КИБЕРВОЙНЫ — ОРУЖИЕ ЗАВТРАШНЕГО ДНЯ?

Роман Кисурин

Тот, кто преуспел в военном деле, подчиняет чужие армии, не вступая в битву, захватывает чужие города, не осаждая их, и разрушает другие государства без продолжительного сражения. Он должен сражаться под Небом с высшей целью «сохранения». Тогда его оружие не притупится и плоды победы можно будет удержать. В этом стратегия наступления.

Сунь Цзы. *Искусство войны*

Основной проблемой при обсуждении феномена кибервойн являются используемые определения и термины. Часть специалистов по информационной безопасности определяют понятие «кибервойны» как действия, предпринятые исключительно в военное время, и включают кибернетическую войну в более общую стратегию глобального военного конфликта как одну из его частей. Другие эксперты трактуют это понятие предельно широко, подразумевая под ним весь спектр незаконной сетевой активности, — от кибертерроризма и кибер-преступности до подросткового кибервандализма. Эти две крайние точки зрения вносят дополнительную путаницу в определение того, чем же фактически сегодня является кибервойна и какие именно отличия позволяют нам вывести эту форму социального конфликта в отдельный тип военных взаимодействий в специфическом, не свойственном какому-либо другому известному конфликту пространстве. Причины возникновения широкой дискуссии о феномене «кибервойн» напрямую связанны с глубокими изменениями в структуре и социальной организации современного общества и с появлением нового типа сетевых сообществ и форм взаимодействия между ними.

Проблематизация этой темы происходит не только в сфере аналитических дискуссий по поводу возможного будущего, но и в рамках актуальной повестки дня в политико-правовом и медийном поле. Сегодня такая дискуссия инициирована и поддерживается по преимуществу Соединенными Штатами в рамках разработки стратегии национальной безопасности и, как следствие, новой концепции «войн завтрашнего дня».

В качестве реализованных примеров подобной стратегии Соединенными Штатами можно упомянуть:

— национальную стратегию кибербезопасности, предусматривающую нанесение превентивных ударов обычными вооружениями в случае обнаружения масштабной кибератаки на правительственные объекты и систему гражданской инфраструктуры США;

— создание сети специализированных центров национальной кибербезопасности по всему миру, таких как NCCIC[1];

— организацию специальных «кибервойск», специализирующихся на разработке принципиально новых методов ведения военных действий посредством использования «киберпространства», и придание этим методам активного, наступательного характера. Подобные

[1] *Национальный центр кибербезопасности и интеграции коммуникаций (NCCIC). Центр является составной частью подразделения Министерства национальной безопасности — директората обеспечения защиты информации и инфраструктур.*

войсковые группы уже существуют в США и некоторых странах НАТО, например, такие как: NETWARCOM, CYBERFOR и FCC[1]

В 1982 году канадский писатель-фантаст Уильям Гибсон в новелле «Сожжение Хром» впервые использовал термин «киберпространство» в качестве метафорической абстракции, обозначающей второй мир, виртуальную реальность, существующую внутри компьютеров и компьютерных сетей. Сегодня этот термин популярен как никогда и включается в качестве приставки к таким общеупотребительным понятиям, описывающим феномен конфликта, как «война», «оборона», «атака», «терроризм», «преступность», и по отношению ко многим другим, вводя их в новый контекст значений, в котором, учитывая отсутствие общепринятой инструментальной и описательной составляющей, эти термины могут приобретать совершенно отличное от общепринятого смысловое содержание.

К истории вопроса

Идея построения вычислительных сетей с коммутацией пакетов[2] зародилась в США в конце 50-х, в самый разгар холодной войны. Министерство обороны США задалось вопросом, что произойдет с национальной системой коммуникаций в случае ядерной войны и как обеспечить ее работоспособность в случае возможного глобального конфликта. Ответом на этот вопрос стало создание в начале 1958 г. по указанию Д. Эйзенхауэра в рамках министерства обороны США правительственного ведомства, сыгравшего в дальнейшем ключевую роль в появлении Всемирной паутины, — «Агентства передовых исследовательских проектов» (ARPA). Одной из основных причин создания подобного агентства явились успехи, которые демонстрировал Советский Союз в сфере освоения космических технологий, и, в частности, запуск второго искусственного спутника Земли, оснащенного коммуникационным оборудованием двойного назначения.

В момент своего создания ARPA представляла собой довольно необычную организацию, состоящую больше чем наполовину из научных работников, имеющих звание докторов философии и занимающихся разработками концепций и методов соединения компьютеров друг с другом. В 1962 г. Пол Беран (Paul Baran) из RAND[3] Corporation в сотрудничестве с ARPA представил свой доклад «On Distributed Communication Networks», в котором было выдвинуто предложение использовать децентрализованную систему коммутаций компьютеров, когда в случае разрушения большей части единиц сети она сохраняет свою работоспособность.

