
# СТРЕЛЫ КЕНТАВРА: КИБЕРВОЙНА ПО-АМЕРИКАНСКИ

# Леонид Владимирович Савин
# Стрелы кентавра. Кибервойна по-американски

*Текст предоставлен правообладателем*
*http://www.litres.ru/pages/biblio_book/?art=57088380*
*Стрелы кентавра. Кибервойна по-американски / Савин, Л.: Кислород; Москва; 2020*
*ISBN 978-5-901635-98-8*

## Аннотация

Книга посвящена весьма эффективным элементам ведения войны в наши дни – действиям в киберпространстве. Войны «традиционных форматов» затратны, сопровождаются риском боевых потерь, встречают критику не только со стороны других стран, но и большинства граждан государства – инициатора конфликта. В отличие от них кибервойна – это не только применение Интернета с целью нанесения урона противнику, это использование коммуникаций, систем командования и управления, новейших военных технологий, средств связи, а также пропаганда и дезинформация в социальных сетях. Хотя в международном праве понятие «кибервойна» не определено, в США уже более 10 лет существует Киберкомандование, специализированные подразделения проводят виртуальные операции по всему миру, и их интенсивность возрастает.

Россия также стала целью американских кибератак, что подтверждено официально. В книге детально описаны все уровни кибервойны – юридические и политические аспекты, доктрины и стратегии, технологии и методики. Особое внимание уделено структурным подразделениям Киберкомандования США, включая беспилотники, виртуальные панели управления, искусственный интеллект, нейротехнологии и многое другое. Рассмотрены целевые заказы подрядчиков ВПК США и программы агентства DARPA. Уделено внимание практическому опыту США и НАТО по проведению кибероперациий против различных субъектов, а также действия хакеров-наемников.

*В формате a4.pdf сохранен издательский макет.*

# Содержание

# Леонид Савин
# Стрелы кентавра. Кибервойна по-американски

Савин Леонид Владимирович – известный публицист, главный редактор информационно-аналитического издания «Геополитика» и руководитель администрации Международного Евразийского движения, член Военно-научного общества.

# Введение

Кента́вр (Κένταυρος) в древнегреческой мифологии – это смертное разумное существо с телом лошади, а торсом и головой человека. Кентавры живут в глухих местах, как правило, горах и лесах. Один из героев эллинских сказаний, Геракл был воспитан кентавром по имени Хирон, который, по стечению обстоятельств, погиб от руки своего воспитанника. Образ кентавров, вероятно, возник как плод фантазии народов, еще не знавших верховой езды и впервые столкнувшихся с конными всадниками неких северных кочевых племен: скифов, касситов или тавров.

В политике образ кентавра был использован Никколо Макиавелли. В книге «Государь» он отмечал: «Вы должны знать, что бороться можно двумя способами: во-первых, законно, во-вторых, насильственно. Первый способ присущ человеку, второй – животным; но так как первого часто недостаточно, следует прибегать и ко второму. Таким образом, государю необходимо уметь превосходно пускать в ход то, что свойственно и человеку и животному. Именно этому иносказательно учили государей древние авторы, рассказывавшие о том, как Ахилла и многих других государей в древности отдавали на воспитание кентавру Хирону, чтобы он их взрастил и выучил. Что это значит иметь наставником полуживотное-получеловека, как не то, что государь должен

уметь совместить в себе обе эти природы, потому что одна без другой сделала бы его власть недолгой».

Далее у Макиавелли образ власти, представленной в виде кентавра, перенимает Антонио Грамши: наполовину человек и наполовину зверь – это необходимая комбинация согласия и принуждения.

В контексте войн и конфликтов прошлого столетия весьма примечателен следующий факт. Известный британский геополитик и автор концепции географической оси истории Хэлфорд Макиндер в 1920 г. написал докладную записку британскому правительству о необходимости создания новых независимых государств из частей Российской Империи, находясь на борту королевского крейсера «Кентавр».

В военном сообществе США «кентавром» сейчас называют гибридную команду, куда входят люди и машины. Такие человеко-машинные команды ставят новые проблемы, а военные проводят эксперименты, чтобы найти оптимальное сочетание человеческого и машинного познания. Искусственный интеллект, роботы-убийцы, специальные приложения и алгоритмы командования, манипуляции социальными сетями – все это является частью глобальной распыленной военной машины США, кентавром XXI века, который ищет новые способы принуждения других стран и народов.

Но помимо кентавров, мир американских военных населен горгонами, минотаврами, гремлинами и прочей нечи-

стью. Имена монстров и божеств из греко-романской (и не только) мифологии в Пентагоне присваивают программам, проектам и различным изделиям. В данной книге мы ознакомимся с новой интерпретацией этих существ.

И эти странные сущности имеют способность проникать сквозь границы, ведь если ранее защита национальной территории происходила по периметру границ, то киберпространство имеет иную природу. Инциденты с кибератаками на инфраструктуры различных стран, в том числе в России, показывают, что появилась новая возможность наносить удары «из ниоткуда», подвергая риску не только военных, но и гражданских лиц, проводить кампании по дезинформации, сеять панику и хаос.

О наступательных операциях в киберпространстве представители Пентагона открыто заговорили в феврале 2019 г.[1]. В то же время руководство Киберкомандования США официально подтвердило, что их специалисты провели кибератаку против российской инфраструктуры[2]. А в декабре 2019 г. глава Киберкомандования США Пол Накасоне сно-

---

[1] Cohen, Rachel S. CYBERCOM Chief: 133 Cyber Teams Will Be Insufficient as Adversaries Improve // Air Force Magazine, Feb. 14, 2019.https://www.airforcemag.com/CYBERCOM-Chief-133-Cyber-Teams-Will-Be-Insufficient-as-Adversaries-Improve/

[2] https://www.washingtonpost.com/world/national-security/us-cyber-com-mand-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.htm-l?noredirect=on

ва сообщил, что в качестве мер предотвращения вмешательства в выборы американского президента в 2020 г. они опять проведут кибератаки против Российской Федерации[3]. На сухом языке Государственного департамента США это звучало так: «При авторизации предпринимаются действия по нарушению или ухудшению способностей злонамеренных кибер-субъектов национального государства вмешиваться в выборы в США».

Генерал Пол Накасоне отметил, что в качестве целей будет выбрано «высшее руководство и российская элита, но, наверное, не сам президент Владимир Путин, потому что это будет выглядеть слишком провокационно». Издание «Вашингтон пост» в своей статье указало, что целью станут критические личные данные, которые могут представлять определенную ценность[4]. Можно предположить, что целями таких атак будут не только личные данные. Возможности Киберкомандования США, ЦРУ, Агентства национальной безопасности и других структур, которые занимаются разработкой и применением киберинструментов для различных целей, постоянно совершенствуются. Бюджет из года в год увеличивается, создаются новые подразделения и центры, про-

---

[3] Frazin, Rachel. CyberCom mulls aggressive tactics if Russia interferes in next election: report // The Hill, 12.25.19.https://thehill.com/policy/cybersecurity/475921-cybercom-mulls-aggres-sive-tactics-if-russia-interferes-in-next-election

[4] https://www.washingtonpost.com/national-security/us-cybercom-contem-plates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html

водятся специализированные конкурсы и мероприятия, на которых проходит вербовка перспективных хакеров.

Киберпространство, которое не имеет физических границ, в качестве зоны боевых действий стало активно использоваться американскими военными с 90-х гг., а теперь считается одним из доменов, где ведутся боевые действия, наряду с сушей, морем, воздухом и космосом. Более того, в современных боевых операциях киберинструменты считаются жизненно необходимыми для успешного выполнения многочисленных задач.

Киберкомандование в структуре вооруженных сил США начало работу в 2010 г., а на полную мощь вышло только к концу 2018 г. При этом все виды войск имели свои подразделения, специализирующиеся на компьютерных сетях и хакерских взломах. Теперь происходит интеграция этих структур, в том числе на международном уровне. Военнослужащие стран НАТО регулярно принимают участие в киберучениях, где условными противниками являются Россия, Китай и еще ряд стран.

За все это время в США вышло немало публикаций, посвященных кибервойне в целом и кибервойскам в частности. Начинают проводиться сравнительные исследования кибервойск разных стран[5]. Однако в отечественной литературе ощущается нехватка исследований и материалов по теме

[5] Pernik, Piret. Preparing for Cyber Conflict: Case Studies of Cyber Command. Tallinn: International Centre for Defence and Security, 2018.

кибервойны и операций в киберпространстве. Данный труд подготовлен с целью ликвидации этого недостатка.

Хотя в книге будет дан анализ в основном военной стороны вопроса, необходимо учитывать, что спецслужбы США и дипломатия также используют киберинструменты для достижения своих целей, в том числе методами, противоречащими международным правовым нормам. Поэтому по мере необходимости и в соответствующем контексте будет рассмотрена деятельность не только американских военных, но и других ведомств. Кроме того, часть военно-промышленного комплекса США также занимается созданием кибероружия, следовательно, есть необходимость освещения работы некоторых подрядчиков Пентагона, а также блока НАТО.

При структуризации материала мы применяли логический метод и разбили книгу на три части. Первая часть состоит из трех глав, и она посвящена рождению нашего существа – кентавра. В первой главе рассмотрено определение кибервойны, концепции кибермогущества, киберпространства и кибероружия. Во второй главе будут детально проанализированы доктринальные и стратегические документы США в отношении киберпространства и применения военной силы. Третья глава является своего рода продолжением второй, только в ней будет сделан осмотр не официальных документов, а рекомендаций и аналитических докладов, подготовленных научно-экспертным сообществом США. Вторая часть посвящена непосредственно кибервой-

скам – это «анатомия кентавра». Четвертая глава рассматривает историю Киберкомандования США и оценки его деятельности в стадии начального функционирования со стороны военных специалистов. В пятой главе рассмотрены киберподразделения и методы их работы в различных войсках – армии, ВВС, ВМС, Морской пехоте, Силах специальных операций, космических войсках. Шестая глава посвящена подрядчикам, которые готовят обеспечение кибермогущества американских военных. Третья часть книги описывает широкий и многолетний опыт работы американских военных – от учений и маневров до наступательных кибероперациий, как против отдельных государств, так и негосударственных акторов в лице террористических организаций. Уделяется внимание и теоретическим аспектам, связанным с киберпространством и перспективными технологиями. В седьмой главе рассмотрены различные киберучения, а также наступательные операции против различных государств. Восьмая глава посвящена теме роботов и тактике роения автоматизированных комплексов. В девятой главе говорится об искусственном интеллекте, возможном его применении в военных целях и первых программах Министерства обороны США. Десятая глава повествует о применении социальных сетей в интересах военных США, а также относительно новом феномене меметической войны. Одиннадцатая глава рассматривает нейробиологические исследования, связанные с влиянием на человеческое сознание, и примене-

ние данной науки в военных целях. Двенадцатая глава объединяет два кейса – представления американских политиков и военных об угрозах со стороны России и Китая, а также предложения о том, как им противодействовать.

Основные источники для книги – это документы Министерства обороны США, специализированные американские СМИ, освещающие деятельность вооруженных сил, целевые исследования аналитических центров, а также монографии по данной теме. Подавляющее большинство – американского происхождения. Это сделано намеренно, чтобы показать именно точку зрения США на кибервойну, ее проявления, методы ведения боевых действий в киберпространстве и потенциальных противников. Поэтому при написании мы старались избегать оценочных суждений.

# Часть 1
# Рождение кентавра

## Глава 1
## Кибервойна и ее характеристики

Лет двадцать назад первое, что могло прийти обывателю на ум при упоминании о кибервойне, – это киборги-убийцы из фантастических голливудских боевиков типа «Терминатор». Сейчас ситуация изменилась. Слово «кибервойна» стало активно использоваться в СМИ, часто не в военном значении. С этим термином связывают не только боевые характеристики и атрибуты военных действий, но еще и хакерские взломы, манипуляции, пропаганду и убеждения в социальных сетях и распространение контента через электронные СМИ.

Несмотря на спорные мнения и продолжающиеся уточнения в отношении дефиниций, ни у кого не вызывает сомнений, что США – безусловный лидер в вопросе ведения кибервойн. На ралли в штате Огайо в январе 2020 г. Дональд Трамп в эксклюзивном интервью телеканалу 13abc из Толедо сказал: «Кибер – это целая тема. Это совершенно новое поле. У нас есть потрясающие люди. Мы лучшие в кибер, чем

кто-либо еще в мире. Но мы на самом деле не использовали эту силу, этот интеллект для кибер. Мы не делали этого. А теперь делаем. И у нас, у меня есть невероятные люди, отвечающие за кибер. Если мы когда-нибудь получим удар, мы будем бить в ответ очень сильно. Мы сможем ударить очень сильно. И это новая форма войны – боевых действий, – и я думаю, что мы очень хорошо ее контролируем»[6].

