УДК 327.5:355.4:004.42

Чернышенко С. А.,
аспирант, Одесский национальный университет имени И. И. Мечникова, г. Одесса, Украина

КИБЕРВОЙНА: ТЕОРИЯ И ПРАКТИКА

Статья рассматривает проблему кибервойны, анализируется различные авторские понятия. Рассматриваются военно – политические и теоретические аспекты современного состояния и возможности дальнейшего развития практики кибервойны. Приводятся примеры усилии различных стран в области создания соответствующих структур.

Ключевые слова: *кибервойна; киберпространство; кибертерроризм; кибератака; кибероружия.*

Рассмотрением данной проблемы посвящены работы таких зарубежных ученых, как: американцев С. Бейдлмана, Р. Кларка, француза М. Пинарда, немца С. Гейкена, поляка Л. Жанченвського, новозеландца А. Коларика, россиян Е. Ларину, Н. Коволёва, В. Овчинского, С. Матвиенко, Л. Савина. Из отечественных исследователей представляют интерес публикации Д. Дубова, А. Мережко.

Постановка проблемы. Современный период развития цивилизации характеризуется существенным ростом коммуникативных технологий. Сегодня информация и информационные потоки могут использоваться как в благоприятных, так и деструктивных целях. Они оказали свое влияние на характер, формы и способы ведения боевых действий. В XXI веке войны ведутся не только на земле, в море, воздухе но и в «киберпространстве». Проблемы «кибервойны» и «кибертерроризма» являются новыми видами угроз для национальной и международной безопасности и требуют изучения и политологической концептуализации.

Цель работы – рассмотреть понятие «кибервойна», «кибертерроризм» «киберпространство» и «кибероружие»; проанализировать современное состояние данной проблемы в и мире.

Основной материал. В последние время термины с приставкой «кибер» получили широкое употребление в международно-политическом дискурсе и нашли отражение в стратегических доктринах не только государств, но и международных организаций, включая НАТО. Проблема – отсутствие единого понятийного пространства как в научной литературе, так и международно-правовых документах, что понимать под терминами «кибервойна», «кибертерроризм», «кибератака» и «киберпространство».

Термин «кибервойна» прочно вошел в лексикон военных, специалистов по информационной безопасности и политиков, но среди представителей экспертного сообщества нет единой оценки, основная причина в том, что апеллируя к понятию «война», которое должно опираться на четкое правовое определение и не может употребляться произвольно.

Американский эксперт в области кибербезопасности Р. Кларк, автор книги «Кибервойна», предлагает следующие определения: «Кибервона – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения» [11].

Отечественный эксперт А. Мерешко предлагает следующие определения: «Кибервойна – использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической, информационной безопасности и суверенитета другого государства» [8].

Из вышеперечисленного можно охарактеризовать «кибервойну» как вид военных действий с использованием компьютеров и Интернета, нацеленный в первую очередь на важнейшие системы функционирования и жизнеобеспечения государства, таких как: электростанции, энергетические сети, транспортные пути, системы водоснабжения и водоотведения и тому подобное.

Французский исследователь, директор Института международных и стратегических отношений (IRIS) Максим Пинард, считает, что термин «кибервойна» нельзя идентифицировать с какой-то конкретно реальностью. Пинард признает самосуществования «кибератак», но это не имеет отношения к «кибервойне», так как невозможно определить двух противоборствующих противников, стремящихся нанести друг другу военный и экономический урон. По его мнению, «кибератаки» являются лишь проявлением разновидности классических методов саботажа и разрушения вражеских коммуникаций [16].

Российский специалист, научный руководитель независимого экспертно-аналитического центра «Эпоха» Игорь Попов считает, что употребления термина «кибервойна» вряд ли допустимо в официальной среде, научной литературе и военных документах. Он предлагает вместо термина «кибервойна», более логично употреблять термин «действия в киберпространстве в военных целях» или более кратко – «действия в киберпространстве» [1].

Что же касается определения «кибертерроризм» данный термин был введен в оборот в 1980 году старшим исследователем американского Института безопасности и разведки в Калифорнии Бэри Колином, чтобы обозначить террористические действия в виртуальном пространстве. Бэри Колин полагал, что о

реальном «кибертерроризме» можно будет говорить не раньше чем в первые десятилетия XXI века [14]. Но первые террористические «кибератаки» были отмечены уже в начали 1990-х годов.