Итогом десятилетней деятельности ведомства стала разработка в 1969 г. проекта сети, объединившей суперкомпьютеры оборонных, научных и управляющих центров в единую сеть, которая получила название ARPANET (Advanced Research Projects Agency Network). Первая действующая информационная сеть ARPANET объединила компьютерные системы университетов Лос-Анджелеса, Стэнфорда, Санта-Барбары и Солт-Лейк Сити. Основной декларируемой целью проекта было изучение способов поддержания связи в условиях ядерного нападения и разработка концепции децентрализованного (распределенного) управления военными и гражданскими объектами в период ведения войн.

История глобальной сети Интернет начинается примерно с 1980 года, когда ARPA стало переводить компьютеры, подключенные к своим исследовательским центрам, на новый универсальный протокол передачи данных и объединения сетей TCP/IP[4]. В 1983 году Министерство обороны США разделило ARPANET на две независимые сети: гражданскую — ARPANET и военную — MILNET. С этого момента компьютерные сети стали появляться во многих научных и государственных учреждениях США и европейских стран, а документация по сетевым протоколам становится доступна широкой аудитории специалистов.

И именно в этот момент начинаются первые известные взломы компьютерных сетей хакерами[5]. Одними из первых известных взломщиков ARPANET были Кевин Митник, получивший в 1983 году доступ к самым защищённым компьютерам того времени, компьютерам Пентагона, и к электронной документации Министерства обороны США, и Кевин Поулсен, взломавший засекреченную базу данных ФБР. В это

---

[1] *CYBERFOR и NETWARCOM — специальные подразделения армии США, в обязанности которых входят криптографическая работа, информационная разведка, обеспечение информационной поддержки, защита от нападений через компьютерные сети и с использованием противником высоких технологий.*

[2] *Коммутация пакетов (КП, packet switching) — разбиение сообщения на «пакеты», которые передаются отдельно и каждый из которых имеет свой адрес назначения. Разница между сообщением и пакетом: размер пакета ограничен технически, сообщения — логически. При этом, если маршрут движения пакетов между узлами определён заранее, говорят о виртуальном канале (с установлением соединения).*

[3] *Корпорация РЭНД (RAND Corporation), первоначально учрежденная в 1948 году как независимый некоммерческий институт, финансируемый ВВС США и Фондом Форда, положила начало исследованиям в области системного анализа и теории игр, а также созданию долгосрочных прогнозов, всестороннему анализу стратегических и технических проблем в интересах обеспечения национальной безопасности США. С начала 1960-х специалисты RAND занимаются вычислительной техникой и программированием. В разное время в экспертный совет корпорации входили такие известные личности, как Фрэнсис Фукуяма и Збигнев Бжезинский.*

[4] *TCP/IP — аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/интернет-протокол) — это согласованный заранее стандарт, служащий для обмена данных между двумя узлами (компьютерами в сети), причём неважно, на какой платформе эти компьютеры и какая между ними сеть. TCP/IP служит мостом, соединяющим все узлы сети воедино, за это он и завоевал свою популярность. TCP/IP зародился в результате исследований, профинансированных ARPA в 1970-х годах. Он был задуман как общий стандарт, который объединит все сети в единую виртуальную «сеть сетей» (internetwork).*

[5] *Исследователи, использующие обширные компьютерные знания для осуществления несанкционированных действий в компьютерных сетях.*

Один из центров киберкомандования армии США

же время компьютерными энтузиастами разрабатываются первые средства автономного нападения на компьютеры и сети, вредоносные программы, самостоятельно размножающиеся и атакующие компьютеры в сети, — вирусы и черви.

Все это привело к тому, что в середине 1980-х годов Бэрри Коллин, старший научный сотрудник Американского института безопасности и разведки, предлагает термин «кибертерроризм» для обозначения террористических действий в виртуальном пространстве. Предложенный термин не получил широкого применения и до начала 90-х использовался для составления аналитических прогнозов на будущее, однако тогда никто и не предполагал, в том числе и сам автор, утверждавший, что о кибертерроризме можно будет говорить не раньше, чем в первые десятилетия XXI века, что первые массированные кибератаки будут зафиксированы уже в начале 1990-х годов.

Оружие завтрашнего дня?

Появление Интернета не только радикально изменило средства символической коммуникации, но и постепенно трансформировало реальную социальную организацию общества. Начиная с начала 1990-х г. в среде аналитиков и экспертов в области информационной безопасности проводятся активные дискуссии в области таких тем, как сетевые и информационные войны, обсуждаются вопросы возникновения сетевых сообществ и форм, а также организуемые ими конфликты в сфере Интернета.