Конечно же, Трамп имел в виду новую, более агрессивную стратегию кибербезопасности Белого дома и обновленную философию кибероперации Министерства обороны. В 2018 г. Министерство обороны начало следовать новой доктрине кибероперации для лучшей защиты сетей и инфраструктуры США. Но дело не только в защите. Подход, известный как «передовая оборона», позволяет кибервойскам США быть активными внутри чужой сети за пределами США, чтобы либо действовать против противников, либо предупреждать союзников о надвигающейся киберактивности, которую они наблюдают в зарубежных сетях[7].

---

[6] EXCLUSIVE: Trump talks about Iran, trade and the importance of Toledo, Jan 09, 2020.https://www.13abc.com/content/news/EXCLUSIVE-Trump-talks-about-Iran-trade-and-the-importance-of-Toledo-566863691.html

[7] Vercellone, Chiara. Trump says US 'better at cyber than anyone in the world', 13.01.2020.https://www.fifthdomain.com/dod/2020/01/13/trump-says-us-better-at-cy-ber-than-anyone-in-the-world/

# Что такое кибервойна?

«Это новый вид войны не только для тех, кто ведет ее, но и для нейтральных сторон, которые смотрят на нее. Наука и изобретения позаботились о том, чтобы не осталось ни одной страны и ни одной прослойки общества, которые не знакомы с ее ужасами, угрозами и тревогами»[8]. Эти строки были написаны в 1940 г., хотя могут быть вполне применимы и сегодня, и век спустя, в 2040 г. Автор писал о том, что благодаря радио люди уже не могут спрятаться от информации. Как предсказывал Герберт Уэллс – «голос незнакомца всегда в наших ушах». Но насколько же это выражение подходит под определение кибервойны!

Конечно, как и в случае с термином «война», который тоже имеет широкое значение (достаточно вспомнить такие понятия, как «война с наркоманией», «война с бедностью» и т. п., что подразумевает применение совершенно иных мер, чем при ведении боевых действий), есть определенная привычка воспринимать его в зависимости от контекста, то и в отношении «кибер» нужно отметить, что терминология этого слова гораздо шире, чем кажется на первый взгляд.

Следует напомнить, что понятие «кибернетика» в совре-

---

[8] Saerchinger, Cesar. Radio, Censorship and Neutrality // Foreign Affairs, January 1940.http://www.foreignaffairs.com/articles/69970/cesar-saerchinger/radio-censor-ship-an d-neutrality

менный обиход ввел ученый Норберт Винер в 1948 г., который предложил понимать под ним науку об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе. Хотя первые шаги в этом направлении были предприняты еще раньше. Американский инженер и историк Дэвид Минделл ссылается на работу Льюиса Мэмфорда «Техника и цивилизация», которая вышла в 1934 г. В ней была выдвинута теория исторических периодов, делящихся на фазы в соответствии с основными технологиями. Вначале была фаза «эотехники», когда задействовались вода, дерево и ручные изделия. Ее сменила фаза «палеотехники», в которой применялся пар, металл и фабрики. «Неотехнику» он охарактеризовал «математической точностью, физической экономикой, химической и хирургической чистотой, а также электрическим светом и новыми материалами типа бакелита». По Мэмфорду, при неотехнике автоматические процессы достигнут такой точки, когда существование рабочего будет поставлено под вопрос. Человек начнет сливаться с машиной, что приведет к драматическим эффектам. Границы между ними станут неясными. Как пишет Дэвид Минделл, у Мэмфорда наиболее важной мыслью было то, что техника связана с возможностью представлять мир посредством символов и легко ими манипулировать[9].

Теория Мэмфорда нашла отклики, так как были и другие

[9] Mindell D. Between Human and Machine: Feedback, Control, and Computing before Cybernetics. Baltimore: The John Hopkons University Press, 2002.

подобные концепции, – Гарольд Газен предложил идею сервомеханизмов, а Гарольд Блэк в 1927 г. – телефонные наушники с отрицательной обратной связью, что позволило инженерам соединить контроль и коммуникацию. Отрицательная обратная связь уже использовалась американцами во время Второй мировой войны для управления радарами и артиллерийскими установками[10].

Однако можно вспомнить и более ранние прецеденты. В 1905 г., через 9 лет после того как Маркони запатентовал беспроводной телеграф, японская морская разведка обнаружила в Цусимском проливе русскую эскадру. Сообщение об этом с помощью беспроводной связи было оперативно передано на базу, и императорский флот Японии, используя преимущество, атаковал русские корабли, что предопределило итог сражения, которое было названо первой военно-морской битвой современности[11].

Через 10 лет после Цусимского сражения американский журнал «Популярная механика» отмечал о важных новшествах, которые приобрело военное командование после

---

[10] На тему взаимосвязи человеческого персонала и техники у Минделла вышло еще две книги – «Digital Apollo: Human and Machine in Spaceflight», посвященная взаимоотношениям человека и компьютера в космической программе США «Аполлон», а также «War, Technology, and Experience aboard the USS Monitor». Baltimore: The John Hopkons University Press, 2000.

[11] Steel Ships at Tsushima – Five Amazing Facts About History's First Modern Sea Battle, 9 June, 2015.https://militaryhistorynow.com/2015/06/09/the-battleships-of-tsushima-five-amazing-facts-about-historys-first-modern-sea-battle/

открытия беспроводного телеграфа, при этом подчеркивая, что «вмешательство в беспроводную связь практически невозможно»[12]. Однако сейчас перехват, блокирование и искажение контента, который передается по беспроводной связи, является банальным фактором безопасности коммуникаций[13].

Философ Поль Вирильо в середине 80-х гг. также отмечал, что «информационная осведомленность в критических условиях, которыми, несомненно, является война, напрямую связана с выживаемостью. Принимая дарвинистскую модель эволюции, либо рассматривая примеры современной конкуренции, мы сможем обнаружить, что наиболее успешным является тот, кто обрабатывает более комплексный поток информации и поэтому способен лучше адаптироваться к окружающей обстановке. В свое время вопрос скорости обработки информации привел к появлению новой науки – кибернетической теории»[14].

Следовательно, речь идет не столько о компьютеризирова-ных сетях, сколько о широких общественных процессах, каким, собственно, и является война в разных формах сво-

---

[12] Worts, G. F. Directing the War by Wireless, Popular Mechanics, May 1915. P. 650.

[13] Савин Л. Геополитика и киберпространство: новая парадигма безопасности // Геополитика, 28.12.2017.https://www.geopolitica.ru/article/geopolitika-i-kiberprostranstvo-novaya-paradigma-bezopasnosti

[14] Virilio P. Speed and Politics. New York, Semiotext(e): Foreign Agents Services Andromeda, 1986. P. 23.

его проявления. И те же киборги, если применять концепцию Винера, это не столько роботизированные механизмы или люди с различными имплантатами, сколько управляемые персоны, через которых проходят информационные процессы. Хотя слово «киборг» впервые было использовано в исследовании НАСА по теме длительного пребывания в космическом пространстве. Это сокращение от двух слов – «кибернетический организм», что подразумевало динамическое взаимодействие органических (тело) и биомехатронных (машинных) частей[15].

В американском военном издании Signal за сентябрь 2010 г. упоминается полемика, связанная с терминологией кибервойны, где профессор Национального университета обороны США Дэниел Куэл и предложил вернуться к первоисточнику. Он совершенно верно замечает, что основа слова «кибер» заимствована из кибернетики Норберта Винера – теории контроля и коммуникации между животным (человеком) и машиной, и должна быть расчленена на три различных элемента. Во-первых, это соединение – сеть, затем контент – сообщение, и, наконец, познание – эффект, полученный от сообщения. Эта деконструкция показывает, насколько отличаются навыки человека и организаций, начиная от операций в компьютерной сети до общественных дел, которые тоже вовлечены в управление информацией, так как по-

[15] Clynes, M.E.; Kline, N.S. Cyborgs and Space. Astronautics, 1960.

следняя проходит между машиной и человеком[16].

Джон Аркилла и Дэвид Ронфельд из корпорации RAND, пожалуй, были первыми, кто заговорил о кибервойне. В своей статье «Грядет кибервойна!» от 1993 г. они указывали, что «информационная революция подразумевает усиление кибервойны, в которой ни масса, ни мобильность не будут определять результаты; вместо этого сторона, которая знает больше, сможет рассеять туман войны, но при этом погрузить в него противника, и, как следствие, получит решающие преимущества. Коммуникации и разведка всегда были важны. Как минимум, кибервойна подразумевает, что они будут востребованы еще больше и будут развиваться как дополнение к общей военной стратегии. В этом смысле она напоминает существующее понятие «информационной войны», которое подчеркивает значение коммуникации, командование, управление и разведку. Тем не менее, информационная революция может подразумевать всеобъемлющие последствия, которые требуют существенных изменений в военной организации и состоянии войск. Кибервойна может быть для XXI в. тем, чем блицкриг был для XX в. Она также может предоставить американским военным возможность увеличить силу «удара» с меньшим объемом «мышц». В то время как кибервойна на военном уровне относится к конфликту, связанному со знаниями, сетевая война относит-

[16] Campen A. Cyberspace Spawns a New Fog of War // SIGNAL Magazine, September 2010.

ся к социальной борьбе, чаще всего связанной с конфликтами низкой интенсивности со стороны негосударственных субъектов, таких как террористы, наркокартели или распространители оружия массового уничтожения на черном рынке. Обе концепции подразумевают, что будущие конфликты будут решаться в большей степени «сетями», чем «иерархиями», и что тот, кто овладеет формой сети, получит значительные преимущества»[17]. Это заявление было довольно революционным для своего времени, а правота авторов была подтверждена историей следующих десятилетий.

Следует также напомнить, что Интернет – это продукт Министерства обороны США, хотя, как указывают авторы издания Foreign Affairs, он «всегда был чем-то более значимым, чем просто местом для конфликтов и конкуренции; это основа мировой торговли и коммуникации. Тем не менее, киберпространство, как часто думают, не является просто частью общего достояния, как воздух или море. Государства отстаивают юрисдикцию, а компании утверждают, что являются собственниками физической инфраструктуры, составляющей Интернет, и данных, которые его пересекают. Государства и компании создали Интернет и несут ответственность за его поддержание. Действия, предпринимаемые в государственном секторе, влияют на частный сектор, и наоборот. Таким образом, Интернет всегда был гибридным по сво-

[17] Arquilla, John and Ronfeldt, David. Cyberwar Is Coming! RAND Corporation, 1993.https://www.rand.org/pubs/reprints/RP223.html

ей природе»[18].

Отсюда они делают вывод, что угроза кибервойны реальна, поскольку с Интернетом связаны различные виды деятельности предыдущих столетий, ради которых или с помощью которых велись войны. А сейчас «государства используют инструменты кибервойны, чтобы подорвать саму основу Интернета: доверие. Они взламывают банки, вмешиваются в выборы, крадут интеллектуальную собственность и ставят частные компании в тупик»[19].

Если на Западе говорят о войне с позиции науки, то всегда вспоминают Карла фон Клаузевица и его постулаты. Поскольку война, согласно его теории, – это продолжение политики иными средствами (что подчеркивает инструментальный характер войны), как правило, с помощью насилия, и направлено на подавление воли противника, следует задать вопрос: насколько этот аргумент может быть применим к действиям в киберпространстве?

Томас Рид считает, что «в акте кибервойны фактическое применение силы, вероятно, будет гораздо более сложной и опосредованной последовательностью причин и следствий, которые в конечном итоге приведут к насилию и жертвам. Однако такое опосредованное уничтожение, вызванное ки-

---

[18] Flournoy, Michele and Sulmeyer, Michael. Battlefield Internet. A Plan for Securing Cyberspace // September/October 2018.https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet

[19] Ibidem.

бератакой, может, без сомнения, быть актом войны, даже если насильственными были только последствия, а не средства. Кроме того, в сообществах с высокой степенью сетевого взаимодействия ненасильственные кибератаки могут привести к экономическим последствиям без насильственных последствий, которые могут превысить ущерб от менее масштабной физической атаки»[20]. При этом он утверждает, что кибератаки не соответствуют трем критериям Клаузевица – инструментальности, насилию и политическому характеру[21].

Алекс Кальво придерживается другой точки зрения, отмечая, что летальность во время конфликта не является критерием войны, и приводит в пример войну между Аргентиной и Великобританией в 1982 г. Следовательно, если кибератаки не приводят к жертвам, это еще не значит, что они не являются актом войны. По его мнению, кибервойна – это такая же война, поскольку современные технологии изменили классическое понимание войны как в западной (Клаузевиц), так и в восточной традиции (Сунь Цзы, Каутилья)[22].