В работе «Кибервойна и кибертерроризм», изданное в соавторстве двух исследователей – поляком Л. Жанченвським и новозеландцем А. Колариком – дается такое определения «кибертерроризма»: «Кибертерроризм – это мотивированные атаки, которые осуществляются субнациональными группами или тайными агентами, или отдельными индивидами против информационных и компьютерных систем, компьютерных программ или данных, результатом которых являются насилия против нонкомбатантов (в данном случай прежде всего речь идет о гражданском населении)» [20, с. 13].

Сегодня «кибертеррорист», находясь практически в любой точке земного шара, с помощью специального программного обеспечения и специальной вычислительной техники, может нанести огромный вред компьютерным сетям и информации, которая содержится в них, с целью достижения определенных идеологически-политических целей, в том числе смена власти или нарушения работы органов власти, а также системы управления жизнеобеспечения страны, саботажа, кражи военных данных или гражданских активов и ресурсов для нанесения экономического ущерба определенному государству.

Террористические организации и группы, включая такие, как «Аль-Каида» и «ИГИЛ», активно используют Интернет для связи и обмена информацией, ведения пропаганды и вербовки новых членов и организации подрывной деятельности. Например, хакеры, имеющие отношения к «ИГИЛ», 8 апреля этого года взломали сайт и аккаунт «Fecebook» французского телеканала «TV5 Monde» [15].

Американский исследователь С. Бейдлман предлагает следующие определения «кибератаки»: «Кибератака может рассматриваться как совокупность «кибероперации» с использованием противником компьютеров и информационных технологий с целью достижения определенных эффектов или целей через киберпространства» [19, с. 12].

Отечественный исследователь Д. Дубов на основе вышеизложенного определения дает следующие: «Кибератака может рассматриваться как совокупность действий противника или вражеской группы, которые желают достичь определенных негативных для объекта атаки цели и эффекта с использованием компьютерной техники в частности или возможностей киберпространства в целом, чаще всего – с использованием специально разработанных для таких заданий средств» [3, с. 23–24].

Совокупность «кибератак», которые превышают своим общим негативным влиянием определенного порогового значения, могут рассматриваться как начало «кибервойны». Примером «кибератаки», которая вошла в историю, является выведения из строя системы управления ПВО Ирака во время операции «Буря в пустыне». Спецслужбам США удалось заразить специальными вирусами компьютерную систему из памяти принтеров, приобретенных для этой системы у одной коммерческой фирмы [5].

Что же касается определения «киберпространства», обратимся к американской практике исследования проблемы «кибербезопасности», где базовое определение понятия «киберпространство» изложено в документе «Национальная военная стратегия для операции в киберпространстве» 2006 года, где «киберпространство» определяться как: «…сфера, которая характеризуется возможностью использованием электронных и электромагнитных средств для запоминания, модификации и обмена данными через системы и связанную с ними физическую инфраструктуру» [21, с. 9].

Сегодня «кибервойна» реальность, она способна захватить весь мир, поскольку участвующие в ней компьютеры и сервера могут находиться в любой точке планеты. «Кибероружие» обладает свойством «двойного действия»: наносить массовый урон и поражать избирательные цели, всё зависит от замысла нападающих. Примером может служить вирус Stuxnet, который в 2009 году «проник» в компьютерную систему ядерного объекта в городе Натанце, где происходило обогащения урана для Иранской ядерной программы. В конечном итоге вредоносной программе удалось вывести эти центрифуги из строя [7, с. 67].

Так же Stuxnet поразил систему управления на строящихся АЭС в Бушере. Компьютерная система не была подключена к интернету, но это не помогло. Вирус принес на станцию кто-то из сотрудников или иностранных рабочих и запустил в сеть, в результате ядерная программа Ирана оказалась парализована. Многие склоняются к версии о том, что вирус Stuxnet мог быть написан секретными кибернетическими подразделениями Израиля или США [17]. В 2012 году в Интернете был обнаружен вирус, который получил названия Flame, он атаковал компьютерные сети в том же Иране и на всем Ближнем Востоке. Flame способный похищать файлы с данными, удаленно изменять настройки компьютеров, включать на них микрофоны и записывать разговоры, а также копировать переписку в программах моментального обмена сообщениями [5].