Впервые публично о возможности войны в информационной сфере заговорили в середине 1990-х г. XX в. Сам термин «кибернетическая война» ввели в обиход исследователи пентагоновского центра «РЭНД». В частности, в меморандуме 1993 года под названием «Кибернетическая война грядет!» аналитики Джон Аркия и Дэйвид Ронфелдт утверждали, что военное столкновение между крупными нациями в киберпространстве практически неизбежно.

В конце 1996 г. на одном из симпозиумов представитель Министерства обороны США Роберт Банкер представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия. Ключевым моментом в нем явилось разделение всего театра военных действий на две составляющих — традиционное пространство и киберпространство, причем последнее, по словам автора, имеет более важное значение. Банкер предложил доктрину «киберманевра», которая должна стать естественным дополнением существующих военных концепций. В число сфер ведения боевых действий помимо земли, моря, воздуха и космоса было предложено включить и инфосферу. Как подчеркнул военный эксперт, основными объектами поражения в грядущей войне станут информационная инфраструктура и психология противника.

Место кибервойны в классической войне на примере новой стратегической концепции глобального удара не так давно озвучил и заместитель председателя «Объединенного комитета начальников штабов США» генерал морской пехоты Джеймс Картрайт. По его словам, нижний предел потенциала глобального удара «подразумевает возможность достичь любой точки Земли в течение часа», а верхний предел — «примерно за 300 миллисекунд». «Это — кибернетика», — добавил он. Такие взгляды Джеймс Картрайт выразил в ходе высказанных им соображений по поводу того, как должно выглядеть сдерживание в XXI веке. Интересно, что в том же докладе, говоря о распространении баллистических ракет, Картрайт отметил, намекая на кибероружие, что новое нападение — причем, возможно, ядерное — «может занять лишь несколько минут. Это означает, что нам необходимы средства сдерживания, которые позволят предотвратить подобный конфликт, ядерными силами ограничиваться нельзя».

В ходе общественных дискуссий, спровоцированных заявлениями политиков и военных экспертов в связи с громкими событиями последних нескольких лет, которые впервые были классифицированы как кибервойны, некоторые специалисты по информационной безопасности высказывали и альтернативные точки зрения на происходящие события. Знаменитый бывший хакер Кевин Поулсен обвинил политиков и СМИ в том, что они злоупотребляют фактором страха: «В каком-то смысле эстонские атаки были проще, чем предыдущие «кибервойны» — например, между израильскими и палестинскими хакерами, Индией и Пакистаном, Китаем и США, — сказал он, — но даже те атаки нельзя было назвать кибервойной, по крайней мере, если следовать научному определению этого термина. Я сомневаюсь, что когда-либо мы столкнемся с настоящими кибервойной или кибертерроризмом».

И тем не менее большинство экспертов сходятся на том, что в современной ситуации имеет смысл говорить о «холодной кибервойне», то есть о негласных военных действиях, разворачивающихся по всем правилам современной военной науки в киберпространстве. Холодной эту войну делает ее юридический статус, так как такая война никогда не была объявлена, соответственно подобную войну никогда нельзя будет закончить традиционным дипломатическим способом, а также характер ведения боевых действий,

Штаб-квартира АНБ. Мэриленд, США

Фрагмент разностной машины Чарльза Бэббиджа

характеризующийся повышенной скрытностью и незаметностью, и во многом отсутствием физических жертв. Впрочем, из-за того, что выявить источник кибератак, как правило, очень сложно или даже невозможно, вся информация о подготовке к кибератакам на сегодняшний день, по мнению независимых специалистов, не имеет реальных доказательств. И, как и в классической холодной войне, в киберпространстве уже давно идет собственная гонка вооружений. По многочисленным сообщениям агентств, специализирующихся на информационной безопасности, сильнейшие государства мира активно создают и расширяют инфраструктуру для эффективного ведения боевых действий в киберпространстве. Страны разворачивают специализированное ПО, тестируют сети и налаживают шпионскую деятельность в рамках подготовки к использованию Интернета для ведения войн. В частности, активно готовятся к конфликтам в киберпространстве США, Израиль, Россия, Китай и Франция, некоторые страны Ближнего Востока и некоторые ведущие государства ЕС. Все они регулярно устраивают «кибератаки» друг на друга, не только проверяя на прочность инфраструктуру безопасности, но и исходя из локальных политических мотивов. В качестве характерных примеров подобных войн можно привести несколько событий последнего времени, получивших широкий резонанс в СМИ и в высказываниях официальных лиц заинтересованных стран.