Кибервойна в качестве конфликта имеет разные трактовки, хотя большинство исследователей склонны считать, что она проходит исключительно в виртуальном пространстве, а

---

[20] Rid, Thomas. Cyber war will not take place. New York: Oxford University Press, 2013. P. 3.

[21] Если насчет насилия с Томасом Ридом можно согласиться, то два вторых – политический и инструментальный характер могут вполне соответствовать киберконфликту.

[22] Calvo, Alex. Cyberwar is War // Small Wars Journal, Apr 6, 2014.

электронная война служит для создания помех в работе радиосвязи противника, вывода из строя аппаратуры, подавления сигналов различных приборов и сенсоров (либо отправки ложных сигналов) непосредственно перед началом либо во время вооруженного конфликта.

В более широком смысле «будущее боевое пространство состоит не только из кораблей, танков, ракет и спутников, но и из алгоритмов, сетей и сенсорных сеток. Как никогда ранее в истории, будущие войны будут вестись за гражданскую и военную инфраструктуру спутниковые системы, электрические сети, сети связи и транспортные системы, а также сети между людьми. Оба этих поля битвы – электронное и человеческое – подвержены манипулированию алгоритмами противника»[23]. Но вся упомянутая инфраструктура уже существует, следовательно, наличие оборонительных и наступательных возможностей в данном контексте является потенциалом кибервойны.

## Дискуссия ученых, экспертов и политиков

Одним из ранних фундаментальных исследований по кибервойне является книга Мартина Либики «Киберсдерживание и кибервойна», изданная корпорацией RAND в 2009 г.

[23] Weinbaum, Cortney and Shanahan, John N.T. Intelligence in a Data-Driven Age // Joint Force Quarterly, Vol. 90, 3rd Quarter 2018. P. 5.

Хотя Либики не определяет, что же такое кибервойна, он вводит понятия операционной кибервойны и стратегической кибервойны. Если первая представляет собой действия против военных целей через эксплуатацию их доступа или уязвимостей, то вторая является кампанией кибератак, развернутой одним субъектом против государства и его общества, главным образом, но не исключительно с целью влияния на поведение целевого государства[24]. В работе также описываются причины возникновения таких войн и их цели.

«Государства могут оказаться в состоянии кибервойны двумя путями: из-за преднамеренной провокации или эскалации. Кибервойна может возникнуть умышленно из убеждения одного государства, что оно может получить преимущества над другим, разрушая или выводя из строя информационные системы последнего (сродни стратегическим воздушным атакам во Второй мировой войне). Кибервойна может также начаться как эскалация и обратное противодействие в кризисе, которые обретут собственную жизнь (больше похожую на мобилизацию в Первой мировой войне). В любом случае начало кибервойны означает, что первичное сдерживание не удалось.

Тем не менее, отмечалось, что вторичное сдерживание – способность устанавливать линию, которую «нельзя пересечь» – все еще может быть успешным.

---

[24] Libicki, Martin C. Cyberdeterrence and cyberwar. Santa Monica: RAND Corporation, 2009. p. 117.

В любом случае следует предположить, что государства участвуют в кибервойне для достижения определенных целей, а не в качестве самоцели. Правда, нельзя предполагать, что государства являются абсолютно рациональными участниками в том смысле, что они оценивают издержки и играют беспристрастно. Многие затягивали войну, потому что воюющие стороны боялись этого, независимо от ощутимой прибыли или убытка: первый, кто выйдет из боя, потеряет лицо и окажется под воздействием чужой повестки дня. Такие мотивы вполне могут наполнить кибервойну. Просто необходимо предположить, что некоторая степень инструментальной рациональности сохраняется.

Кибервойна имеет внешние и внутренние цели. Внешняя цель является причиной кибервойны в первую очередь (например, чтобы подчинить другую сторону своей воле). Внутренняя цель связана с управлением самими боевыми действиями (их прекращением, ограничением их масштабов) и недопущением перерастания в насилие»[25].

Автор также отмечает, что в кибервойне эффекты от оружия нельзя считать независимыми от уязвимостей противника и его способности на восстановление. Обе стороны учатся одновременно. «По этой причине ранние попытки, финты и уколы могут быть информативными только на грубом уровне, чтобы проверить, является ли противник слабым или сильным оппонентом. На оперативном уровне про-

[25] Ibidem. p. 118.

тивники могут мало что узнать после этих ранних ходов, потому что в ответ на эти действия территория радикально меняется. При этом, возможно, нет веской операционной причины сразу же все оставить – внезапность имеет здесь большое операционное преимущество, – но и у любой важной стратегической причины его нет. Если кибератаки являются второстепенным явлением для обычной войны или если кибервойна считается неизбежной, стратегические киберсоображения могут быть вторичными, и операционной логики в киберпространстве может быть достаточно. Но это произойдет, если конфликт ограничен киберпространством… Стратегическая кибервойна может использоваться для того, чтобы обратить внимание других на то, что их системы не настолько надежны, чтобы они могли позволить себе участвовать в такой борьбе»[26].

Ричард Кларк и Роберт Кнэйк в 2010 г. выпустили книгу под названием «Кибервойна», которая вызвала возрождение внимания ученых к этой теме и дебаты о том, будет ли кибервойна иметь место или нет[27]. Она имела большой успех и много переизданий, и, в отличие от предыдущих научных дискуссий на эту тему, ее обсуждение происходило на фоне новостного освещения последствий вредоносной программы Stuxnet, первой кибератаки, которая, возможно, пере-

[26] Ibidem. p. 126.

[27] Clarke, Richard A. and Knake, Robert. Cyber War. The Next Threat to National Security and What to Do About It. Harper Collins Publishers, 2010.

шагнула порог применения силы, нанеся физический ущерб иранским ядерным установкам.

Подполковник ВВС США Стивен Каганин в 2011 г. опубликовал исследование о принципах войны в киберпространстве, где утверждал, что «американские военные до сих пор не разработали теорию войны в киберпространстве»[28].

В 2013 г. Дэвид Роткопф придумал синоним, который отражал глобальный характер кибервойны, – прохладная война (Cool War). Как указывал автор, «эта преемница холодной войны имеет ту же черту, которая указывает, что она не связана с горячим конфликтом на поле боя, но отличается по характеру и ожиданиям. Эта новая война является «прохладной», а не «холодной» по двум причинам. С одной стороны, она немного теплее, чем холодная, потому что происходит постоянное втягивание наступательных мер, где противники хотя и далеки от фактической войны, но регулярно пытаются нанести урон или ослабить конкурентов или получить преимущество путем ущемления суверенитета и проникновения за линию обороны. А с другой стороны, она «прохладна» в том, что включает в себя последние передовые технологии таким образом, что меняется парадигма конфликта в гораздо большей степени, чем когда-либо во времена холодной войны, которая была, в конце концов, старомодной геополитической борьбой за преимущество, при этом отвергая

[28] Cahanin, Steven E. Principles of War for Cyberspace, Air War College, 15 January 2011. p. 2.

потенциал старой школы тотальной войны.

Прохладная война в значительной степени отличается не только из-за участников или характера конфликта, но и потому, что она может вестись неопределенный срок – постоянно, даже без намеков на начало боевых действий. По крайней мере, в теории.

Прохладная война, конечно, не ограничивается лишь возможностью постоянного призрака войны с помощью кибератак. Она продвигается дальше, в продолжающуюся дискуссию об использовании беспилотных летательных средств для наблюдения и уничтожения. Все эти новые технологии облегчают способность наносить удары и доминировать над противником, не ставя человеческую жизнь или материальные ресурсы под угрозу, или дают своим традиционным вооруженным силам особые преимущества, когда они вступают в конфликт, тем самым уменьшая риск. Цель холодной войны состояла в том, чтобы получить преимущество, переходящее к следующему этапу горячей войны, или, возможно, для ее предотвращения. Цель прохладной войны состоит в том, чтобы иметь возможность наносить удары постоянно, не вызывая горячие войны…

В мире прохладной войны горячих войн будет меньше, и они будут происходить на фоне нового, другого, постоянного вида войны. Вместо того чтобы убивать противников, новые технологии предоставляют возможности просто доставлять им неприятности, снижать их способности, обманывать

их, лишая основных фондов, когда это необходимо. И это тоже, конечно, дает технологически развитым странам большое преимущество над теми, которые не имеют таких ресурсов»[29].

Подобную оценку высказал Мартин Либики, отметив, что «в то время как кибератаки теоретически могут отключить инфраструктуру или поставить под угрозу жизнь гражданских лиц, их последствия вряд ли достигнут тех масштабов, о которых предупреждают американские чиновники. Немедленный и прямой ущерб от крупной кибератаки на США может варьироваться от нуля до десятков миллиардов долларов, но последний потребует широкого отключения электроэнергии или сопоставимого ущерба. Прямые потери, вероятно, будут ограниченны, а косвенные причины будут зависеть от различных факторов, таких, как возможное поражение диспетчерских служб. Косвенное воздействие может быть больше, если кибератака вызвала большие потери доверия, в частности, в банковской системе»[30].

Бывшая чиновница Пентагона Роза Брукс в своей книге «Как все стало войной, а военные стали всем», изданной в 2016 г., пишет: «скорее всего, кибербитвы будут связа-

---

[29] Rothkopf, David. The Cool War. February 20, 2013.http://www.foreignpolicy.com/artides/2013/02/20/the_cool_war_china_cyberwar?page=full

[30] Libicki, Martin C. Don't Buy the Cyberhype // Foreign Affairs, August 16, 2013. http://www.foreignaffairs.com/articles/139819/martin-c-libicki/ dont-buy-the-cyberhype

ны с информацией и контролем: у кого будет доступ к конфиденциальной медицинской, личной и финансовой информации… кто сможет контролировать машины повседневной жизни: серверы, на которые полагаются Пентагон и Нью-Йоркская фондовая биржа, компьютеры, которые следят за работой тормозов наших автомобилей, программное обеспечение, которое запускает наши домашние компьютеры»[31].

Эта тема волновала не только политологов и государственных деятелей. В 2009 г. компания McAfee издала доклад, где говорилось, что «существуют значительные доказательства того, что государства во всем мире разрабатывают, тестируют, а в некоторых случаях используют или поощряют применение киберсредств для получения политической выгоды… Будут ли эти атаки помечены как кибершпионаж, кибердеятельность, киберконфликт или кибервойна, они представляют собой новые угрозы в киберпространстве, которые существуют за пределами области киберпреступности. Международный киберконфликт достиг высшей точки, где он представляет уже не просто теорию, но значительную угрозу… Влияние кибервойны почти наверняка выходит далеко за рамки военных сетей и касается глобальных систем связи, информации и коммуникационной инфраструктуры, на которую полагаются очень много аспектов современного общества. Поскольку так много поставлено на карту, для ми-

[31] Brooks, Rosa. How Everything Became War and the Military Became Everything: Tales from the Pentagon. Simon Schuster, 2016.

рового сообщества пришло время начать дебаты по многим вопросам, связанным с кибервойной»[32].

Профессор Джеймс Виртц из Высшей школы ВМС США отмечал, что «кибервойна – это исключительно техническая тема, в которой доминируют инженеры, математики и ученые-компьютерщики – люди, которых можно простить за то, что они сфокусированы на последнем патче, необходимом для некоторой программы, и за то, что они не думают о связи между технической эксплуатацией и великой политической стратегией. В некотором смысле проблемы, связанные с кибервойнами, часто рассматриваются не просто как нечто технически новое в военном ландшафте, но как нечто беспрецедентное в военных делах»[33].

Указывалось, что раз кибератаки пока еще не привели к гибели или увечью людей, следовательно их нельзя классифицировать как военные действия ввиду отсутствия физического насилия[34].

В международном праве вооруженные конфликты квалифицируются в соответствии с теорией первого выстрела – т. е. они начинаются с того момента, когда вооруженные си-

---

[32] Virtual Criminology Report 2009. McAfee, Inc. p. 33.

[33] Wirtz, James J. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy // Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015. p. 29.

[34] Rid, Thomas. Think Again: Cyberwar // Foreign Policy, March/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar#6

лы одной страны применяются против другой[35]. А как быть в случае, когда источник атаки трудно идентифицировать? Что, если кибервмешательство является новой формой военного обмана? Журналист Фред Каплан утверждал, что во время бомбардировки НАТО Югославии в 1999 г. подразделение Пентагона взломало системы противовоздушной обороны Сербии, чтобы создать впечатление, будто самолеты США летят с другого направления, чем на самом деле. Это говорит о том, что киберинструменты могут являться вспомогательным оружием при конвенциональных боевых действиях. 6 сентября 2007 г. ВВС Израиля нанесли ракетный удар по зданию ядерного реактора в г. Дейр эз Зор Сирийской Арабской Республики. Известно, что налету предшествовала кибератака на систему ПВО Сирии, в результате которой был выведен из строя радар возле границы с Турцией.

