термін «кібервійна» міцно увійшов у лексикон військових, фахівців з інформаційної безпеки та політиків, але серед представників експертного співтовариства немає єдиного визначення цього поняття. Американський експерт в області кібербезпеки Р. Кларк, автор книги «Кібервійна», пропонує наступне визначення: «Кібервійна – дії однієї держави з проникненням у комп'ютери або мережі іншої держави для нанесення збитків або руйнування» [1]. Вітчизняний експерт міжнародного права О. Мережко пропонує таке тлумачення: «Кібервійна – використання Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» [2]. З перерахованого вище можна охарактеризувати «кібервійну» як вид військових дій із використанням комп'ютерів та Інтернету, націлений в першу чергу на найважливіші системи функціонування та життєзабезпечення держави: електростанції, енергетичні мережі, транспортні шляхи, системи водопостачання та водовідведення тощо.

Сукупність «кібератак», які перевищують своїм загальним негативним впливом певний поріг, можуть розглядатися як початок «кібервійни». Прикладом «кібератаки», яка увійшла в історію, є виведення з ладу системи управління ППО Іраку під час операції «Буря в пустелі». Спецслужбам США вдалося заразити спеціальними вірусами комп'ютерну систему з пам'яті принтерів, придбаних для цієї системи у однієї комерційної фірми [3].

Сьогодні «кібервійна» – не далеке майбутнє, а реальність, і вона здатна захопити весь світ, оскільки комп'ютери і сервери, що беруть участь в ній, можуть перебувати в будь-якій точці планети.

Експерти з НАТО розглядають мілітаризацію Інтернету в якості одного з найголовніших і найбільш небезпечних трендів розвитку «кіберпростору». Помічник генерального секретаря НАТО з питань безпеки Сорін Дукару вважає, що успішне протистояння «кібератакам» – це один з найголовніших викликів, які кидає Альянсу сучасний мінливий світ. На думку Дукару, цілком допустимо, щоб країни НАТО здійснювали «кібернаступ» по недружніх їм країнам [4].

У багатьох країнах, таких як США, Ізраїль, Франція, Німеччина, Росія, Індія, Іран, Пакистан, Південна і Північна Корея – вже давно з'явилися структури у збройних силах, які відповідають за ведення «кібервійни». Але найбільше розвинутий в цьому питанні Китай. Німецький експерт в області «кібербезпеки» Сандро Гейко стверджує, що в Китаї на державному забезпеченні знаходяться 15 тис. штатних хакерів [5]. За даними американської компанії, пов'язаної з цифровою безпекою, Mandiant, на 2013 рік збройні сили КНР провели понад 100 «кібератак» на американські компанії та організації [6].

У 2010 році США першими створили «кіберкомандування». Китай, Іран та інші країни теж поспішили створити свої «кібервійська» із відповідними доктринами та стратегіями [7]. З 2011 року діє «Стратегія операцій в кіберпросторі міністерства оборони США», даний документ містить набір «стратегічних переваг в кіберпросторі», до яких відносяться оперативний зв'язок і можливості обміну інформацією та знаннями в сфері інформаційних технологій, у тому числі здійснення експертиз у сфері кібербезпеки. Додатковий акцент робиться на розвитку міжнародного співробітництва США в кіберпросторі в рамках міжнародної взаємодії, колективної самооборони, а також встановлення міжнародних норм, що регулюють кіберпростір.

Компанії «Center for Strategic» та «International Studies» оцінили збитки світової економіки від кіберзлочинності за 2014 рік у розмірі 445 млрд доларів [8]. Найбільший удар від незаконних дій хакерів зазнають США, Китай, Японія та Німеччина – економіки цих країн щороку не дораховуються в цілому близько 200 млрд доларів [8]. У країнах, що розвиваються збиток набагато нижче, але він буде рости в міру збільшення проникнення Інтернету в цих регіонах. За даними дослідження, світова інтернет-економіка генерує від 3 трлн доларів на рік. Приблизно 15-20% від цієї суми забирають «кіберзлочинці» [8]. Єврокомісія заявила, що за даними на 2014 рік, мінімум 1 млн користувачів Інтернету щодня піддається «кібератакам». А сукупний збиток для бізнесу від діяльності «кіберзлочинців», за різними оцінками, становить від 89 до 250 млрд євро на рік. Звичайним користувачам буде корисно знати, що у всесвітній мережі наразі існує більше 150 тис. комп'ютерних вірусів різної модифікації [9].