Компании Center for Strategic and International Studies оценили убытки мировой экономии от «киберпреступности» за 2014 год в размере 445 млрд долларов [10]. Наибольший удар от незаконных действий хакеров приходиться на США, Китай, Японию и Германию – экономики этих стран ежегодно не досчитываются в общей сложности около 200 млрд долларов [10]. В развивающихся странах ущерб гораздо ниже, но он будет расти по мере увеличения проникновения Интернета в этих регионах. По данным исследования, мировая интернет-экономика генерирует от 3 трлн долларов в год. Примерно 15–20 % забирают «киберпреступники» [10]. Еврокомиссия заявила, что по данным за 2014 год, минимум 1 млн пользователей Интернета каждый день подвергается «кибератакам». А совокупный ущерб для бизнеса от деятельности «киберпреступников», по разным оценкам, составляет от 89 до 250 млрд евро в год. В Сети циркулирует не имения 150 тыс. компьютерных вирусов разной модификации [6].

Эксперты из НАТО рассматривают милитаризацию Интернета в качестве одного из главных и наиболее опасных трендов развития «киберпрост-

рансва». Помощник генерального секретаря НАТО по вопросам безопасности Сорин Дукару считает, что успешное противостояние «кибератакам» – это один из главных вызовов, которые бросает Альянсу меняющийся мир. По мнению Дукару, вполне допустимо, чтобы страны НАТО осуществляли «кибернаступления» в отношении недружественных им странам [16].

Направление политики НАТО в сфере «кибероборонны» было принято в январе 2008 года и одобрено главами государств в правительстве на саммите в Бухаресте в апреле этого же года. Согласно итоговой декларации саммита было утверждено положения: «обеспечить возможности для оказания поддержки стране-союзнице, по ее требованию, в противодействии кибератаке» [23]. В рамках данного процесса в Эстонии был создан Центр передового опыта в области киберзащиты, а Военный комитет НАТО утвердил Концепцию киберзащиты, предусматривающую практические программные действия. Восприятия «киберугроз» было отражено в новой Стратегической концепции обороны и обеспечения безопасности НАТО, принятой на саммите в Лиссабоне в ноябре 2010 года [5]. Согласно статьи 5 Вашингтонского договора НАТО, нападения на одного члена альянса является нападением на всех [5; 16]. Таким образом, «киберпространство» подпадает под действия данной статьи, а страны НАТО могут рассматривать любую атаку против своих информационных сетей как нападение на них в целом, а следовательно, могут осуществлять право на индивидуальную и коллективную самооборону.

В около 30 стран, таких как: США, Израиль, Франция, Германия, Россия, Индия, Иран, Пакистан, Южная и Северная Корея – уже давно появились структуры в вооруженных силах, которые ответственны за ведения «кибервойны». Но более всех продвинулся в этом вопросе Китай. Немецкий эксперт в области «кибербезопасности» Сандро Гейкен утверждает, что в Китае на государственном довольствие 15 тыс. штатных хакеров [2]. По данным американской компании, связанной с цифровой безопасностью, Mandiant, на 2013 год вооруженных силы КНР провели более 100 «кибератак» на американские компании и организации [12].

В политике США в киберпространстве отдано явное приоритетное направление, «кибероборонне» и «кибербезопасности». В документах «Стратегическое видение. Киберкомандования воздушных сил» (2008 года) и «Стратегия национальной безопасности США» (2010 года) указываюсь, что «военные должны и впредь иметь возможности защищать интересы США во всех основных сферах: на земле, в воздухе, на море, в космосе и в киберпро-странстве [18; 22, с. 22].