В 2016 г. Роберт Уорк, тогдашний заместитель министра обороны США, признал, что Соединенные Штаты сбрасывают «кибербомбы» на ИГИЛ[36] (хотя он не уточнил, что это повлекло за собой)[37]. По крайней мере, в одном случае такие нападения заставили бойцов ИГИЛ покинуть основной командный пункт и бежать на другие посты, тем самым

---

[35] Fleck, Dieter (ed.), The Handbook of International Humanitarian Law. New York City: Oxford University Press, 2008. p. 44.

[36] Здесь и далее при упоминании: организация запрещена на территории РФ.

[37] Klare, Michael T. Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. November 2019.https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-out-comes-dangerous-new-pathways-escalation

раскрывая свое местоположение. Однако когда американские военные уже проводили кибероперации против ИГИЛ в Ираке, не было единого мнения, что же считать кибервойной[38].

## От информационной войны к кибервойне

Очевидно, что за последние 30 лет происходила трансформация понимания того, как квалифицировать новые формы конфликтов. В 90-х гг. были разработаны взаимосвязанные концепции информационной войны, сетевой войны и кибервойны. В США военные начали активно использовать информацию во время войны во Вьетнаме (1955–1975 гг.), которая «подтолкнула […] к дискуссии о точных боеприпасах, дистанционных датчиках на поле боя и компьютерной обработке всевозможных логистических, административных и операционных данных»[39]. Сложность и широкое применение различных неразрывно связанных информационных систем было воспринято так, будто это увеличивает

[38] Kelly, Mary Louise. Rules for Cyberwarfare Still Unclear, Even As U.S. Engages in It. WABE, April 20, 2016.https://www.wabe.org/rules-for-cyber-warfare-still-unclear-even-as-u-s-en-gages-in-it/

[39] Warner M. Cybersecurity: A Pre-History // Intelligence & National Security 27(5), October 2012. p. 789.

хрупкость информационных потоков на поле битвы[40]. Более детальное понимание этих процессов пришло после операции «Буря в пустыне» против Ирака. Через некоторое время после ее проведения в 1993 г. вышел специальный меморандум председателя Объединенного комитета начальника штабов «Война командования и управления»[41]. В том же году ВВС США создают Центр информационной войны[42]. ВМС США учредили аналогичный центр в 1995 г.[43]. И армия США в 1995 г. организовала Центр активности по информационной войне на суше[44]. В 1996 г. вооруженные силы США вводят специальный термин «информационные операции»[45].

Ранее вместо слова «кибер» использовалось «информа-

---

[40] Rona, Thomas P. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, 1976.

[41] Chairman of the Joint Chiefs of the Staff, Memorandum of Policy no. 30: Command and Control Warfare, 1993.

[42] Air Intelligence Agency, "Air Force Information Warfare Center," Air Force Intelligence Agency Almanac, no. 97 (August, 1997a). p. 20; Kuehl, Dan. Joint Information Warfare: An Information-Age Paradigm for Jointness, Strategic Forum Institute for National Strategic Studies, no. 105, March, 1997. p. 2.

[43] Office of the Chief of Naval Operations, OPNAV Instruction 3430.26: Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 1995. p. 8.

[44] Sizer, Richard A. Land Information Warfare Activity, Military Intelligence Professional Bulletin. January-March, 1997.

[45] United States Army, Field Manual no. 100-6: Information Operations. Washington, DC: U.S. Government Printing Office, 1996.

ционная среда». Например, пять «измерений»: суша, море, воздух, космос и информация были обозначены как среды активности вооруженных сил в документе от 2000 г. «Совместное видение 2020». В нем говорится: «Силы США способны […] действовать во всех сферах – на земле, море, воздухе, космосе и информации»[46]. Информационная область «была преобразована в киберпространство, являющееся определенно более четким термином», в 2000-х гг.[47]. Предыдущие доктрины, касающиеся того, что было определено как информационные операции, подчеркивали необходимость защиты собственных информационных систем и недопущения, деградации или разрушения возможностей соперников в сфере командования и управления, например, с помощью «компьютерных вирусов»[48].

---

[46] The Joint Chiefs of Staff, Joint Vision 2020: America's Military – Preparing for Tomorrow // Joint Force Quarterly 2000, 57–76. p. 61.

[47] The Chairman of the Joint Chiefs of Staff, The National Military Strategy for Cyberspace Operations. Washington, DC: Office of the Chairman, 2006. p. 3.

[48] Office of the Chief of Naval Operations, OPNAV Instruction 3430.26: Implementing Instrution for Information Warfare/Command and Control Warfare (IW/C2W). Washington, D.C.: Department of the Navy, 1995; United States Army Training and Doctrine Command, TRADOC Pamphlet 525-69: Military Operations Concept for Information Operations. См. также: David and McKel-din III (eds.), Ideas as Weapons: Influence and Perception in Modern Warfare. pp. 7-12 and pp. 27–34; Arquilla and Borer (eds.), Information Strategy and Warfare: A Guide to Theory and Practice. pp. 56-230; Macdonald, Propaganda and Information Warfare in the Twenty-First Century. pp. 6-117; Ventre, Information Warfare.; Hirvela, "Discovering how Information Warfare Distorts the Information Environment.".; Cordray III and Romanych, "Mapping the Information Environment.

Доктрина информационных операций обозначала эти возможности следующим образом: «Основные возможности для проведения [информационных операций] включают, но не ограничиваются психологическими операциями, операциями по обеспечению безопасности, военным обманом, электронной войной и физическим нападением/уничтожением, и могут включать в себя атаки на компьютерные сети»[49]. В более поздних документах было удалено слово «могут» и стало четко указываться, что информационные операции имеют подмножество действий, известных как «операции в компьютерной сети» (computer network operations, CNA)[50].

В конце 1990-х и начале 2000-х гг. различные команды, которые существовали ранее, были объединены и переименованы в команды по информационным операциям. В первую очередь старые коллективы по информационной войне, которым было поручено шифрование, электронная война, психологические операции и операции по обеспечению безопасности, были объединены в «новые» команды[51].

---

[49] The Joint Chiefs of Staff, Joint Publication 3-13: Joint Doctrine for Information Operations. pp. I-9, I-10.

[50] United States Department of Defense, Information Operations Roadmap. Washington, D.C.: Department of Defense, 2003; United States Marine Corps Combat Development Command, A Concept for Information Operations. Quantico: United States Marine Corps, 2002; The Joint Chiefs of Staff, Joint Publication 3-51: Joint Doctrine for Electronic Warfare. Washington, D.C.: The Joint Chiefs of Staff, 2000.

[51] Navy Information Operations Command. NIOC Norfolk's History, United

В 2010-х гг. эти довольно произвольные доктринальные взгляды были скорректированы. Отношения и интеграция информационных операций с другими военными возможностями были сформулированы следующим образом: «информационные операции говорят не о наличии отдельных возможностей, а скорее об использовании этих возможностей в качестве множителя силы для создания желаемого эффекта. […] Есть много военных возможностей, которые способствуют проведению информационных операций и должны быть приняты во внимание в процессе планирования»[52].

Нужно отметить, что эта доктрина была написана задолго до того, как беспроводные сети, полностью зависящие от электромагнитного спектра, стали обычным явлением. Эта «растущая распространенность беспроводных [Интернет] и телефонных сетей в оперативной среде создали широкий спектр возможностей и уязвимостей, когда [электронная война] и тактика [операций в компьютерной сети], методы и процедуры используются синергетически»[53]. Эти потенциальные синергетические преимущества и взаимозави-

---

States Navy. public.navy.mil/fcc-c10f/niocnorfolk/Pages/NIOCNorfolkHistory. aspx; United States Army Intelligence and Security Command, The INSCOM Story. INSCOM History Office. inscom.army.mil/organisation/History.aspx; 688th Cyberspace Wing, A Brief History of the 688th Cyberspace Wing. Joint Base San Antionio-Lackland: 688th Cyberspace Wing History Office, 2016.

[52] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. 3–14.

[53] The Joint Chiefs of Staff, Joint Publication 3-13.1: Electronic Warfare. Washington, D.C.: The Joint Chiefs of Staff, 2007. pp. x-xi.

симости привели к созданию набора операций, называемых киберэлектромагнитная деятельность (cyber electromagnetic activities, CEMA)»[54].

2011 г. стал переломным в отношении того, как американские военные стали воспринимать киберпространство. 15 ноября 2011 г. Минобороны США в форме категорического предупреждения заявило, что США оставляет за собой право ответных мер с позиции военной силы против кибератак и наращивает свои технологические возможности для того, чтобы точно определить сетевых злоумышленников. «Мы сохраняем право на применение всех возможных средств – дипломатических, международных, военных и экономических – для защиты нашей нации, наших союзников, наших партнеров и наших интересов»[55]. Было сказано, что «США необходимо знать кибервозможности других государств для того, чтобы обороняться от них и увеличить свои возможности для отражения кибератак, которые могут возникнуть»[56]. Также говорилось, что Национальное агентство безопасности обеспечит соответствующую поддержку Киберкомандо-

---

[54] Field Manual 3-12: Cyberspace and Electronic Warfare Operations. Department of the Army, Washington, D.C. 05 February 2013.

[55] U.S. reserves right to meet cyber attack with force. Nov 15, 2011. http:// www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE-7AF02Y20111116

[56] DoD Cyberspace Policy Report. Nov. 2011. p. 3. http:// www.defense.gov/ home/features/2011/0411_cyberstrategy/docs/NDAA%20Section %20934%20 Report_For%20webpage.pdf

ванию США, что позволит Министерству обороны планировать и осуществлять кибероперации.

Вице-председатель компании Booz Allen Hamilton и бывший директор по национальной разведке Национального Агентства Безопасности в администрации Дж. Буша Майк МакКоннэлл в 2012 г. сказал, что США уже осуществляют кибератаки на другие государства с помощью компьютерных сетей[57].

## Власть над киберпространством

У любой войны есть театр военных действий. В вооруженных силах США пространством, где ведутся боевые действия, согласно документу от 2000 г. считаются суша, воздух, море, космос и информация[58]. В 2006 г. информационное пространство было заменено на киберпространство и признано более удачным термином[59].

Таким образом, киберпространство – пятое измерение, следующее после суши, моря, воздуха и космического пространства[60].

---

[57] US launched cyber attacks on other nations. 24 January, 2012. http://rt.com/ usa/ news/us-attacks-cyber-war-615/

[58] The Joint Chiefs of Staff, Joint Vision 2020: America's Military – Preparing for Tomorrow // Joint Force Quarterly 2000, 57–76. p. 61.

[59] The Chairman of the Joint Chiefs of Staff, The National Military Strategy for Cyberspace Operations. Washington, DC: Office of the Chairman, 2006. p. 3.

[60] Kuehl, Dan. From Cyberspace to Cyberpower: Defining the Problem, in

Специалисты ВВС США, в частности майор Бёрдуэлл и подполковник в отставке Роберт Миллз, на страницах издания Air Power акцентировали, что киберпространство хоть и является уникальным, но в качестве места силового присутствия и применения систем С2 (командование и управление) киберпространство аналогично другим зонам ведения боевых действий. «Следовательно, мы можем применить уроки воздушных и космических операций для киберпространства и рекомендуем Киберкомандованию адаптировать нашу доктрину для внедрения в кибервойсках», – указывали они[61].

Генри Киссинджер отмечал, что «киберпространство бросает вызов всему историческому опыту»[62]. Он предположил, что «рабочая схема для организации глобальной киберсреды будет являться императивом. Она не должна ограничиваться только одной технологией, но являться процессом самого определения, который будет помогать лидерам понимать опасности и последствия… Дилемма таких технологий состоит в том, что невозможно установить правила поведения без всеобщего понимания, как минимум, некоторых ключевых возможностей. Но очевидно, что эти возможности большинство из акторов будут раскрывать неохотно. США об-

Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: Potomac Books, 2009. p. 4.

[61] Birdwell B., Mills R. War Fighting in Cyberspace. Evolving Force Presentation and Command and Control // Air Power. Spring 2011. p. 35.

[62] Kissinger, Henry. World Order. Penguin Books Limited, 2014. p. 196.

виняли Китай в краже секретов через киберпроникновения, аргументируя, что уровень активности беспрецедентен. Но готовы ли США раскрыть свои собственные успехи по кибербразведке?»[63].

Поэтому, как указывает Киссинджер, асимметрия и близкие по духу вещи мирового беспорядка выстраиваются на отношении между кибермогуществом как в дипломатии, так и в стратегии. Внимание многих стратегических соперников сдвигается с физической сферы в информационную, где происходит сбор и анализ данных, проникновение в сети и психологические манипуляции. Отсутствие формулирования каких-либо правил международного поведения приводит к кризису, который появляется из внутренней динамики системы.