Кибернетическая война с Эстонией

После того как в апреле 2007 года эстонские власти приступили к демонтажу бронзовой статуи Советского солдата, началась мощнейшая кибератака, парализовавшая работу всего госаппарата страны, так как к тому моменту Эстония уже давно перешла на электронный документооборот. Армия роботов, состоявшая из зараженных компьютеров, парализовала при помощи бесконечных запросов, отправленных на соответствующие серверы, работу парламента, министерств, банков и средств массовой информации. Атакующие компьютеры находились в разных частях земного шара, однако эстонские эксперты до сих пор убеждены в том, что цифровая атака была осуществлена Россией.

Важный момент — события 2007 года в Эстонии повлекли за собой изменения в планировании системы безопасности НАТО, и фактическим результатом этого стало включение вопросов кибербезопасности в актуальную повестку дня правительства самой Эстонии и других стран НАТО и создание в Таллине в 2008 году Центра компетенции НАТО по борьбе с кибертерроризмом. В ближайшее время, по предложению США, на его базе будет создана лаборатория экспертизы киберпреступлений по стандартам ФБР, а также международный учебный центр. В 2010 году, по предложению Эстонии, страны ЕС проведут совместные учения по противодействию киберпреступности.

Российско-грузинский конфликт 08.08.08

Прообразом модели будущих кибервойн, по мнению экспертов, может служить и недавний конфликт между Грузией и Россией в августе 2008 года. Итогом этого конфликта в киберпространстве стала полная недоступность на время боевых действий всех правительственных информационных интернет-ресурсов грузинской стороны. Особенность конфликта заключалась в том, что с обеих сторон эти нападения были скоординированы с действиями реальной армии.

Китай против США: история с Google

Продолжающийся конфликт компании Google с властями КНР в контексте складывающихся напряженных межгосударственных отношений между США и Китаем воспринимается специалистами как конфликт в области кибербезопасности.

Соединенные Штаты обвиняют КНР в том, что на протяжении последних 15 лет Китай развернул широкомасштабный сбор секретных данных об американских компаниях и правительстве. Американские аналитические агентства предсказывают, что будущие атаки могут быть нацелены на сети и базы данных Пентагона, а данные, которые могут добыть китайские хакеры по заказу правительства, будут использованы как в мирное время, так и в случае возникновения военного конфликта с США.

В докладах Министерства обороны США добавляется, что эти нападения из Китая более изощренны и лучше организованы, чем те, что когда-либо исходили от хакерских групп из других стран, а «конфликт достиг уровня военной кампании», что позволяет американским экспертам сделать вывод, что за атаками стоит китайское правительство, и классифицировать данный конфликт как «кибервойну».

Но не все прозрачно и с самой корпорацией Google Inc. Из открытых источников известно, что первая по популярности в мире поисковая система, обрабатывающая более 45 миллиардов запросов в месяц,

Знамение будущего. Ханс Грудинг, около 1935 г.

связана рядом партнерских соглашений с Агентством национальной безопасности (NSA), ведущей и наиболее секретной разведывательной организацией в США, в компетенцию которой входят и вопросы, связанные с военными действиями в киберпространстве.

Заключение

Основная дилемма «кибервойн» — отсутствие видимой границы между кибератакой и кибезащитой. Такая ситуация позволяет потенциальному государству-агрессору легко получить в случае необходимости casus belli для развязывания реального военного конфликта. И до тех пор, пока все используют одинаковые процессоры, операционные системы и протоколы сетевого взаимодействия, провести четкую грань между оружием киберзащиты и кибернападения будет невозможно. Этот фактор, названный экспертами Агентства национальной безопасности США — «equities issue» (проблемой собственного капитала), делает потенциально равноуязвимыми все стороны, готовящиеся к кибервойне.

Но не следует забывать также и о том, что большинство наиболее востребованных программных продуктов в мире создается под негласным контролем американских специальных служб, связанных с разработкой средств нападения и защиты в киберпространстве. Среди таких продуктов следует упомянуть и самую популярную в мире операционную систему Microsoft Windows, а также две мегакорпорации, производящие до 95% всех процессоров использующихся в персональных компьютерах, — Интел и АМД.

Можно с уверенностью говорить о том, что практически все более или менее крупные программные продукты, от операционных систем до криптографических шифров содержат так называемые «черные ходы». Подобные уязвимости сознательно или по ошибке, оставленные разработчиками, позволяют контролировать вычислительные мощности не только отдельных компьютеров, но и целых сетей, состоящих из десятков и сотен тысяч вычислительных машин. И сегодня вероятность того, что домашние компьютеры внезапно могут превратиться в элемент военной киберсистемы, атакующей совсем не виртуальных противников, реальна, как никогда.