США первыми, в 2010 году, создали «киберкомандование». Китай, Иран и другие страны тоже поспешили создать свои «кибервойска» с соответствующими доктринами и стратегиями [13]. С 2011 года действует «Стратегия операций в киберпространстве министерства обороны США», содержание данного документа заключается в описании стратегического контекста, содержит набор «стратегических преимуществ в киберпространстве», к которым относятся оперативная связь и возможности обмена информацией и знаниями в сфере информационных технологий, в том числе осуществление экспертиз в сфере кибербезопасности. Дополнительный акцент делается на развитии международного сотрудничества США в киберпространстве в рамках международного взаимодействия, коллективной самообороны, а также установлении международных норм, регулирующих киберпространство [24]. В 2012 году в США было заложено в бюджет затраты на поддержания сетевой безопасности порядка 10,5 млрд долларов. Новые подразделение Пентагона по «кибербезопасности» будут иметь до 10 тыс. сотрудников, а рынок «кибервооружения» будет составлять не менее 100 млрд долларов [4].

На первом международном форуме по кибероборонне и кибербезопасности, прошедшего с 13 по 15 июня в рамках выставки вооружений «Евросатори-2012» в пригороде Парижа, командующий киберкомандованем сухопутных войск США генерал-лейтенант Рет Эрнандес заявил о разработке новой оперативной защиты киберпространства: «Стратегия Министерства обороны США по действиям в киберпространстве предусматривает применение новых оперативных концепций по его защите» [9].

Министерство обороны США под термином «киберпространство» понимает глобальную область информационного пространства, включающего взаимосвязанную сеть инфраструктур информационных технологий, в том числе Интернет, телекоммуникационные сети, компьютерные системы и встроенные в них процессоры и контроллеры [9]. В информационных сетях Министерство обороны США готово вести как оборонительные, так и наступательные «кибероперации» [9]. В оборонительные «кибероперации» входят оказания помощи союзным странам в создании более информированной и динамичной обороны «киберпространства». Наступательные «кибероперации» направлены на противодействие и блокирование угроз, возникающих в «киберпространстве».

Заключение. Сегодня главным вопросам в повестки обсуждения перед мировым сообществом должна стать выработка правил регулирующих ведение агрессивных действий в «киберпространстве». Данная проблема требует скорейшего разрешения, поскольку создаваемые образцы кибероружия отличаются глобальной досягаемостью, практически мгновенным воздействием без какого-либо способа получения предупреждения о его применение. Такие характеристики позволяют приравнять его к стратегическим наступательным вооружениям, но разработка и применение кибероружия не ограничиваются ни одним международным соглашением. Противостояние и соперничество государств и негосударственных акторов в киберпространстве идет уже сейчас, хотя назвать это войной с научной и международно-правовой точки зрения было бы некорректно. Очевидно, что надо выработать единую доктрину реагирования на угрозы данного типа, связанные с использованием киберпространства в агрессивных целях.