Поскольку киберпространство является одновременно средой для конфликта и его инструментом, возникает вопрос власти и принуждения в этом пространстве. Если классическая геополитика использует понятия Морского могущества (Sea Power) и Сухопутного могущества (Land Power), а позже появилось господство в воздухе и господство в космосе, с недавнего времени заговорили и о новом могуществе или господстве в киберпространстве (Cyber Power). США придают этому особое значение. Скотт Тимке считает, что для поддержания американского могущества Вашингтоном сейчас применяются цифровые технологии. Одним из стра-

[63] Ibidem. p. 198.

тегических инструментов и является цифровое принуждение[64].

Офицер ВВС США Роберт Ли указывает, что «кибермогущество будет таким же революционным для войны, как и военно-воздушные силы, но текущая векторизация этой области будет определять, какая нация достигнет кибергосподства и с какой целью. На раннем этапе появления киберпространства Соединенные Штаты, в первую очередь, рассматривали кибермогущество как средство налаживания широких возможностей командования и управления через боевые зоны. Киберпространство сосредоточено на связи, да и оперативный успех зависел от поддержания линий коммуникации. Так как эта область расширялась, она взяла на себя дополнительные роли по обеспечению поддержки сил традиционных военных операций, в то время как эксперты исследовали другие роли – это процесс, который произошел на самом высоком уровне секретности. Многие из первых лидеров киберпространства поняли, что кибератривы предлагают ряд вариантов для атаки, защиты и эксплуатации, которые никогда прежде не были возможны для военачальников. В довольно взаимосвязанном мире, где существенные достижения в области технологии были обычным делом, возможности и оружие в киберпространстве стали еще более впе-

[64] Timcke, Scott. Capital, State, Empire: The New American Way of Digital Warfare. London: University of Westminster Press, 2017.

чатляющими»[65].

Предполагается, что кибермогущество может быть использовано для получения преимуществ внутри киберпространства, но киберинструменты также могут работать для создания преимущественных выгод в других сферах за пределами киберпространства. Джозеф Най-младший обосновывает этот аргумент динамикой американского могущества. По аналогии с морским могуществом, которое относится к применению ресурсов в морских пространствах, для того чтобы выигрывать морские сражения, контролировать важные морские пути типа проливов и демонстрировать присутствие в морском пространстве, оно также включает в себя возможности использовать океаны для того, чтобы влиять на сражения, торговлю и мнения на самой суше… Развитие воздушных сил при Франклине Рузвельте было жизненно важным во время Второй мировой войны. А после появления межконтинентальных ракет, а также спутников для связи и разведки в 1960-х гг., началось теоретизирование о специфическом пространстве господства в воздухе[66]. Следовательно, киберпространство также имеет потенциал для проекции через него власти той или иной державы.

Най определяет кибермогущество как «способность по-

---

[65] Lee, Robert M. The Interim Years of Cyberspace.// Air & Space Power Journal, January-February 2013. p. 58.

[66] Birdwell B., Mills R. War Fighting in Cyberspace. Evolving Force Presentation and Command and Control. Air Power. Spring 2011. p. 4.

лучать предпочтительные результаты за счет использования электронных взаимосвязанных информационных ресурсов киберсферы. Кибермогущество может использоваться для получения предпочтительных результатов в киберпространстве, или оно может использовать киберинструменты для получения предпочтительных результатов в других областях вне киберпространства»[67].

Подобное мнение высказывалось еще в 1995 г., когда была дана экспертная оценка, что «глобальное могущество способно выдерживать риск или поражать какие-либо цели в любом месте, вести проектировку быстро и точно, часто имея решающие последствия. Доставка глобального могущества в любую среду боевых действий требует командования и управления в киберпространстве, от которых зависят современные американские военные возможности»[68].

Как мы видим, киберпространство открывает дополнительные возможности для ведения войны, причем их комбинация может быть различна. «Кибероперации – это просто еще один набор инструментов из арсенала командира»[69].

Если открываются возможности для США, то они могут открыться и для других стран. Из-за этого «парадокс, с

---

[67] Nye, Joseph S. Jr. The Future of Power. New York: Public Affairs, 2011. p. 123.

[68] Endsley, Mica R. Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors 37, no. 1 (1995): 32–64.

[69] Trias, Eric D. and Bell, Bryan M. Cyber This, Cyber That. . So What? // Air & Space Power Journal. Spring 2010. p. 91.

которым сталкивается Министерство обороны, заключается в том, что асимметричное преимущество, предоставляемое применением инструментов цифрового века, может легко стать асимметричным недостатком. То есть само преимущество, получаемое благодаря скорости, возможности соединения и нелинейным воздействиям, полученным за счет использования преимуществ киберпространства, может быть нарушено или отклонено с помощью встречных рычагов, доставляемых противниками через одну и ту же среду»[70]. Цифровой век изменил геометрию поля битвы. На самом деле изменения в войне за последние несколько десятилетий были настолько глубокими, что многие центральные принципы военной теории, сохраняющиеся в течение нескольких поколений или даже тысячелетий, более неприменимы – в некоторых случаях они действительно опасны. Возможно, лучшая иллюстрация этого момента – признание того, что поле битвы больше не связано физически или не описывается в узкой рамке традиционных кинетических эффектов. Скорость, связность и нелинейный характер среды, в которой должны работать бойцы, коренным образом меняет метод того, как нужно думать о целях и угрозах, с которыми мы сталкиваемся. Геометрия, которая использовалась на протяжении всей истории, может больше не применяться[71]. А

[70] Allardice, Robert and Topic, George. Battlefield Geometry in our Digital Age. From Flash to Bang in 22 Milliseconds. PRISM 7, No. 2, 2017. p. 79.

[71] Ibidem. p. 80.

«взаимозависимость кибердомена со всеми остальными доменами представляет значительные профили риска и предполагает необходимость продумать эту концепцию обеспечения миссии с другой точки зрения, чем нынешняя и историческая «трехмерная война»[72].

Кибероперации могут проводиться во всех областях ведения боевых действий: в воздухе, космосе, киберпространстве, на суше и море. В предыдущие годы оперативные доктрины для киберпространства оставались довольно сырыми (подробно эти доктрины будут рассмотрены в отдельной главе), поэтому доктрины для воздушного пространства и космического пространства оставались актуальными и применимыми к сфере киберпространства. Теперь же у американских военных есть четкое определение киберпространства – это «глобальный домен в информационной среде, состоящий из взаимозависимой сети информационных технологий и данных резидентов, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные процессоры и контроллеры»[73]. А получив над ним контроль, Пентагон будет претендовать уже на глобальное доминирование.

Поскольку кибермогущество может быстро и особым образом поражать сети и информационные системы по всему

---

[72] Ibidem. p. 82.

[73] The Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms. Washington, D.C.: Joint Chiefs of Staff, 2017. p. 58.

миру, размывая линию боевого сражения, эта особенность в сочетании с его разрушительной силой порождает страх перед его возможностями среди населения – такой же сильный, как и от террористических атак[74]. Следовательно, в США считают, что недооценивать его силу влияния на общественное мнение и политику будет серьезной ошибкой. Даже если рассматривать исключительно военную сторону киберконфликтов, они сильно отличаются от войны на суше, море, в воздухе и космосе. «Свобода действий – это характеристика превосходства в киберпространстве… Приблизительным резюме для превосходства в киберпространстве может быть «свобода действий в течение атаки» (т. е. возможность действовать даже во время атаки и после нее)»[75].

Но есть и другая точка зрения, согласно которой, наоборот, кибервозможности применительно к конфликтам «смягчают» их природу и минимизируют ущерб как противника, так и затраты атакующей стороны. Профессор Военно-морской школы США Дороти Деннинг считает, что «если вы можете достичь того же эффекта с кибероружием вместо кинетического оружия, часто этот вариант этически предпочтительнее… Если операция нравственно оправдана, то кибермаршрут, вероятно, предпочтительнее, потому что он вы-

---

[74] Lee, Robert M. The Interim Years of Cyberspace // Air & Space Power Journal, January-February 2013. p. 63.

[75] Trias, Eric D. and Bell, Bryan M. Cyber This, Cyber That. . So What? // Air & Space Power Journal. Spring 2010. p. 96–67.

зывает меньше вреда»[76].

Также отмечалось, что «успех согласно традиционной парадигме войны не обязательно эквивалентен успеху в киберсфере… Гений Клаузевица может быть неприменим для войны в киберпространстве. «Парадоксальная троица» войны по Клаузевицу состоит из насилия, шанса и субординации политики. Физическое насилие, присущее войне, не существует в киберпространстве. В киберсфере американские военные сосредоточены на элементах господства и отрицания, основанных на успехе нынешних доктрин в отношении воздушного пространства, суши и моря, вместо того чтобы рассматривать более адаптивные подходы, которые могли бы гарантировать больший успех, а также большие риски»[77].

Наконец, киберпространство не имеет в себе и через него не может применяться насилие в традиционном смысле. Разрушение может происходить, но оно не постоянно и восстановимо. И оно не эквивалентно смерти или поражению… «В киберсфере виртуальная реальность замещает физическую среду, а традиционная структура знания смещается. Киберсреда высвобождает человечество из физической реальности, ассоциируемой *с* традиционной войной. В кибер-

---

[76] Stewart, Kenneth. Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare. America's Navy, 6/4/2013. http://www.navy.mil/submit/display. asp?story_id=74613

[77] Alfonso, Kristal L. M. A Cyber Proving Ground. The Search for Cyber Genius // Air & Space Power Journal. Spring 2010. p. 61

пространстве смерть не является финалом»[78].

## Дебаты по поводу угроз и безопасности

В экспертном сообществе США существовал довольно широкий спектр мнений в отношении того, что считать кибервойной и киберугрозами и как на них реагировать. Известный специалист по сетевым войнам Джон Аркилла указывал, что «подвиги кибервойн малого масштаба (Аркилла приводит в пример атаки на правительственные сайты Эстонии в 2007 г. и соответствующую инфраструктуру Грузии в августе 2008 г., приписывая данную инициативу российской стороне, а также инцидент с вирусом Stuxnet на иранских ядерных объектах. – *Прим. авт.)* в конечном итоге могут достичь больших размеров, учитывая явные уязвимости передовых военных и различных систем связи, которые с каждым днем все больше охватывают мир. Вот почему я думаю, что кибервойнам суждено сыграть более заметную роль в будущих войнах»[79].

Поскольку консенсуса в отношении кибервойны не было ни среди военных, ни среди политиков, в США начали использовать терминологию киберугроз и кибероперацій.

Отмечалось, что «кибероперации могут быть проведены

---

[78] Ibidem. p. 64–66.

[79] Arquilla J. Cyberwar Is Already Upon Us // Foreign Policy, March/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_ upon_us

во всех областях ведения боевых действий: в воздухе, космосе, киберпространстве, на суше и море. Кроме того, несмотря на незрелость оперативных доктрин для киберпространства, доктрины для воздуха и космического пространства остаются актуальными и применимыми к сфере киберпространства… Хотя кибероперации имеют различные способы достижения эффектов, с точки зрения ВВС они похожи на другие воздушные и космические операции»[80]. А поскольку кибероперации применимы везде, то возникают новые категории.

«Контрвоздух, контркосмос, контрсуша, контрморе – операции, осуществляемые для достижения желаемой степени превосходства в данной области и в то же время направленные на недопущение использовать те же области врагом. Киберзадачи для данных сфер состоят в манипулировании базами данных, образами, контролем и энергией систем вооружений… Мы предлагаем следующее определение контркиберпространства (countercyberspace): функция, состоящая из операций для достижения и поддержания желаемого уровня превосходства в киберпространстве путем уничтожения, деградации или разрушение возможностей врага по использованию киберпространства…

Превосходство в воздухе и космическом пространстве характеризуется свободой действий и спонтанной свободой от

---

[80] Trias, Eric D. and Bell, Bryan M. Cyber This, Cyber That. . So What? // Air & Space Power Journal. Spring 2010. p. 91.

атаки. Свобода действий – это характеристика превосходства в киберпространстве… Приблизительным резюме для превосходства в киберпространстве может быть «свобода действий в течение атаки» (т. е. возможность действовать даже во время атаки и после нее)»[81].

Аркилла указывал, что есть возможность выработать определенный код поведения. Например, не применять кибератаки против исключительно гражданских объектов. По крайней мере, такая договоренность возможна между государствами. Некоторые теневые сети, т. е. радикальные политические группировки, также могут следовать некоему кодексу. Второй тезис маловероятен, так как в случае терроризма целью действий подобных групп является запугивание населения для достижения своих политических целей, и киберпространство предоставляет для этого хорошую возможность.