Висновки

Сьогодні головною темою обговорення у світі має стати регулювання ведення агресивних дій в «кіберпросторі». Дана проблема потребує якнайшвидшого вирішення, оскільки створені зразки кіберзброї вирізняються глобальною досяжністю, практично миттєвим впливом без будь-якого способу отримання попередження про її застосування. Такі характеристики дозволяють прирівняти її до стратегічних наступальних озброєнь, але розробка та застосування кіберзброї не обмежуються жодним міжнародним договором. Протистояння і суперництво держав у кіберпросторі йде вже зараз, хоча назвати це війною з наукової та міжнародно-правової точки зору було б некоректно. Очевидно, що треба виробити єдину доктрину реагування на загрози даного типу, пов'язані з використанням кіберпростору в агресивних цілях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Овчинский В. Холодная война 2.0 [Електронний ресурс] / В. Овчинский, Е. Ларина // цит. из Richard A. Clarke and Robert K. Knake» Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010) / доклад Изборскому клубу. – Режим доступу: http://dynacon.ru/content/articles/4224/

2. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3233.

3. Кибернетическая безопасность и свобода информации [Електронний ресурс]. - Режим доступу: http://mediakritika.by/article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.

4. Эдуардо Феббро Кибервойна между Россией и Западом («Pagina 12», Аргентина) [Електронний ресурс] / Э. Феббро. – Режим доступу: http://inosmi.ru/world/20140930/223333408.html.

5. Госучреждения Германии страдают от хакерских атак [Електронний ресурс]. - Режим доступу: http://www.dw.de/госучреждения-германии-страдают-от-хакерских-атак/a-16691699.

6. Пора вырабатывать правила ведения кибервойн [[Електронний ресурс]. - Режим доступу: http://www.psj.ru/press/detail.php?ID=73634.

7. Савин Л. Холодная кибервойна [Електронний ресурс] / Л. Савин // Информационно-аналитический портал Геополитика. – Режим доступу: http://www.geopolitica.ru/article/holodnaya-kibervoyna#.VUAFU9Ltmkp.

8. Мировая экономика теряет 445 млрд долларов из-за «киберпреступков» [Електронний ресурс]. - Режим доступу: http://www.dailycomm.ru/m/27316/.

9. Ковалёв Н. «Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью» [Електронний ресурс] / Н. Ковалёв // Интервью для интернет-газеты «Столетия». – Режим доступу: http://qps.ru/odR7k.

10. Слободянюк А. В. Соціальні норми та цінності як невід'ємні характеристики категорії влади [Текст] / А. В. Слободянюк // Вісник Київськ. нац. ун-ту ім. Т. Шевченка. Серія "Соціологія. Психологія. Педагогіка". - Вип. 9. - Київ, 2000. - С. 5-7.

11. Слободянюк А. В. Психологія управління та конфліктологія [Текст] : навчальний посібник для практичних та семінарських занять / А. В. Слободянюк, Н. О. Андрущенко. – Вінниця : ВНТУ, 2010. – 120 с.

Писаренко Ксенія Михайлівна — студент групи МОі-13б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: kseniia.pisarenko@best.eu.org

Науковий керівник: ***Слободянюк Анатолій Володимирович*** — канд. соц. наук, доцент кафедри суспільно-політичних наук, науковий керівник лабораторії соціологічних досліджень Вінницького національного технічного університету, Вінницький національний технічний університет, м. Вінниця

Pysarenko Kseniia M. — Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: kseniia.pisarenko@best.eu.org

Supervisor: ***Slobodianiuk Anatolii V.*** — PhD in Sociology, assistant professor of social and political sciences, scientific director of the laboratory of sociological researches Vinnitsa National Technical University, Vinnytsia National Technical University, Vinnytsia