ЛИТЕРАТУРА

1. Война в киберпространстве: уроки и выводы для России [Электронный ресурс] // Круглый стол в редакции «Независимого военного обозревателя». – Режим доступа : http://nvo.ng.ru/concepts/2013-12-13/1_war.html.
2. Госучреждения Германии страдают от хакерских атак [Электронный ресурс]. – Режим доступа : http://www.dw.de/госучреждения-германии-страдают-от-хакерских-атак/a-16691699.
3. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – № 5. – С. 19–37.
4. Кибервойна: вымысел или реальность [Электронный ресурс] // Журнал Безопасность. – Режим доступа : http://www.securityinfowatch.ru/view.php?section=news&item=121.
5. Кибернетическая безопасность и свобода информации [Электронный ресурс]. – Режим доступа : http://mediakritika.by/article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.
6. Ковалёв Н. «Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью» [Электронный ресурс] / Н. Ковалёв // Интервью для интернет-газеты «Столетия». – Режим доступа : http://www.stoletie.ru/.
7. Матвиенко Ю. А. Предупредить – значит вооружить (кибертерроризм вчера, сегодня и завтра) / Ю. А. Матвиенко // Геополитика. – 2011. – Вып. VI. – С. 59–82.
8. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете) [Электронный ресурс] / А. А. Мережеко // Політичний менеджмент. – Режим доступа : http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
9. Министерство обороны США разрабатывает новые оперативные концепции защиты киберпространства [Электронный ресурс]. – Режим доступа : http://itstrateg.net/news/ministerstvo-oborony-ssha-razrabatyvaet-novye-operativnye-kontseptsii-zashchity-kiberprostranst.
10. Мировая экономика теряет 445 млрд долларов из-за «киберпреступков» [Электронный ресурс]. – Режим доступа : http://www.dailycomm.ru/m/27316/.
11. Овчинский В Холодная война 2.0 [Электронный 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 доступа : http://dynacon.ru/content/articles/4224/.
12. Пора вырабатывать правила ведения кибервойн [Электронный ресурс]. – Режим доступа : http://www.psj.ru/press/detail.php?ID=73634.
13. Савин Л. Холодная кибервойна [Электронный ресурс] / Л. Савин // Информационно-аналитический портал Геополитика. – Режим доступа : http://www.geopolitica.ru/article/holodnaya-kibervoyna#.VUAFU9Ltmkp.
14. Старостина Е. «Кибертерроризм- подходы к проблеме» [Электронный ресурс] / Е. Саростина. – Режим доступа : http://www.crime-research.ru/articles/Starostina1.
15. Хакеры из «ИГ» взломали популярный французский телеканал [Электронный ресурс]. – Режим доступа : http://news.am/rus/news/261089.html.
16. Эдуардо Феббро Кибервойна между Россией и Западом («Pagina 12», Аргентина) [Электронный ресурс] / Э. Феббро. – Режим доступа : http://inosmi.ru/world/20140930/223333408.html.
17. Юферев С. Кибервойны – войны будущего[Электронный ресурс] / С. Юферев // Военное обозрение. – Режим доступа : http://topwar.ru/3261-kibervojny-vojny-budushhego.html.
18. Air Force Cyber Command Strategic Vision [Electronic resource] / DTIC Online. – Mode of access : http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060&Location=U2&doc=GetTRDoc.pdf.
19. Beidleman W. Scott. Defining and deterring cyber war [Electronic resource] / U.S. Army War College, Carlisle Barracks. – Mode of access : http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc. pdf &AD=ADA500795.
20. Cyber Warfare and Cyber Terrorism (edited by Lech J. Janczewski and Andrew M. Colarik). – Hershey, PA: Information Science Reference, 2008. – 532 p.
21. National Military Strategy for Cyberspace Operations / Department of Defense – AccesNational Military Strategy for Cyberspace Operations [Electronic resource] / Department of Defense. – Mode of access : http://www.dod.gov/ pubs/foi/ojcs/07-F-2105doc1.pdfs mode: – http://www.dod.gov/ pubs/foi/ojcs/07-F-2105doc1.pdf.
22. National Security Strategy/White House [Electronic resource]. – Mode of access : http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
23. NATO Bucharest Summit Declaration, Art. 47, 3 April 2008 / NATO [Electronic resource]. – Mode of access : http://www.nato.int/docu/pr/2008/p08-049e.html. – Title fromscreen.
24. U.S. Department of Defense, «Strategy for Operating in Cyberspace», July 2011. – [Electronic resource] 09-28-2011– Mode of access : www.defense.gov/news/d20110714cyber.pdf.

С. О. Чернишенко,
Одеський національний університет імені І. І. Мечникова, м. Одеса, Україна

КІБЕРВІЙНА: ТЕОРІЯ ТА ПРАКТИКА

У статті розглянуто проблему кибервійни, проаналізовано різні авторські поняття. Розглянуто воєнно-політичні і теоретичні аспекти сучасного стану і можливості подальшого розвитку практики кибервійни. Наведено приклади зусилль різних країн в галузі створення відповідних структур.

Ключові слова: *кибервійна; кіберпростір; кибертерроризм; кібератака; кіберзброя.*

S. Chernyshenko,
The Odessa I. I. Mechnikov National University, Odessa, Ukraine

CYBERWAR: THEORY AND PRACTICE

The article is devoted to the problem of cyber-warfare and the analysis of different concepts of the problem. Military – political and theoretical aspects of the current state and opportunities for further development of the practice of cyber-warfare are considered. Examples of the efforts of various countries to establish appropriate structures are cited.

Keywords: *cyberwar; cyberspace; cyberterrorism; cyberattack; cyberweapons.*

Рецензенти: ***Мілова М. І.,*** д-р політ. наук, професор;
Бобіна О. В., канд. політ. наук, доцент.

Дата надходження статті до редколегії 02.05.2015