Томас Рид отмечал, что паникеры кибервойны хотят, чтобы Соединенные Штаты рассматривали кибербезопасность как новый вызов геополитического масштаба. Они считают, что киберпространство становится новой областью для военного соперничества с такими конкурентами, как Россия и Китай, и они думают, что для предотвращения этого нужны новые соглашения по ограничению кибероружия. Даже известны попытки установить международные нормы по этой теме: правительство Великобритании созвало конференцию

[81] Ibidem. pp. 92–97.

в Лондоне в конце 2011 г., первоначально намереваясь сделать Интернет более безопасным на основе согласия с новыми правилами. А Россия и Китай предложили на Ассамблее ООН в сентябре 2011 г. создать «международный кодекс поведения для обеспечения информационной безопасности». После этого дипломаты стали обсуждать, должна ли Организация Объединенных Наций попытаться создать некий эквивалент контроля над ядерными вооружениями в киберпространстве.

По мнению Рида, попытки ввести ограничения на кибероружие посредством международных соглашений имеют три основных проблемы. Первая трудность связана с проведением разграничительной линии между киберпреступностью и политическим киберактивизмом. Например, хакер из страны А украл около 20 000 номеров кредитных карт граждан страны Б с торгового сайта и предал эту информацию огласке. В ответ группа хакеров страны Б взламывает сайты интернет-магазинов страны А и угрожает распространить конфиденциальную информацию по кредитным картам. Как определить границу в этих действиях? Даже если и возможно отличить преступника от спонсируемой государством политической деятельности, в обоих случаях часто используются одни и те же средства.

Вторая трудность носит практический характер: проверить наличие кибероружия фактически невозможно. Точно подсчитать размеры ядерных арсеналов и контролиро-

вать деятельность по обогащению радиоактивных материалов уже представляет огромную проблему, установка же камер, чтобы следить за программистами и «проверять», не разрабатывают ли они вредоносные программы, является несбыточной мечтой.

Третья проблема находится в политической плоскости, и даже более фундаментальна: киберагрессоры могут действовать политически, но не применяя военные методы, так как они, вероятно, очень заинтересованы в том, чтобы быть анонимными. Подрывная деятельность всегда процветала в киберпространстве, поскольку сохранить свою анонимность легче, чем достать арсенал оружия.

Поэтому наступательные кибервозможности становятся объектом спекуляций со стороны различных групп интересов и организаций. Бывший секретарь Военно-воздушных сил и член Совета национальной безопасности США Томас К. Рид в книге «У пропасти: взгляд внутреннего исполнителя на историю холодной войны»[82] даже написал, что в январе 1982 г. президент США Рональд Рейган одобрил план ЦРУ по организации диверсии против экономики Советского Союза. Через канадское посредничество в СССР была заброшена технология с «логической бомбой», которая впоследствии спровоцировала взрыв сибирского газопровода в 1982 г. Инцидент на газопроводе действительно был, хотя

[82] Reed, Thomas C. At the Abyss: An Insider's History of the Cold War. NY: Random House, 2004. https://archive.org/details/atabyssinsidersh00reed

множество нестыковок в книге Томаса К. Рида позволяют усомниться в действительности изложенных фактов. А сама эта книга была названа рядом отечественных специалистов элементом информационной войны. Другой автор, ссылаясь на главу киберкомандования США Кита Александра, даже привязал инцидент на Саяно-Шушенской ГЭС к возможной кибератаке на инфраструктуру российской гидроэлектростанции. Количество подобных спекуляций со временем будет только увеличиваться.

По мнению Бена Бьюкенена из Белферского центра, разделение на оборону и атаку еще более размывает понятие киберпространства, кибербезопасности и кибервойны.

Он считает, что для того, чтобы обеспечить свою кибербезопасность, государства иногда вторгаются в стратегически важные сети других государств и будут угрожать – часто непреднамеренно – безопасности этих других государств, рискуя эскалацией и подрывом стабильности[83].

Одной из серьезных проблем является то, что механика совершения нападения и обороны в кибериндустрии отличается от обычной войны или ядерных сил. Так, например, если вы совершаете атаку в кибероперациях, это требует гораздо больше подготовительной работы – разведки системы противника и т. д., который фактически получает ваш вре-

---

[83] Sebenius, Alyza. Writing the Rules of Cyberwar // The Atlantic, June 28, 2017.https://www.theatlantic.com/international/archive/2017/06/cyberattack-rus-sia-ukraine-hack/531957/

доносный код в свои сети, а не как в контексте холодной войны, когда вы запускаете ракету, но делаете много подготовительной работы на своей территории до запуска этой ракеты. Замыслы уже видны на уровне подготовки. Например, если какое-то государство строит стены и башни, то окружающие народы вряд ли окажутся под угрозой, потому что эти стены и башни не могут двигаться. Но если они строят бомбардировщики и танки, это может выглядеть более угрожающим. В этом контексте легко отличить нападение от обороны и узнать, в чем состоит угроза.

Полковник Чарльз Уильямсон-III В своей статье «Ковровые бомбардировки в киберпространстве», опубликованной в журнале «Вооруженные силы» сравнивал кибероборону с Троей. Этот город «выдерживал атаки объединенных греческих армий десять лет и пал после того, когда по глупости внутрь стен была занесена угроза в виде гигантской деревянной лошади». Имея в виду современные вирусы-трояны, автор сокрушается, что время строительства крепости в Интернете для США прошло, и осталось лишь распознавать врага и выбрасывать его вон, если только будет возможность его найти и если он не успел сделать тайный лаз.

Известный в США журналист, колумнист The New Yorker и обладатель Пулитцеровской премии Сеймур Херш в ноябре 2010 г. в статье «Угроза онлайн» развенчал ряд распространяемых мифов о киберугрозах. «Представители американской разведки и служб безопасности, – пишет С. Херш, –

по большей части согласны, что китайские военные, или, если на то пошло, независимые хакеры, теоретически способны создать определенный уровень хаоса внутри Америки. Однако… эти опасения преувеличиваются из-за путаницы между кибершпионажем и кибервойной. Кибершпионаж – это наука тайного захвата трафика электронной почты, текстовых сообщений, других электронных средств связи и корпоративных данных… А кибервойна предполагает проникновение в чужие сети с целью их подрыва, демонтажа и выведения из строя. Стирание различий между кибервойной и кибершпионажем выгодно для военных подрядчиков…»[84]

И далее: «нет ни единого задокументированного случая отключения электричества, связанного с кибератакой. И мультяшная картинка, на которой хакер нажатием кнопки может выключить фары по всей стране, не соответствует действительности. Национальной электрической сети в США не существует. Есть более ста государственных и частных компаний, которые управляют своими собственными линиями, с отдельными компьютерными системами и отдельными мерами безопасности. Это означает, что поставщик электричества, который оказался под кибератакой, будет иметь возможность воспользоваться энергией из близлежащих систем».

---

[84] Hersh, Seymour. The Online Threat. Should we be worried about a cyber war? // The New Yorker, November 1, 2010. http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all

Далее Сеймур Херш ссылается на Брюса Шнайера, ученого-компьютерщика, заявившего, что он не представляет, как напугавший многих вирус Stuxnet мог создать новую угрозу. «Безусловно, нет никаких фактических доказательств того, что червь был направлен против Ирана или кого-либо еще. Вместе с тем он очень хорошо разработан и хорошо написан и отлично подходит для тех, кто хочет верить, что идет кибервойна». По словам бывшего оперативника Агентства национальной безопасности США, которого цитирует Херш, АНБ получило бесценный опыт по кибершпионажу во время нападения на Ирак в 1991 г. Эти методы совершенствовались в ходе бомбардировок Югославии в 1999 г., затем – во время нападения в 2003 г. на Ирак. «Что бы ни придумали против нас китайцы, мы можем сделать гораздо лучше», – говорит этот специалист. Наши [американские. – *Прим. авт.]* наступательные кибервозможности гораздо более продвинуты».

Наступательные кибероперации могут иметь различные последствия. Они могут быть заменой обычного оружия, такого как бомба, и могут также включать в себя совершенно новые действия, такие как манипулирование финансовыми данными. Эти эффекты могут быть постоянными или они могут быть временными и обратимыми – последнее является особенно интригующей особенностью наступательных кибероперациий. Эрик Розенбах, бывший помощник министра обороны и главный советник по кибернетическим во-

просам в Пентагоне с 2011 по 2015 г., подчеркнул эти качества, когда сказал о кибероперациях следующее: «Место, где я думаю, что это будет наиболее полезно для высокопоставленных политиков, – это то, что я называю «пространство между». Что же это за «пространство между»? У вас есть дипломатия, экономические санкции и, наконец, у вас есть военные действия. Между ними есть это пространство, верно? В кибер есть много вещей, которые вы можете сделать в этом пространстве, которые могут помочь нам достичь национальных интересов»[85].

Первый директор Киберкомандования Кит Александр в начале 2012 г. заявил, что возможности защищать военные сети США ограничены. Иными словами, специальные подразделения не могут защитить сети, которые являются элементом оборонной структуры государства. У Пентагона на тот момент было около 15 тысяч сетей, и следить за каждой в отдельности весьма затруднительно. Была поставлена задача уменьшить количество сетей с 15 до 3 тысяч, а также перейти к облачным вычислениям, что, по мнению экспертов, дешевле и легче в плане защиты[86].

Показательным для понимания тенденций в отношении

---

[85] Cyber Leaders: A Discussion with the Honorable Eric Rosenbach, panel discussion, Center for Strategic and International Studies, Washington, DC, October 2, 2014. http://csis.org/event/cyber-leaders.

[86] Shachtman N. Military Networks 'Not Defensible,' Says General Who Defends Them. January 12, 2012. http://www.wired.com/dangerroom/2012/01/ nsa-cant-defend/

кибервойны, происходящих внутри военного сообщества США, является деятельность Стратегической многоуровневой оценки в структуре Пентагона. На одной из их конференций A New Information Paradigm? From Genes to "Big Data" and Instagram to Persistent Surveillance…Implications for National Security, прошедшей в октябре 2014 г.[87], генерал-лейтенант Киберкомандования армии США Эд Кардон отметил, что «мы находимся в новой глобальной парадигме, вызванной информационно-технической революцией. Вследствие этого угрозы и уязвимости растут, зачастую очень сложными способами. Американские военные доминируют в операционной среде, но теряют в стратегии, потому что мы боремся в информационной среде. Мы находимся в политической борьбе, и кибероперации являются ключом к успеху в этой области. Кибероперации могут использоваться на всех этапах конфликта, но особенно в фазе 0 и фазе 1». Он высказал надежду, что организации, подобные SMA[88], могут помочь преодолеть разрыв между оперативной

[87] A New Information Paradigm? From Genes to "Big Data" and Instagram to Persistent Surveillance…Implications for National Security. 8th Annual Strategic Multi-Layer Assessment (SMA) Conference, Joint Base Andrews, 28–29 October 2014.

[88] Стратегическая многоуровневая оценка (Strategic Multi-Layer Assessment, SMA) – обеспечивает поддержку планирования командам со сложными эксплуатационными императивами, требующими мультидисциплинарных и межведомственных решений, которые не входят в компетенцию службы / агентства. Решения и участники запрашиваются в правительстве США и других структурах. SMA принимается и синхронизируется Объединенным командованием.

и информационной средой.

Занимавший на тот момент пост главы Киберкомандования и директор Национального агентства безопасности адмирал Майкл Роджерс заявил, что «в эпоху цифровых технологий Министерство обороны США должно быть гибкой организацией, способной быстро создавать сообщества, представляющие интерес, в ответ на широкомасштабные непредвиденные кризисы (такие, как Эбола). Большие данные предоставляют новые возможности для отвлечения критической информации от шума, чтобы получать понимание и знания. Однако для того, чтобы использовать силу информации, нам необходимо налаживать партнерские отношения с отдельными лицами и организациями, с которыми мы никогда раньше не работали, от частного сектора, промышленности, научных кругов, НПО, аналитических центров, отдельных лиц и других. Вот почему инструменты и методологии, разработанные сообществом SMA, так важны».

По мнению Роберта Маннинга из Атлантического Совета, «на стратегическом уровне киберконфликт становится новым измерением межгосударственной войны. Усилия по противодействию и подготовке к такой конфронтации возложены на Киберкомандование США и Национальный совет по безопасности в Белом доме. Если употреблять несовершенную аналогию, стратегическая киберугроза имеет много общего с ядерными угрозами. Обе они построены на атаке, обе могут быть причиной огромного разрушения, которое

выведет из строя необходимую национальную инфраструктуру и нанесет ущерб или ослепит вооруженные силы, которые зависят от электроники»[89]. Сторонники такого подхода в США, в свою очередь, разделились на тех, кто выступает за наращивание военных возможностей в киберпространстве, и тех, кто предлагает установить контроль за кибервооружениями, наподобие того, который был обусловлен договорами между США и СССР в сфере ограничения вооружений и носителей ядерных боеголовок.

Есть и те, кто считает, что концепция ядерного сдерживания не подходит для киберпространства, особенно если рассматривать ее с позиции нанесения ответного удара.

Профессор Колледжа информации и киберпространства Национального университета обороны США Джим Чен утверждает, что исследование вопроса возмездия в киберсфере показывает пять уникальных особенностей:

– Таргетирование – непростая задача, поскольку атрибуция в киберпространстве может потребовать значительного времени и усилий. Задержка в атрибуции влияет на сдерживание наказанием, а не сдерживанием путем отрицания, поскольку первый вариант требует, чтобы цель была точно определена до любого ответного удара;

– Кибероружие не так серьезно, как ядерное оружие или другое физическое оружие. В настоящее время в кибернети-

---

[89] Manning, Robert A. ENVISIONING 2030: US Strategy for a Post-Western World. Atlantic Council. Washington DC, 2012. pp. 55-56

ческой области нет виртуального массового разрушительного оружия, такого как ядерное, даже если критическая инфраструктура может стать целью атаки. В этом смысле кибервозмездие относительно ограничено в масштабах и возможностях;

– Неопределенность необходима для сдерживания наказанием. Неважно, используется ли оно в физическом мире или в киберпространстве;

– Возмездие, как ожидается, будет выполнено в течение короткого периода времени, особенно в киберсфере;

– Кибероружие может создавать уникальные эффекты, которые не могут создать ядерное оружие или другое физическое оружие. Кроме того, они хороши в создании неожиданных эффектов в виртуальной среде или в сочетании виртуальной и физической сред[90].

При этом нужно учитывать, что каждый год появляются новые виды кибероружия.

Питер Сингер и Аллан Фридман предполагают, что «различные типы кибероружия будут необходимы для различных целей сдерживания. Когда вы хотите подать сигнал, то «шумное» кибероружие с очевидными эффектами может быть лучше, в то время как скрытое оружие может быть более важным для наступательных операций. В результате, однако, это будет знакомо тем, кто борется с прошлыми страте-

[90] Chen, Jim. Cyber Deterrence by. Engagement and Surprise // PRISM 7, NO. 2, 2017. P. 6.

гиями сдерживания: в стремлении предотвратить войну новое оружие будет постоянно развиваться, что приведет к гонке вооружений. Короче говоря, растущая способность проводить различные виды кибератак еще больше усложняет и без того сложную область сдерживания. Без четкого понимания или реального набора контрольных примеров для изучения того, что работает, странам, возможно, придется в большей степени полагаться на сдерживание путем отрицания, чем на методы ядерного века»[91].

Американские эксперты еще в 2011 г. определили 33 государства, которые включали кибервойну в свое военное планирование. Они варьируются от государств с довольно продвинутыми доктринами и военными организациями, в которых работают сотни или тысячи людей, до стран с более базовыми механизмами, где кибератаку и кибервойну включают в существующие возможности для радиоэлектронной борьбы.

Общие элементы в военной доктрине включают использование кибервозможностей для разведки, информационных операций, нарушения работы критических сетей и услуг, для «кибератак», а также в качестве дополнения к электронной войне и информационных операций. В некоторых государствах предусмотрены конкретные планы информационных

---

[91] Singer, Peter W. and Friedman, Allan. What about deterrence in an era of cyberwar? // Armed Force Journal, January 9, 2014.http://www.armedforcesjournal.com/what-about-deterrence-in-an-era-of-cy-berwar/

и политических операций[92]. Наличие таких стратегий давало американским военным и политикам, которые их поддерживают, обоснование для изменения собственных доктрин и корректировки законодательства.

## Законодательство США и кибервойна

Отмечалось, что «Женевская конвенция и другие инструменты международного права и регулирования определяют, что приемлемо и неприемлемо, что является и не является атакой для традиционной войны. Ничего из этого не относится к киберсфере, где определения кибервойны еще не установлены, не говоря уже о правилах и положениях, которыми должны руководствоваться на практике»[93].

В докладе отециальной комиссии Конгрессу США в 2008 г. было указано, что дать точное определение таким терминам, как «кибератака», «киберпреступление» и «кибертерроризм», проблематично, так как существуют сложности как с идентификацией, так и с намерением или политической мотивацией атакующего. В докладе «кибертерроризм» предлагается определять как «противозаконные атаки и угрозы атак на компьютеры, сети и информационные на-

[92] Lewis, James A. and Timlin, Katrina. Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization. Washington, D.C.: Center for Strategic and International Studies, 2011.

[93] Richards, Julian. Cyber-War: The Anatomy of the Global Security Threat. Basingstoke: Palgrave Macmillan, 2014. p. 19.

копители, когда они сделаны с целью запугивания или угроз в отношении правительства или служащих для достижения политических или социальных целей. Киберпреступление – это преступление, совершенное с помощью компьютеров или имеющее целью компьютеры… Оно может включать в себя кражу интеллектуальной собственности, коммерческих секретов и законных прав. Кроме того, киберпреступление может включать в себя атаки против компьютеров, нарушающие их работу, а также шпионаж»[94].

Эти вопросы остаются актуальными. Что такое «кибервойна», так и не было определено. Но за последние годы в законодательной практике США были заметны явные усилия по милитаризации права в области киберпространства. Часто под надуманными предлогами сенаторы предлагали подкрепить на законодательном уровне ряд жестких мер.

В 2014 г. сенатор США Роберт Мендендес, представляющий комитет по международным отношениям, предложил внести КНДР в список стран – спонсоров терроризма по причине обвинений в кибератаке на компанию Sony.

Но согласно законам США, кто бы ни стоял за этой атакой, она не попадает под определение терроризма, т. к. при взломе компьютеров не было ни насилия, ни применения силы. Поэтому нужно было ввести какую-то новую формулировку, которая устроила бы все заинтересованные стороны в США.

---

[94] Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. January 29, 2008. p. 3–4.

Так, в начале февраля 2016 г. сенаторы Марк Кирк и Кристен Джиллибрэнд представили законопроект, направленный на скорейшее внедрение программ ведения электронной войны, связанной в основном с использованием электромагнитной энергии для перехвата и подавления радиосигналов противника. Законопроект был подготовлен после того, как Пентагон учредил Исполнительный комитет по ведению электронной войны.

А в мае 2016 г. Комитет Сената США по вооруженным силам решил включить требование «акта войны» в отношении кибербезопасности в финансовый план Минобороны США на 2017 год. Требование содержало призыв к президенту «разработать политику по определению того, когда действие, выполняемое в киберпространстве, представляет собой акт войны против Соединенных Штатов»[95].

Учитывая темпы изменений в глобальной цифровой среде, предполагалось, что любое определение должно быть достаточно расплывчатым или достаточно широким, чтобы включать в себя все сценарии, которые, несомненно, будут сопровождать все быстро развивающиеся технологии, такие как Интернет вещей[96], подключенные транспортные сред-

---

[95] Courtney, William and Libicki, Martin C. How to Counter Putin's Subversive War on the West. RAND, August 1, 2016. http://www.rand.org/blog/2016/08/ how-to-counter-putins-subversive-war-on-the-west.html

[96] Internet of things, IoT – концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой…

ства, компактные переносимые технологии и робототехнику.

8 июня 2017 г. законодатели Комитета по вооруженным силам Палаты представителей представили законопроект, согласно которому должностные лица Министерства обороны должны будут уведомить Конгресс в течение 48 часов с момента начала любой чувствительной кибероперации[97].

Закон будет применяться как к наступательным, так и к оборонным кибероперациям, которые проводятся за пределами сетей Минобороны и производят эффекты вне мест, где США участвуют в боевых действиях. Закон не будет применяться к тайным действиям, которые обычно проводятся разведывательными агентствами, а не военными. Это означает, что атака Stuxnet против технической инфраструктуры Ирана, которая является одной из самых известных наступательных кибероперациий и, как полагают, была запущена, в частности, спецслужбами США, не подпадает под требования закона.

Также парадокс состоит в том, что Киберкомандование и Агентство национальной безопасности США имеют одну «прописку» и оба ведомства возглавляет один и тот же человек.

В законопроекте говорилось о необходимости Пентагона

---

[97] Marks, Joseph. Lawmakers to Pentagon: Tell Us When You Use Cyber Weapons. June 8, 2017.http://www.defenseone.com/politics/2017/06/lawmakers-want-no-tice-when-pentagon-uses-cyber-weapons/138539/?oref=d_brief_nl

уведомить комитеты по вооруженным силам Палаты представителей и Сената о любых обзорах кибероружия, чтобы определить, могут ли они использоваться в соответствии с международным правом.

Отдельный законопроект был представлен в июне 2017 г. депутатом Лу Корреа (демократ, Калифорния), призывавшим Пентагон обновить действующую киберстратегию от 2015 г., чтобы наметить конкретную стратегию для кибернаступлений. Это и было сделано впоследствии.

Законопроект также имел намерение прояснить те методы, с помощью которых США будут помогать союзникам по НАТО разрабатывать аналогичные наступательные киберстратегии. В нем говорилось, что наступательная стратегия должна включать в себя конкретные способы, с помощью которых военные могли бы использовать кибервозможности для пресечения традиционных военных атак на суше, море и в воздухе со стороны России или другого противника.

11 июля 2019 г. Палата представителей в Конгрессе США выступила с требованием к Белому дому направить в Конгресс директиву по кибервойне, которую, по словам высокопоставленных чиновников, администрация отказывается передавать в течение многих месяцев. Голосование касалось секретной директивы NSPM-13 о наступательных компьютерных операциях, которую подписал президент Дональд Трамп в августе 2018 года[98].

---

[98] https://www.washingtonpost.com/world/national-security/trump-authorizes-

Из того, что было известно о NSPM-13, военное руководство, в том числе глава Киберкомандования Пол Накасоне, получили предварительное одобрение для нанесения наступательных ударов по иностранным организациям при определенных специфических условиях без дальнейшего разрешения Белого дома. В соответствии с новой политикой военные планировщики могут готовиться к наступательным кибератакам, выискивая уязвимости в компьютерных сетях соперников и внедряя вредоносное программное обеспечение в эти уязвимые места для возможного использования в случае нанесения ответного удара[99].

Очевидно, что данная директива сыграла свою роль в осуществлении кибератак против России.

В 2019–2020 гг. через Конгресс США в рамках 116-й сессии прошло около 40 законопроектов, связанных с вопросами кибербезопасности, будь то акты кражи через Интернет, учреждение нового органа, финансовая помощь другим государствам или состояние боеготовности. Однако если в поисковике сайта Конгресса США[100] сделать запрос на слово «кибервойна», то результат будет нулевым. Очевидно, что вооруженные силы США готовы вести кибервойну, однако

---

offensive-cyber- operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html

[99] Klare, Michael T. Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. November 2019.https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-out-comes-dangerous-new-pathways-escalation

[100] https://www.congress.gov/

что это такое, у американских законодателей понятия нет.

По-видимому, США будут и далее следовать политике двойных стандартов в отношении действий в киберпространстве. Гари Солис указывает, что «определение многих аспектов кибервойны проблематично, поскольку не существует многонационального договора, непосредственно связанного с кибервойной. Это потому, что до сих пор многие аспекты кибервойны не согласованы. В военном праве, а также в международном обычном праве отсутствуют киберспецифичные нормы, а практика толкования применимых норм в государственной практике развивается медленно. Нет даже согласия относительно того, пишется ли «кибератака» в одно слово или в два»[101]. Некоторые ученые проявляют беспокойство из-за такой неопределенности: «ООН потерпела неудачу, страны потерпели неудачу, корпорации потерпели неудачу, в то время как тенденции кибервойны были последовательно, если не экспоненциально, негативными. «Кибер Перл-Харбор» остается угрозой… Бездействие подвергает американских военнослужащих риску: ничто не мешает иностранному государству объявить 10-й флот «Янки-киберпиратами» и обвинить их в совершении кибервоенных преступлений даже в отсутствие явного международного права»[102]. Но в отношении применения своих воен-

[101] Solis, Gary D. Cyber Warfare // The Law of Armed Conflict. International Humanitarian Law in War. Cambridge University Press, 2016. pp. 673–709.

[102] Waugh, Steve. Geneva Conventions for Cyber Warriors Long Overdue //

ных возможностей в США пошли наиболее простым путем. Согласно Международной стратегии действий в киберпространстве от 2011 г. «разработка норм поведения государств в киберпространстве не требует переосмысления обычного международного права и не делает существующие международные нормы устаревшими. Давние международные нормы, определяющие поведение государства – во времена мира и конфликтов, – также применяются в киберпространстве»[103].

National Defense, March 18, 2020.https://www.nationaldefensemagazine.org/articles/2020/3/18/geneva-conven-tions-for-cyber-warriors-long-overdue

[103] International Strategy for Operating in Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011.https://publicintelligence.net/white-house-international-strategy-for-cyber-space/

# Глава 2
# Стратегии и доктрины

Для такого вида деятельности, как война, независимо от ее формы, вооруженные силы и руководство, принимающее решения, разрабатывают стратегии и доктрины. Без них не обходится ни одно государство. Существуют политические декларации, план действий на определенное количество лет и инструкции, как действовать в определенных ситуациях. Кибервойна не является исключением. При этом, хотя у США есть целое Киберкомандование для манипуляций с Интернетом, военными коммуникациями и технологиями беспроводной связи, киберпространство является приоритетным направлением не только у военных, разведки и других специализированных ведомств, но и для внешней политики США в целом. Дипломатические усилия и военное строительство в этой области взаимосвязаны. Также действия в киберпространстве могут отличаться по методике и целеполаганию. В связи с этим все виды вооруженных сил адаптировали свои подходы к киберпространству. Объединенный комитет начальников штабов в качестве зонтичной организации также издавал ряд стратегических и доктринальных документов по теме киберпространства.

Поскольку национальная стратегия безопасности, а с недавнего времени еще и национальная киберстратегия на-

ходятся в ведении политического руководства страны, военные были вынуждены регулярно адаптировать свои подходы.

В данной главе мы проанализируем эволюцию ряда доктрин и стратегических документов в этой области. Так как некоторые из них впоследствии были отменены, а другие заменены на более актуальные, то будут проанализированы наиболее значимые и адекватные к настоящему времени. Хотя некоторые старые документы также упомянуты, чтобы показать историческую преемственность и формировавшийся контекст.

## Эпоха Клинтона – Буша

Пожалуй, самый ранний документ высокого уровня, где фигурирует приставка «кибер» – это Президентская директива № 63 от 1998 г. – в ней использовались такие термины, как «кибератака», «киберсистемы», «киберинформационные военные угрозы» и «киберинфраструктура». В ней отмечалось, что киберугрозы были выявлены в области защиты критической инфраструктуры и понимаются как «электронные, радиочастотные или компьютерные атаки на информацию или компоненты коммуникации, которые контролируют критическую инфраструктуру»[104].

Следующим президентским документом стал «Защита

[104] Clinton, William J. Presidential Decision Directive 63, The White House, Washington, DC, 1998.

американского киберпространства, национальный план по защите информационных систем»[105]. В нем содержалось 33 новых понятия с приставкой «кибер-», которые трактовались с позиции национальной безопасности. Среди них были такие термины, как «кибервойна» и «кибернация». Хотя основная идея плана была о безопасности, а не военных действиях, Пентагон через некоторое время начал адаптировать этот терминологический аппарат для своих нужд.

В начале 2000-х гг. Министерство обороны США руководствовалось ограниченными документами в этой сфере. Известна стратегия Пентагона по информационному обеспечению (Information Assurance, IA) от 2004 г. Затем ее обновленная версия была переиздана в декабре 2005 г.[106]. В ней затрагивались вопросы сертификации и управления компьютерными сетями, которые находились в ведении Пентагона. Там не говорилось о кибератаках и каких-либо операциях в киберпространстве.

В 2006 г. был издан официальный доклад Пентагона, подписанный Дональдом Рамсфельдом, под названием «Дорожная карта информационных операций»[107]. В этом документе гласилось, что информация, которая является частью пси-

---

[105] Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue. Washington, DC: The White House, 2000.

[106] Information Assurance Workforce Improvement Program. DoD 8570.01M. https://fas.org/irp/doddir/dod/m8570_01.pdf

[107] Brookes, Adam. US plans to 'fight the net' revealed // BBC, 27 January 2006. http://news.bbc.co.Uk/2/hi/americas/4655196.stm

хологических операций вооруженных сил, в конечном счете попадает на компьютеры и телевизионные экраны обычных американцев. Было указано, что «информация, предназначенная для зарубежной аудитории, в том числе общественной дипломатии, а также психологические операции, все больше и больше потребляется отечественной аудиторией… Послания в психологических операциях будут все чаще озвучиваться в средствах массовой информации для гораздо более широкой аудитории, в том числе американской общественности. Стратегия должна быть основана на предпосылке, что Министерство обороны будет «бороться с сетью», так как это может быть система вооружений противника»[108]. Выражение «fight the net» неоднократно встречается в документе. Специалисты Пентагона имели в виду широкий спектр возможностей, связанный с интернет-технологиями, – от блокировки и радиоэлектронного подавления чужих ресурсов до чистки информационного контента в информационном поле, которое представляет стратегический интерес США (например, цензурирование призывов к очередной антивоенной кампании или журналистского расследования).

Между тем, в том же 2006 г. Пентагон официально признал, что использует специфические методы в интернет-простран-стве, т. е. ведет «черную пропаганду», иначе гово-

---

[108] Information Operations Roadmap // BBC, 30 October 2003. http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/27_01_06_psyops.pdf

ря, распространяет дезинформацию[109]. Официально, согласно заявлению командующего «операциями по взаимодействию» Центрального командования ВС США Ричарда Мак-Нортона, это было сделано для того, чтобы читатели имели возможность читать онлайн позитивные истории. Поэтому в сообщениях блогерами-военными намеренно распространялась некорректная, неправдоподобная и неполная информация с места ведения боевых действий.

Всеобъемлющая национальная инициатива по кибербезопасности (Comprehensive National Cybersecurity Initiative, CNCI) была учреждена президентом Джорджем Бушем-младшим в президентской директиве по национальной безопасности 54 / президентской директиве по внутренней безопасности 23 (NSPD-54 / HSPD-23) в январе 2008 года[110]. Инициатива описывала цели кибербезопасности США и охватывала несколько учреждений, включая Министерство внутренней безопасности, Управление по вопросам менеджмента и бюджета и Агентство национальной безопасности.

Министерство обороны США в нем упоминалось один раз – «Министерство внутренней безопасности сможет адаптировать сигнатуры угроз, определенные АНБ, в ходе его миссии по разведке за рубежом и информационного обеспече-

---

[109] Raw obtains CENTCOM email to bloggers. October 16, 2006. http://www.rawstory.com/news/2006/Raw_obtains_CENTCOM_email_to_bloggers_1016. html

[110] https://fas.org/irp/offdocs/nspd/nspd-54.pdf

ния Минобороны для использования в системе EINSTEIN 3 для поддержки Федеральной системы безопасности Министерства внутренней безопасности. Обмен информацией о кибервторжениях будет проводиться в соответствии с законами и надзором за деятельностью, связанной с внутренней безопасностью, разведкой и обороной в целях защиты неприкосновенности частной жизни и прав граждан США»[111].

Устав по сетевым операциям Министерства обороны США был обнародован в ноябре 2008 г. и представлял собой довольно объемный документ в 273 страниц[112]. В нем содержалось общее описание сетевых операций, их компонентов, принципов и эффектов; распределение ролей и ответственности, список центров и управлений; уровни (глобальный, театра военных действий, тактический); политика применения сетевых операций и методы их оценки.

Сетевые операции были представлены широким спектром компонентов, необходимым для получения информационного превосходства бойцов.

По своей сути это был, скорее, технический документ с указанием стандартов, иерархий и словаря, чем некая стратегия с политическими целями и идеологическими установ-

---

[111] The Comprehensive National Cybersecurity Initiative, 2008. p. 3.https://fas.org/irp/eprint/cnci.pdf

[112] Network Operations. FM 6-02.71. Headquarters Department of the Army Washington, DC. 19 November, 2008.

ками.

## Прицел на киберпространство

Новая стратегия, которая отражала видение Пентагона в отношении киберпространства, идентичности и информационного обеспечения, вышла в августе 2009 г.

Там было обозначено, что:

– Миссии и операции Министерства обороны должны продолжаться в любых киберусловиях и ситуациях;

– Киберкомпоненты систем вооружений Министерства обороны и других оборонных платформ должны функционировать должным и ожидаемым образом;

– Кибератакивы Министерства обороны коллективно, последовательно и эффективно применяются для собственной обороны;

– Министерство обороны имеет готовый доступ к информации, а также каналам командования и управления, чего нет у врагов;

– Информационное предпринимательство Министерства обороны безопасно и плавно расширяется на партнеров по миссии.

Киберпространство в данной стратегии упомянуто как глобальный домен внутри информационного предпринимательства, который охватывает конструкт Сетевых операций по активности и обороне Глобальной информационной сети

и в рамках Стратегического командования США интегрирует сетевые операции с другими кибероперациями через новое Киберкомандование.

«Киберобеспечением» назывались меры по подготовке сетецентричных миссий и информационных предприятий для ответа на враждебные действия в «киберврвремени».

Идентификационное обеспечение обозначено как меры по достижению интеграции и аутентификации идентичности информации, инфраструктуры и оформления процессов и процедур при сохранении, в то же время, безопасности и приватности для поддержки операций Министерства обороны.

А информационное обеспечение – это меры по защите и обороне информации и информационных систем, вытекающие из доступности, интегрированности, аутентификации, конфиденциальности и отсутствия сбоев. Оно включает в себя возможность восстановления информационных систем методом внедрения мощностей по защите, детекции и реагирования.

Среди вызовов были названы вопросы объединения киберресурсов, готовность отражать вражеские действия, включая иррегулярную войну и кибератаки, зависимость от кибермощностей, киберасимметрию, когда атакующая сторона может нанести несоизмеримый ущерб по сравнению с собственными затратами, а также прогнозы в отношении ки-

берэффектов[113].

В 2009 г. также выходит План ВВС США для киберпространства. Это был небольшой документ на 12 страницах, регламентировавший дальнейшие действия ВВС по обеспечению соответствующих директив и меморандумов Президента США и Министерства обороны по теме операций в киберпространстве.

Отмечалось, что для выполнения поставленных задач ВВС будет агрессивно заниматься:

– консолидацией и защитой сегмента ВВС в сетях Минобороны;

– созданием мощностей через повышение способностей персонала и разработку инновационных операционных возможностей, подключение новых партнеров и интеграции их возможностей в воздухе и космосе;

– разработкой доктрины, политики, безопасности и рекомендаций для эффективной работы в киберпространстве;

– приоритетами и поиском необходимых ресурсов для киберпространства;

– увеличением разведывательных и аналитических возможностей;

– смещением парадигм с фокусировки на сети к фокусировке на миссии;

---

[113] Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy, Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, August 2009. p. 4.https://dodcio.defense.goV/portals/0/documents/dod_ia_strategic_plan.pdf

– разработкой киберэкспертизы для нужд миссий;

– повышением возможностей принятия решений у командиров через повышение ситуационной осведомленности;

– изменениями в поведении, практике и культуре через внедрение тренингов, стандартов, коммуникации и отчетности;

– модернизацией и поддержкой технологий и оборудования, которые используются для боевых коммуникаций;

– удалением «шероховатостей» в системе командования и управления, безопасности и доктрине для улучшения междоменной эффективности;

– комбинированием и сведением традиционных операций с операциями в киберпространстве для сдерживания атак и влияния на результаты;

– партнерством с Министерством обороны и другими службами по интеграции, синхронизации и консолидации сетевой инфраструктуры, используемой объединенными силами[114].

Также отмечалось, что промышленность поставляла 90 % всего необходимого для инфраструктуры киберпространства, что потенциально коррелировалось с успехом миссий Министерства обороны. При этом указывалось о необходимости разработки новых механизмов взаимодействия с сообществами по исследованию и инновациям, связанными с

[114] The United States Air Force Blueprint for Cyberspace. November 2, 2009. p. 3–4.https://nsarchive2.gwu.edu//dc.html?doc=2692105-Document-4

киберпространством, чтобы точно понимать новые нужды и приоритеты в науке и технологиях. Также говорилось о внедрении соответствующей киберкультуры у военнослужащих.

Следующий документ представлял обзор, подготовленный Лабораторией по кибервойне, эксплуатации и информационному доминированию Атлантического Центра Космических и Военно-морских систем. В нем было предложено определение «кибервойны», как война в киберпространстве, по сути, любое действие, направленное на то, чтобы заставить противника выполнить нашу национальную волю, и осуществляемое против программного, аппаратного и компьютерного обеспечения управления процессами в системе противника[115].

Были выделены основные элементы, необходимые для создания высокоэффективной стратегии кибервойны:

– Интеллектуальное слияние и сотрудничество;

– Объединение разведки из нескольких источников, чтобы делать адекватные выводы;

---

[115] Houten, Vincent Van. Space and Naval Warfare Systems Center Atlantic, An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab, January 28, 2010. p. 4.https://assets.documentcloud.org/documents/3521680/Document-03-Vin-cent-Van-Houten-Space-and-Naval.pdf

# Конец ознакомительного фрагмента.